EVERYONE'S NIGHTMARE
PRIVACY AND DATA BREACH RISKS

MAY 2014 EDITION

This edition is updated as of May 2014. To obtain a copy of this edition by email or to be placed on the mailing list for future editions, please email PrivacyWhitePaper@edwardswildman.com.

To learn more about our firm, or our Privacy and Data Protection Practice, please visit edwardswildman.com.

EDWARDS WILDMAN

BOSTON • CHICAGO • HARTFORD • HONG KONG • ISTANBUL • LONDON • LOS ANGELES • MIAMI • MORRISTOWN
NEW YORK • ORANGE COUNTY • PROVIDENCE • STAMFORD • TOKYO • WASHINGTON DC • WEST PALM BEACH

This white paper is for guidance only and is not intended to be a substitute for specific legal advice. If you would like further information, please contact the Edwards Wildman Palmer LLP lawyer responsible for your matters.

EDWARDS WILDMAN PALMER LLP

Edwards Wildman's Privacy & Data Protection Group

Mark E. Schreiber, Partner, Chair, Steering Committee, Privacy and Data Protection Group	+1 617 239 0585	Boston	mschreiber@edwardswildman.com
Theodore P. Augustinos, Partner, Steering Committee, Privacy and Data Protection Group	+1 860 541 7710	Hartford	taugustinos@edwardswildman.com
Laurie A. Kamaiko, Partner, Steering Committee, Privacy and Data Protection Group	+1 212 912 2768	New York	lkamaiko@edwardswildman.com
Sarah Pearce, Partner, Steering Committee, Privacy and Data Protection Group	+44 (0) 20 7556 4503	London	spearce@edwardswildman.com

Barry J. Bendes, Partner	+1 212 912 2911	New York	bbendes@edwardswildman.com
Michael P. Bennett, Partner	+1 312 201 2679	Chicago	mbennett@edwardswildman.com
Mark Deem, Partner	+44 (0) 20 7556 4425	London	mdeem@edwardswildman.com
Edwin M. Larkin, Partner	+1 212 912 2762	New York	elarkin@edwardswildman.com
Clinton J. McCord, Partner	+1 310 860 8715	Los Angeles	cmccord@edwardswildman.com
Stephen M. Prignano, Partner	+1 401 276 6670	Providence	sprignano@edwardswildman.com
Ronie M. Schmelz, Partner	+1 310 860 8708	Los Angeles	rschmelz@edwardswildman.com
Thomas J. Smedinghoff, Partner	+1 312 201 2021	Chicago	tsmedinghoff@edwardswildman.com
David S. Szabo, Partner	+1 617 239 0414	Boston	dszabo@edwardswildman.com
Barry Leigh Weissman, Partner	+1 310 860 8704	Los Angeles	bweissman@edwardswildman.com
David L. Anderson, Counsel	+1 310 860 8710	Los Angeles	danderson@edwardswildman.com
Patrick J. Concannon, Counsel	+1 617 239 0419	Boston	pconcannon@edwardswildman.com
Ellen M. Giblin, Counsel	+1 617 239 0484	Boston	egiblin@edwardswildman.com
Sharon Monahan, Counsel	+1 202 939 7902	Washington, DC	smonahan@edwardswildman.com
Dev Batta, Associate	+1 212 912 2977	New York	dbatta@edwardswildman.com
Karen L. Booth, Associate	+1 860 541 7714	Hartford	kbooth@edwardswildman.com
Zachary N. Lerner, Associate	+1 212 912 2927	New York	zlerner@edwardswildman.com
Ari Z. Moskowitz, Associate	+1 202 939 7934	Washington, D.C.	amoskowitz@edwardswildman.com
Matthew Murphy, Associate	+1 401 276 6497	Providence	mmurphy@edwardswildman.com
Jamie Notman, Associate	+1 617 235 5303	Boston	jnotman@edwardswildman.com
Erin Pfaff, Associate	+ 310 860 8717	Los Angeles	epfaff@edwardswildman.com
Nicholas A. Secara, Associate	+1 212 912 2785	New York	nsecara@edwardswildman.com
Ajita Shah, Associate	+44 (0) 20 7556 4385	London	ashah@edwardswildman.com
Kayla Tabela, Associate	+1 617 239 0734	Boston	mtabela@edwardswildman.com
Nora A. Valenza-Frost, Associate	+1 212 912 2763	New York	nvalenza-frost@edwardswildman.com

As of November 2014

TABLE OF CONTENTS

May 2014 Edition

Everyone's Nightmare: Privacy and Data Breach Risks

TABLE OF CONTENTS

(continued)

Page

TABLE OF CONTENTS

(continued)

Page

TABLE OF CONTENTS

(continued)

Page

TABLE OF CONTENTS

(continued)

Page

TABLE OF CONTENTS

(continued)

Page

EDWARDS WILDMAN PALMER LLP

May 2014

Everyone's Nightmare: Privacy and Data Breach Risks

I. Introduction: The Increasing Scope of Privacy and Data Breach Risks

The rapid growth of information in electronic form has resulted in a concomitant exposure of companies to risks and liabilities arising from the collection, use, storage and transmission of information, particularly information about individuals. Information about individuals, especially that of consumers, are among businesses' most valuable assets. However, with the increase in businesses' collection and usage of information about individuals has come an increase in the regulatory scrutiny of such business practices, their transparency, and their exposure of individuals to unauthorized access and usage of their personal information.

In recent years, there has been an increasing number of well-publicized stories of breaches of confidential information. Recent studies of data breaches confirm that they present a costly and significant exposure to companies in all lines of business. While paper sources of information are still subject to inadvertent or malicious disclosures, the growth of electronically collected, transmitted and stored information has resulted in more and larger data breaches, and in an associated increase in potential exposures to companies. Most companies are subject both to their own data breaches and to breaches of other entities that collect, maintain or disseminate confidential information on their behalf. While confidential information of all kinds is subject to data breach, attention and regulation remains heavily focused on breaches involving personal information of individuals, particularly electronically stored and transmitted personal information.

There is a growing body of law directed at protecting personal information globally and mandating responses to breaches of personal information, as well as an expansion of regulations and government guidelines directed at increasing security of networks and IT infrastructure generally. Many of these laws and regulations focus on the types of personal information that is often the subject of data breaches and the target of those seeking to engage in identity theft and use such information for fraudulent financial transactions. As collection and storage of personal information and other confidential information increases, and further laws and regulations are issued, the exposures to companies from lost or stolen information are also likely to expand.

Moreover, there is an expanding body of regulations and statutes that govern companies' business practices that involve the collection and use of information about individuals, and the disclosures they are required to make. The challenge of compliance with this growing body of law, and the fines and penalties that can result from violations, is one of the new and expanding exposures that businesses face.

This paper discusses the body of law that governs data security and breach response, the growth of regulatory scrutiny of companies' collection and usage of information about individuals, the types of exposure and liabilities these present, and the lines of insurance potentially affected. We also recognize that businesses' prized assets includes its intellectual property and trade secrets, which are also increasingly the target of cyber attack and theft. Thus, this paper also discusses breaches and cyber attacks involving other categories of confidential information, as well as some of the privacy issues arising out of the increasing use of social media and the development of new technologies.

II. The Types of Information and Practices at Risk

1. Personal Information in the U.S.

Protecting individuals from identity theft has become a significant focus of U.S. state and federal agencies, and of new state and federal laws and regulations.[1] In the pursuit of this goal, efforts have focused on the security of data concerning consumers, including their personal identification numbers, health information, and financial data such as bank account and credit card information.

In the U.S., categories of information about individuals that can be used for identity theft and fraudulent financial transactions are generally referred to as "Personal Information."[2] Laws and regulations vary from state to state, and between state and federal law, as to exactly what information comprises "Personal Information." Generally, in state statutes setting for breach notification and data security requirements, the definition requires both a name (first initial and last name often suffices), and some additional item of information that could be used to steal a person's identity or access his or her financial accounts (or, in some cases, healthcare information) without authorization. Thus, with some variations in content and nomenclature, the general definition of Personal Information is as follows:

An individual's name plus one or more of the following:

Social Security number;
Driver's license or government issued identification card number;
Credit card or other financial account number;

or, depending on the law or regulation triggered:

Other government identification information that could be used for identity theft; or

---

[1] As defined in the Federal Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), "identify theft" is a fraud committed using the identifying information of another person. 15 U.S.C. 1681a(q)(3).

[2] For purposes of this paper, we refer generally to protected information about an individual as "Personal Information" or "PI." There are differences in the terminology used in statutes and regulations of various jurisdictions, however, such as "personal information" versus "private information" versus "personally identifiable information" or "PII." We note that "personal information" is the term used in the Massachusetts Data Security Regulations, while other statutes use terms such as "personal identifiable information" or "private information." New York Gen. Bus. Law § 899-aa, however, defines "personal information" as "information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person," and defines "private information" as "personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data elements is not encrypted, or is encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; 'private information' does not include publicly available information which is lawfully made available to the general public from federal, state or local government records." *See also* New York State Technology Law §208, applicable to State entities as defined by the statute, and the New York City Administrative Code, Title 10, §10-501, applicable to City agencies, which refers to "personal identifying information" that includes a person's date of birth, mother's maiden name, and other information not included in New York Gen. Bus. Law §899-aa. Breach notification requirements are generally triggered by unauthorized access to or acquisition of "private information," but acquisition of "personal information" that is limited to a name or personal mark unaccompanied by other information such as a Social Security number, driver's license or credit/debit card number may not trigger notification requirements under data protection statutes and regulations. Other states' statutes refer to "personally identifiable information" (PII), *e.g.,* Wisconsin Statutes 19.68.

Password and customer identification numbers that allow access to a financial account without a name.

As regulations directed at protecting Personal Information proliferate, however, the scope of protected information is expanding. The federal Red Flags Rule, discussed below, uses the term "identifying information" to mean any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

(1) Name, Social Security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address or routing code; or

(4) Telecommunications identifying information or access device.[3]

HIPAA, also discussed below, protects "individually identifiable health information," which includes all health information in oral, written, or electronic form that can be identified to a specific individual. Any health information, including demographic information that relates to the past, present, or future physical or mental health or condition of an individual, and with respect to which there is a reasonable basis to believe the information can be used to identify the individual, is protected information under HIPAA.[4]

A data breach involving unauthorized access to Personal Information triggering notification obligations can result from an event as simple as a loss of a laptop that contains personal information of customers or employees.[5] In recent years, publicity has focused on large data breaches that involve sophisticated attacks by wide-ranging criminal rings or politically motivated hackers ("hacktivists") on the databases of companies storing Personal Information of thousands or even millions of individuals. Cyber criminals often target institutions that maintain Personal Information of large numbers of individuals in an effort to achieve large returns from their efforts. Hacktivists may have other motives, such as embarrassment to the company whose data bases are accessed. Publicized data breaches of payment processing companies and retailers in which the credit and debit card information of millions of consumers was obtained by cyber criminals demonstrate the scope of such attacks, and the resultant costs to the targeted company. Costs to

---

[3] Telecommunications identifying information and access device are defined in 18 U.S.C. 1029(e). Telecommunications identifying information means the electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument. Access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

[4] 45 C.F.R. § 160.103.

[5] Three hundred twenty-nine organizations reported 86,455 laptops lost at an average cost of $6.4 million per company, and an overall cost of over $1 billion. Ponemon, *The Billion Dollar Lost Laptop Problem*, Sept. 30, 2010.

victimized companies include the direct costs of assessing and responding to the breach, as well as exposure to third-party claims brought by consumers, employees, and others affected by the breach, and the loss of business and damage to reputation from the publicity following a large breach.[6]

Not all data breaches involving Personal Information actually result in identity theft. As discussed below, however, the mere occurrence of a data breach involving Personal Information can trigger time-sensitive and broad-ranging notification requirements imposed on the entity that sustained the breach, at significant cost to that entity. If the loss or theft of Personal Information does not actually result in identity theft, the company sustaining the breach may be able to avoid or at least minimize common law claims for damages from the individuals whose Personal Information was improperly accessed, but it still must comply with applicable statutory and regulatory obligations triggered by the breach.

a. The Expanding Definitions of Personal Information

What constitutes Personal Information subject to legal protection is evolving, with courts interpreting existing statutes more expansively and legislatures considering new statutes.

In the data breach context, a recent amendment to California's breach notification statutes effective January 1, 2014 extends notification requirements to the breach of California residents' online account credentials -- not limited to credentials that may be used to access a financial account.[7] Other states may soon follow, as they did after California enacted the first U.S. breach notification statute in 2003.[8]

The increase in concern about protecting individuals' information that can be used for identity theft has also led to many companies reporting unauthorized access to information that may not itself be protected Personal Information, but can be used to gain access to such Personal Information, such as in the increasing number of incidents of hackers obtaining customer email addresses. An example of this is the 2011 announcement by Epsilon Data Management LLC[9] that the customer data of many of its more than 2,500 corporate clients was exposed by an unauthorized entry into Epsilon's

---

[6] The typical data breach of Personal Information involves either the inadvertent loss or the criminal theft of data containing Personal Information. However, there is also a theory of data breach referred to as a "voluntary data breach" in which intentional dissemination of information unintentionally results in unauthorized distribution of Personal Information. In late 2009, Netflix, Inc. was sued based on a claim of "voluntary privacy breach" based on the video rental company's purported dissemination to contest participants of data sets containing the rental preferences and ratings of subscribers. Although Netflix encrypted the identities of its subscribers in the data sets, the complaint alleges that researchers were able to crack the encryption and identify individual subscribers. The complaint, filed in the United States District Court for the Northern District of California, pled violations of the Video Privacy Protection Act, which prohibits the disclosure of information identifying a person as having requested or obtained a specific video rental. The parties to the lawsuit reached a confidential settlement in March 2010. As discussed below, increasingly, there are data breaches that involve theft of intellectual property and other confidential information as a result of commercial or political espionage.

[7] Effective January 1, 2014, SB 46 expands the definition of "personal information" in California's breach notification statutes applicable to businesses (Cal. Civ. Code § 1798.82) and government agencies (Cal. Civ. Code § 1798.29) to include "user name or email address, in combination with a password or security question and answer that would permit access to an online account."

[8] Within a few years, most other states adopted breach notice requirements modeled in varying degrees on California's.

[9] Epsilon provides consulting, marketing data, technology and agency services to major retailers. Elinor Mills, *Who is Epsilon and Why Does It Have My Data?*, Apr. 6, 2011, http://news.cnet.com/8301-27080_3-20051038-245.html.

email system. The intruder apparently obtained email addresses and/or customer names. Although email addresses are not generally considered to be Personal Information under most U.S. laws and regulations that trigger notification requirements, Epsilon notified its clients, many of whom sent notifications to their customers regarding the unauthorized entry to Epsilon's database. A major concern was that the hackers could use the email addresses in phishing attacks by sending emails that seemed to come from trusted sources, leading unsuspecting customers to reveal Personal Information that would then be used for identity theft.[10]

There is also an expanding definition of what constitutes Personal Information is the growing number of statute and court decisions directed at protecting consumer privacy, rather than directed at minimizing identity theft.

ZIP codes, for example, are now "personal information" under some states' laws limiting businesses rights to collect or record PI of its customers. In 2011, the California Supreme Court held that businesses' practice of recording customer ZIP Code along with customer names violates a California statute, the Song-Beverly Credit Card Act,[11] which forbids businesses from requesting "personal identification information" during a credit card transaction that is recorded.[12] The California Supreme Court noted that the statute demonstrated legislative intent to prohibit retailers from requesting and recording information about cardholders that are unnecessary to the credit card transaction. The Court held that the word "address" in the statutory definition of personal identification information should be construed to encompass not only a complete address, but also the components of an address. A significant factor in the Court's decision was the ability of retailers to utilize a software program that could identify a customer's full address from the name and ZIP Code and use it for marketing purposes for itself or to sell to others.[13] In March 2013, the Massachusetts Supreme Judicial Court similarly held that ZIP codes are "personal identifying information" under a Massachusetts statute, and may not be collected and recorded as part of a credit card transaction if not required by a credit card company or necessary for the transaction.[14] Other states may follow in the footsteps of California and Massachusetts, although as discussed below courts in some of those jurisdictions have refused to accept such a broad interpretation of what constitutes PI.[15] Moreover, some states' legislatures may soon be considering enacting new

---

[10] "Phishing" is the practice of sending an email that is purportedly from a well-known organization to induce the recipient to reveal information for use in identity theft. The recipient clicks on a link that appears to lead to a legitimate organization's website, but that silently redirects the user to a website that then requests and collects the user's personal information for fraudulent purposes.

[11] Ca. Civ. Code § 1747.08(b).

[12] *Pineda v. Williams Sonoma Stores, Inc.*, 51 Cal. 4th 524 (Ca. 2011).; also available at http://www.courts.ca.gov/opinions/documents/S178241.PDF. *See* Edwards Wildman Palmer LLP Client Advisory, *California Supreme Court's ZIP Code Decision Exposes Retailers to New Litigation Hazard, Statutory Fines*, Apr. 2011, http://www.edwardswildman.com/files/upload/CA_Sup_Ct_ZIP.pdf.

[13] Several other states have statutes restricting retailers' right to collect ZIP Codes of customers that are also the subject of litigation, although they are not yet subject to the interpretation imposed by the California Supreme Court. *See* Massachusetts General Law Ch. 93, §105(a); NJ §56:11-17.

[14] *Tyler v. Michaels Stores, Inc.*, No. SJC-11145, 2013 Mass. LEXIS 40 (Mar. 11, 2013). *See* Edwards Wildman Palmer LLP Client Advisory, *Massachusetts Supreme Judicial Court Expands Consumer Zip Code Privacy Protection in Tyler v. Michaels Stores*, Mar. 2013, http://digilaw.edwardswildman.com/?entry=4652.

[15] *Hancock v. Urban Outfitters, Inc.*, No. 13-939, 2014 WL 988971 (D.D.C. Mar. 14, 2014) (in which a court in the District of Columbia decided not to follow in the footsteps of California and Massachusetts with regard to Zip Code litigation). See Section VII.4. a. on Privacy Litigation below.

laws that would further expand the definition of protected personal information to include, for example, email addresses, as well as other information that identifies a particular individual.[16] There is a continually developing body of case law and statutes that can impact the scope of what is considered Personal Information and the protections afforded it.

Further, recent changes to the Children's Online Privacy Protection Act (COPPA) Rule include an expanded definition of personal information with regard to information collected online from children under 13, which includes persistent identifiers (with some exceptions), geolocation data, photos and audio of children.[17]

The U.S. is gradually shifting toward the broader definitions of Personal Information generally followed in the EU and other countries, and continued expansion of protections to PI afforded by statutes, agency regulations and court decisions can be expected. [18]

b. What is Protected Health Information (PHI)

Often data breaches involve individuals' information that is not what is typically defined as Personal Information under state statutes, but rather is of individuals' health information. This generally occurs when the data breach is of a healthcare or other entity that obtains health information as part of its business. When that information falls within the scope of "Protected Health Information" ("PHI"), it is subject to additional statutory and regulatory oversight and breach response requirements.[19]

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") defines PHI as "individually identifiable health information" that is held or transmitted by a HIPAA-subject entity (*e.g.*, a physician, hospital, health insurer, or business associate) and relates to:

- the individual's past, present or future physical or mental health or condition;
- the provision of health care to the individual; or
- the past, present, or future payment for the provision of health care to the individual;

and that identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

---

[16] See, *e.g.*, California Assembly Bill 1291 which, if enacted in its current form, would amend existing California Civil Code §1798.83 to broadly expand the definition of "personal information" and the requirements for disclosure upon customer request of the information and with whom it was shared.

[17] 16 CFR Part 312, http://www.ftc.gov/policy/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-proposed

[18] See section below on the International Regulatory and Statutory Landscape.

[19] The pertinent statutes are discussed below, in the sections discussing HIPAA, the HITECH Act, and the Health Breach Notification Rule.

Name, birth date, address, and Social Security number are typical examples of "individually identifiable health information" when paired with information relating to the health of that individual, such as a diagnosis, treatment plan, or payment for medical services.

2. Personal Information in the E.U. and UK

The E.U. and countries in the E.U. have a much more expansive view of what constitutes Personal Information, (or "personal data" under the terms of the applicable law) under which generally any data that relates to an individual who can be identified from the data or other information with the data is PI. In the E.U., under the Data Protection Direction (95/46/EC) "personal data" means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person being one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The definition is deliberately broad. The Draft General Data Protection Regulation will see this definition rendered even broader, where personal data will mean "any information relating to a data subject".

In the UK, the primary and overarching definition of personal data is taken from the UK Data Protection Act 1998, which provides that personal data means data which relate to a living individual who can be identified (a) from those data; or (b) from those data and other information in the (or likely to come into the) possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual. That statutory definition above has been supplemented by UK case law. English courts have said personal data also had to have an element of "biographical significance" or "focus" on the individual in question, so that the incidental inclusion of a person's name, for example, in a report that was otherwise not focused upon that person may not necessarily constitute personal data.[20] Recently, UK case law has added further clarification to the definition by explaining that context counts; for example, a name would always be personal data where the context in which it appeared was such that a particular individual could be identified from it.

In 2013, the High Court confirmed the ICO's approach in a decision addressing the nature of personal data in the context of the Freedom of Information Act 2000 (FOIA). [21] , the court held that prior leading case law on the meaning of personal data [22]was limited to a particular factual scenario and is therefore only one of a number of tests that may be applied in determining whether information is personal data. The court found the Article 29 Working Party's Opinion and the ICO's Technical Guidance Note (TGN) must also be considered when determining if information constitutes personal data. In 2014, the Court of Appeal followed suit.[23] In particular, the court found that a First-tier tribunal (determining whether the names of FSA employees were personal data) had been wrong solely to follow the approach taken in previous case law. Instead, the court specifically referred to the TGN.

---

[20] *Durant v Financial Services Authority* [2003], EWCA (Civ) 1746.

[21] *R (Kelway) v The Upper Tribunal* (Administrative Appeals Chamber) and *Northumbria Police and R (Kelway) v Independent Police Complaints Commission* [2013] EWHC (Admin) 2575.

[22] *Durant v Financial Services Authority* [2003], *supra*.

[23] *Edem v The Information Commissioner & Anor* [2014] EWCA (Civ) 92.

The UK regulator (Information Commissioners Office or ICO) has also issued guidance on the definition of personal data which, although not binding, the courts are obliged to consider where applicable.[24] (See Section on EU and UK Regulatory and Statutory Landscape, below.)

3. Breaches of Data Other Than Personal Information

This paper focuses largely on data breaches involving Personal Information, but a data breach can also involve other confidential information, the access to and dissemination of which may cause substantial damages and give rise to legal liability. A data breach can be the result of deliberate criminal activity, or of accidental devise loss. However, regardless, of motive, when the subject is Personal Information, the breach often triggers required statutory responses, as discussed below.

Cyber attacks, especially when they are directed at networks, can also be conducted with the goal of disrupting operations rather than accessing Personal Information, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.[25] There are also increasing reports of attacks whose motive is to obtain confidential business information for commercial or political advantage, in what has been called "cyber espionage." These other types of cyber attacks and breaches are discussed below, as the potential exposures they present are significant, and they are generating increasing attention from both those seeking to affect such attacks and those seeking to protect against them.

a. Secrets of All Sorts

Data required to be kept confidential is not limited to Personal Information, and financial gain through identity theft is not the only goal of hackers.

Confidential data includes trade secrets, intellectual property, proprietary information (*e.g.*, techniques, plans, processes, financial data, and similar business secrets) and other confidential information that owners and keepers of such information want to keep secret, and that others may seek to obtain for their own benefit or to harm others.

Significantly, recent studies report that confidential business information is increasingly being targeted by hackers, in recognition that trade secrets, company information about upcoming projects and bids, and similar "corporate intellectual capital" can be a source of financial gain and competitive advantage through unauthorized use or sale to others.[26] Customer and consumer documents are at risk, and in one study 90% of respondents reported that they are certain or believe

---

[24] http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/determining_what_is_personal_data_quick_reference_guide

[25] A DoS attack is generally one in which an attacker "floods" a targeted network with requests so that it can't be accessed. A DDoS attack is one in which the attacker is using multiple computer to launch the DoS attack. *See, e.g., Understanding Denial-of-Service Attacks*, www.us-cert.gov/ncas/tips/ST04-015.

[26] McAfee and Science Applications International Corporation, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, Mar. 28, 2011.

it very likely that their organization experienced leakage or loss of sensitive or confidential documents during the prior year.[27]

Data breaches involving confidential data that is not within the applicable statutory definitions of Personal Information do not trigger the protection and notification obligations of the large body of state and federal laws directed at protecting against identity theft. They can, however, result in business losses to the breached company, as well as in liability claims by third parties against the targeted company if they cause damage to others, such as the company's clients.

Proprietary intellectual property has become a prime target for hackers, both private and purportedly foreign government sponsored. Proprietary information is considered twice as valuable as day-to-day financial and customer data.[28] As a result, security experts and law enforcement officials report that a thriving criminal market has evolved for converting stolen trade secrets into cash.[29] Cyber espionage reportedly cost U.S.-owned business about $14 billion in economic losses in just a six-month period.[30]

b. Cyber Spies and Hacktivism

In addition to commercially motivated criminal hackers, there are reports of cyber espionage risks from sophisticated industrial spies and nations. At times, the attacks may be politically motivated and committed by what have become known as "hacktivists" (activist hackers), rather than economically motivated, but the goal is still generally the theft of information with resultant loss of valuable assets to the company attacked.

While the politically motivated activities of hacktivists are a form of cyber spying, recently there has been increasing focus on cyber spying on a wide range of industries from foreign sources seeking economic gain, trade secrets, and potentially advantages for use in hostilities.[31]

Definitive proof of foreign government sponsorship of cyber spying tracked to foreign sources has been elusive, although a February 2013 report known as the "Mandiant Report" tried to close that gap and provide objective evidence tying in cyber spying to the government of mainland China. The Mandiant Report concluded that the cyber espionage unit under investigation is "likely

---

27 See, *e.g.*, Ponemon Institute, LLC, *2012 Confidential Documents at Risk Study*, July 2012.

28 Byron Acohido, *Social-media tools used to target corporate secrets*, USA Today, Mar. 31, 2011, http://usatoday30.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm (citing both Forrester Research and Simon Hunt, Chief Technology Officer of McAfee's Endpoint Security Division).

29 *Id*.

30 *Industrial Cyber Attacks, A Costly Game*, Advisen, Apr. 20, 2012 (referring to an FBI report of losses between Oct. 2011 and Apr. 2012).

31 Recent attempts by foreign nations or foreign state-sponsored actors to steal proprietary information from U.S. companies for economic exploitation has gravely concerned U.S. military planners: "The immediate worry for military planners . . . is the growing number of small scale attacks that occur daily on U.S. Companies." *Pentagon investing in cyber to stop growing attacks: Pentagon hikes cyber spending*, Advisen, June 27, 2013, http://cyberfpn.advisen.com/fpnHomepagep.shtml?resource_id=2016334881094819870&userEmail=lkamaiko@edwardswildman.com#top.

government-sponsored and one of the most persistent of China's cyber threat actors," and that it receives direct government support.[32]

Whether the information provided in the Mandiant Report and subsequent investigations will prove sufficient evidence in a court case to establish that a particular attack or installation of spyware was government-sponsored remains to be fully tested. China's premier had issued statements disputing the Mandiant Report's assertions that China's military is behind many massive cyber attacks on U.S. entities.[33] However, in May 2014, the U.S. Justice Department considered the information of Chinese cyber spying sufficient to unseal its indictment of five members of the Chinese People's Liberation Army and charge them with hacking into the networks of major U.S. companies such as Westinghouse Electric, the United States Steel Corporation, U.S. subsidiaries of SolarWord AG, Allegheny Technologies and Alcoa.[34]

The U.S. has also been the target of charges of cyber spying, particularly in light of the National Security Agency (NSA)[35] conduct revealed by Edwards Snowden, starting in early June 2013. The Snowden revelations caused many countries (as well as many inside the U.S.) to point to the U.S. as a major source of government sponsored cyber spying. [36]

Information reported about cyber spying also has revealed the methodologies used for cyber spying as well as their content, ranging from collection of information about individuals from the apps they use on smart phones, to phishing scams to gain access.[37]

The scope of the problem has been identified and discussed in reports by private entities, such as the Mandiant Report, and was also highlighted in government reports such as the October 2011 report from the Office of the National Counterintelligence Executive ("ONCIX") that found that U.S. businesses are prime targets of foreign economic and industrial espionage, as other countries seek to build up their domestic industries with stolen technology and intellectual property from more advanced U.S. firms. The report specifically identified China and Russia as "aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyber

---

[32] Mandiant, *APT1: Exposing One of China's Espionage Units*, Feb. 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. *See* David E. Sanger, David Barboza and Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, The New York Times, Feb. 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all.

[33] *See, e.g.*, Associated Press, *China's new premier rejects U.S. hacking claims*, Yahoo! News, Mar. 17, 2013, http://news.yahoo.com/chinas-premier-rejects-us-hacking-claims-100525298--finance.html.

[34] *See*, Michael S. Schmidt and David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, The New York Times, May 19, 2014; Pete Williams, *U.S. Charges China with cyber-spying on American Firms*, www.cnbc.com, 19 May 2014; Edward Wong, *U.S. Case Offers Glimpse Into Chinas Hacker Army*, The New York Times, May 22, 2014.

[35] The NSA is a U.S. intelligence agency created by Executive Order 13470 in 2008, to collect intelligence to detect and counter espionage and other threats and activities directed by foreign powers or their intelligence services against the U.S. and interests.

[36] *See* Ellen Nakashima, *From obscurity to notoriety, Snowden took an unusual path*, Washington Post, June 9, 2013; Katherine Jacobsen and Elizabeth Barber, *NSA Revelations: A timeline of what's come out since Snowden leaks began*, The Christian Science Monitor, October 16, 2013; David E. Sanger and Nicole Perlroth, *N.S.A. Breached Chinese Servers Seen as Security Threat*, The New York Times, March 22, 2014.

[37] *Spy Agencies Scour Mobile Phone Apps for Personal Data, Documents Say*, The New York Times, January 27, 2014; Danny Yadron, *Alleged Chinese Hacking: Alcoa Breach Relied on Simple Phishing Scam*, Wall Street Journal, May 19, 2014.

space."[38] The leading areas of theft were reported to be key components of the U.S. economy: information technology, military technology, and clean-energy and medical technology.[39] U.S. defense officials report that more than 100 countries have tried to break into U.S. networks.[40] Networks of at least 760 companies, research universities, Internet service providers and government agencies were reportedly the target of China-based cyber spies in the last decade.[41]

Government agencies and contractors are also targets. Companies and agencies comprising the U.S. Military Industrial Complex are a target of cyber attacks aimed at access to confidential information other than Personal Information, and perhaps at business disruption.[42] An early indication of this was the reports that the Defense Department detected 360 million attempts to penetrate its networks in 2008, up from six million in 2006. In the Spring of 2008, there was reportedly a breach of one of the Pentagon's Joint Strike Fighters weapons programs.[43] Reportedly similar incidents resulted in the breach of the Air Force's air-traffic control system.[44] One report of a U.S. Department of Defense breach identifies a vulnerability faced by all companies: thumb drives.[45] Recent statements of government officials confirm that the attempted attacks continue: In March 2012, Defense Secretary Panetta reportedly stated, "we are literally getting hundreds or thousands of attacks every day that try to exploit information in various [U.S.] agencies . . . ."[46]

Private companies involved in development of products for the Defense Department are also targets, with resultant costs including contractual penalties, business interruption and reputational damage. This was demonstrated by the May 2011 cyber attack on Lockheed Martin, a major defense contractor holding sensitive information (although the company reported its secrets remained safe). This attack reportedly may be tied to an earlier hacking attack on the RSA security division of EMC Corporation that reportedly may have comprised security products RSA supplied to companies in the military industry and to other large corporations.[47] The Defense Department has admitted that 24,000 Pentagon files were stolen from a defense contractor around March 2011, and the Pentagon acknowledged that the U.S. military had suffered a major cyber attack in 2008

---

[38] ONCIX, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace – Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Oct. 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[39] *Id.*

[40] Siobhan Gorman and Stephen Fidler, *Cyber Attacks Test Pentagon, Allies and Foes*, The Wall Street Journal, Sept. 25, 2010, http://online.wsj.com/news/articles/SB10001424052748703793804575511961264943300.

[41] Michael Riley and John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, Bloomberg, Dec. 14, 2011, http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html.

[42] See Mandiant Report, *supra*.

[43] S. Gorman and Y. J. Dreazon, *Obama Set to Create 'Cyber Czar' Position,* The Wall Street Journal, May 29, 2009, page A4.

[44] S. Gorman, A. Cole, Y. Dreazen, *Computer Spies Breach Fighter-Jet Project*, The Wall Street Journal, Apr. 21, 2009, page A1.

[45] Deloitte, *The Sixth Annual Global Security Survey* at p. 32 (reporting media speculation that "a recent worm attack, acknowledged by the U.S. Department of Defense (DoD) may have been linked to thumb drives after the DoD subsequently banned them").

[46] Trent Nouveau, *Cyber-attack spectre troubles Pentagon*, TG Daily, Mar. 5, 2012.

[47] Christopher Drew and John Markoff, *Data Breach at Security Firm Linked to Attack on Lockheed*, The New York Times, May 27, 2011.

after malicious code was placed on a flash drive inserted into a U.S. military laptop, with the code spread on both classified and unclassified systems.[48]

Think tanks have also been targeted. In December 2011, Stratfor, a security think tank, was targeted by the hacking group Anonymous (sometimes referred to as "hacktivists"). Confidential customer information was reportedly accessed, as well as individuals' credit card numbers which Anonymous reportedly used to make "donations" to charities.[49] The attack demonstrates that financial gain need not be the focus of a cyber attack for Personal Information to be involved, as well as demonstrating the challenges for even sophisticated security entities to secure their systems against cyber attacks.

The energy industry also has been a frequent target, with cyber attacks reportedly conducted against private and state-owned oil, energy and petrochemical companies, targeting confidential and proprietary information such as project financing bids and exploration plans for oil and gas field operations:

> One series of such attacks has been dubbed "Night Dragon" and identified as originating primarily in China.[50]
>
> > In May 2012, Iran claimed that cyber attacks had caused the loss of data at its Oil Ministry and its main oil export terminal. The forensic examination which followed revealed a malware known as Flame, which is the most sophisticated espionage program known to exist. It can activate computer microphones and cameras, log keyboard strokes, take screenshots, and turn an infected computer into a beacon that can intercept and transmit Bluetooth data.[51]
> >
> > The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") published a notice in April 2012 concerning an ongoing series of cyber intrusions directed at U.S. gas pipelines. It said that since December 2011, there have been targeted spear-phishing[52] exploits aimed at

---

48 Jason Ukman, Ellen Nakashima, *24,000 Pentagon files stolen in major cyber breach, official says,* The Washington Post, Jul. 14, 2011.

49 *See, e.g.*, Sean Ludwig, 10 *things you need to know about Anonymous' Stratfor hack,* Venture Beat, Dec. 28, 2011; Olivia Katrandjian, *Hacking Group 'Anonymous',* ABC World News, Dec. 26, 2011.

50 McAfee, *Global Energy Cyberattacks: "Night Dragon*", Feb. 10, 2011, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

51 Ellen Nakashima, Greg Miller and Julie Tate, *U.S., Israel Develop Flame computer virus to slow Iranian nuclear efforts, officials say*, The Washington Post, Jun. 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

52 "Spear-phishing" is an email fraud (phishing) attempt that targets a specific organization or person, seeking unauthorized access to confidential data. Email messages, sent from what appears to be a trusted source, ask the recipients for information or to click on links that ask them for information or install malware on their computers.

> employees of natural gas pipeline companies. It is not clear whether the intrusions were designed simply to map the gas systems, damage the pipelines, or both.[53]

These attacks can have substantial financial impacts on their targets, including the loss to the breached entity of its own information, business disruption, and potential contractual breaches and resulting claims by third parties. Such cyber attacks on government facilities and critical infrastructure industries raise for all countries in which they occur complex issues of national security, public policy and the appropriate degree of cooperation between government and private sectors.

Moreover, politically motivated attacks can trigger a more traditional data breach of Personal Information. For example, hacktivist searches for information targeting company executives with the goal of embarrassing them can also result in access to executive PI, or that of others in the targeted company. These attacks can potentially trigger company obligations under breach notification statutes or result in companies sending voluntary warnings to those who are perceived as hacktivist targets. While breach notification statutes are not always triggered, the U.S. Department of Justice and other law enforcement agencies have used other statutes, with varying success, to try to hold hacktivists accountable when they can be identified. [54]

c. Cyber Attacks with Physical Effects or Business Disruption as Focus

During the last few years, another type of cyber risk has become increasingly prominent: cyber attacks that are directed not at illicit acquisition of information, but rather at causing significant physical effects or business disruption, including destruction or disruption of computer control systems, and the industrial systems and equipment on which industrial entities and public utilities depend. Other times, attacks seeking information rather than disruption, either deliberately or unintentionally, also cause disruption of the targeted entity's operations, with resultant costs and business consequences.

A major concern has long been the targeting of critical infrastructure such as utilities and transportation by state-sponsored cyber attacks. Recently, however, financial institutions became the focus of what appears to be hacktivism with resulting disruption of business operations in what is generally referred to as "denial of service" ("DoS") or "distributed denial of service" ("DDoS") attacks.[55] Both U.S. and South Korean banks were targeted in March 2013, followed by an attack

---

[53] Darren Goode and Jennifer Martinez, *Risk of cyberattacks clouds natural gas boom*, PoliticoPro, May 8, 2012, http://www.politico.com/news/stories/0512/76060.html; Michael Winter, *Natural gas pipelines under cyber attack since December*, USA Today, May 7, 2012, http://content.usatoday.com/communities/ondeadline/post/2012/05/natural-gas-pipelines-under-cyber-attack-since-december/1.

[54] *See* Allison Grande, *Reuters Hack Attack Will Push Cos. To Firm Up Firewalls*, Law 360, Mar. 15, 2013, http://www.law360.com/articles/424273/reuters-hack-attack-will-push-cos-to-firm-up-firewalls (noting that the U. S. Department of Justice filed an indictment in California federal court charging former Reuters Deputy Social Director with helping hacking group Anonymous break into the Los Angeles Times' website, utilizing the Computer Fraud and Abuse Act as well as a general conspiracy statute U.S.C. Section 371). See stories of May 2014 indictments, Schmidt and Sanger, *5 in China Army Face U.S. Charges of Cyberattacks, supra*

[55] A denial of service attack is an attempt to make a machine or network unavailable to its intended users. In a large-scale attack, the attacker often attempts to overwhelm a site with so many requests for attention that the site is unable to respond to legitimate requests and becomes unresponsive. *See, e.g.*, Arik Hesseldahl, *Denial of Service Attacks Are Getting Bigger and Badder*, Apr. 17, 2013, http://allthingsd.com/20130417/denial-of-service-attacks-are-getting-bigger-and-badder/.

on American Express's website, which went offline for a couple of hours.[56] Financial institutions have been quick to adopt effective defenses against DoS and DDos attacks. In late 2013, several banks, including Regions Bank and JPMorgan Chase, successfully defended themselves against a fourth round of cyber attacks by the Al Qassam Cyber Fighters.[57]

Reportedly, the number of attacks reported to a U.S. Department of Homeland Security cyber security response team grew by 53% in 2012—the agency received notice of 198 attacks, several of which successfully infiltrated defenses.[58]

The potential vulnerability of U.S. infrastructure has been a growing concern in recent years. As the then U.S. Deputy Secretary of Defense put it on September 28, 2011:

> In a development of extraordinary importance, cyber technologies now exist that are capable of destroying critical networks, causing physical damage, or altering the performance of key systems. In the twenty-first century, bits and bytes are as threatening as bullets and bombs.[59]

In March of 2014, Leon Panetta, the former U.S. Secretary of Defense, further cautioned that a possible "cyber Pearl Harbor" may loom on the horizon.[60] According to Panetta, a cyber attack which could "devastate our critical infrastructure and paralyze our nation" is the "the most serious threat [to the United States] in the 21st century."[61] Panetta characterized the ramifications of a focused cyber attack on the nation's infrastructure as being comparable in scope to the damage that Hurricane Sandy inflicted on the East Coast in 2012.[62] Emphasizing the necessity of public awareness on this issue, Panetta stressed, "The American people need to understand that [] this is not about hacking and identity theft, it has the potential for a major attack on the United States."[63]

A key breakthrough was the 2010 discovery that the Stuxnet worm had successfully disrupted the logic control system for the centrifuges that Iran uses to enrich uranium, making about 1,000 of

---

[56] *See* Nicole Perlroth and David E. Sanger, *Cyberattacks Seem Meant to Destroy, Not Just Disrupt*, The New York Times, Mar. 28, 2013, http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html?pagewanted=all; *see also* Sean Gallagher, *"Funded hacktivism" or cyber-terrorists, AmEx attackers have big bankroll*, Mar. 30, 2013, http://arstechnica.com/security/2013/03/funded-hacktivism-or-cyber-terrorists-amex-attackers-have-big-bankroll/.

[57] *Banks' Improved Security Defenses Disarm Cyber Attackers [Payments Source (Online)]*, Advisen, Aug. 5, 2013, http://cyberfpn.advisen.com/?resource_id=20361138310693726 69#top.

[58] David Goldman, *Hacker hits on U.S. power and nuclear targets spiked in 2012*, CNN Money, Jan. 9, 2013, http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html. *See* ICS-CERT Monitor reports published quarterly by the Industrial Control Systems Cyber Emergency Response Team of the U.S. Department of Homeland Security.

[59] William J. Lynn III, *The Pentagon's Cyberstrategy, One Year Later*, Foreign Affairs, Sept. 28, 2011, http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.

[60] Patrick Thibodeau, *Cyberattacks could paralyze U.S., former defense chief warns*, Computerworld, Mar. 11, 2014, http://www.computerworld.com/s/article/9246886/Cyberattacks_could_paralyze_U.S._former_defense_chief_warns.

[61] *Id.*

[62] *Id.*

[63] *Id.*

them unusable.[64] According to reports, the Iranian control system was not connected to the Internet, so it is believed that the Stuxnet virus was transmitted by a USB stick that an unknowing person plugged into an otherwise secure computer. The malware Flame has commonalities with Stuxnet. Initially, Flame was thought to be a tool for espionage only, but after study, researchers have concluded that it has the capacity to completely delete files from computers, which means it can disable operating systems. So it can be used not only for espionage, but also to attack utilities and other critical infrastructure systems.[65]

A high level of expertise was needed to develop Stuxnet and Flame. Unfortunately, once a code is used and discovered, it does not take as high a level of expertise to replicate it. Replicas can be modified to target other industrial control systems.[66] One researcher has reported that he created his own version of Stuxnet in less than three weeks of work, spending less than $10,000 to replicate his target hardware environment.[67]

Actual attacks, or at least intrusions, have been reported although of relatively modest effect so far in the U.S.[68] However, tests conducted by the U.S. Department of Homeland Security demonstrate that cyber terrorists have the capability of disrupting, or even destroying, utilities such as electrical generation and transmission facilities, water treatment facilities, and facilities of the fossil fuel industry.[69] Such attacks may result from what the industry refers to as an Advanced Persistent Threat – that is, a group, such as a foreign government, with both the capability and the intent of targeting a specific entity with a cyber attack.[70]

In the spring of 2009, cyber spies reportedly penetrated the nation's electrical grid.[71] This incident highlighted that utility companies are a target, with resultant effect on those they service. The consequences of the East Coast blackout of 2004 demonstrated the effect and scope of potential business interruption and related losses that can be incurred as a result of a utility failure. As the blackout demonstrated, businesses dependent on refrigeration are especially vulnerable to large losses resulting from electrical failures with resultant first-party and third-party claims.

---

64 Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, Wired, Jul. 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/; Ian Bremmer and Parag Khanna, *Cyberteeth Bared*, The New York Times, Dec. 22, 2010, http://www.nytimes.com/2010/12/23/opinion/23iht-edbremmer23.html?_r=0.

65 Jim Finkle, *Flame can sabotage computers, attack Iran: expert*, Chicago Tribune, Jun. 21, 2012, http://articles.chicagotribune.com/2012-06-21/business/sns-rt-us-cyberwar-flamebre85k1u0-20120621_1_hungary-s-laboratory-stuxnet-and-flame-western-national-security-officials.

66 Kim Zetter, *DHS Fears a Modified Stuxnet Could Attack U.S. Infrastructure*, Wired, Jul. 26, 2011, http://www.wired.com/threatlevel/2011/07/dhs-fears-stuxnet-attacks.

67 Mathew J. Schwartz, *Next DIY Stuxnet Attack Should Worry Utilities*, Information Week, Nov. 22, 2011, http://www.informationweek.com/traffic-management/next-diy-stuxnet-attack-should-worry-utilities/d/d-id/1101494?.

68 *See, e.g., DDoS Attacks Spread Beyond Banking: U. S. Utility Suffers Outage as Bank Strikes Continue*, Bank InfoSecurity, Mar. 12, 2013, http://www.bankinfosecurity.com/ddos-attacks-spread-beyond-banking-a-5596/op-1 (reporting on March 7, 2013 announcement by a DDoS protection provider that it had worked with an unidentified metropolitan utility company to mitigate an attack in mid-February that took their online payment platforms offline for two days).

69 *See, e.g.*, Phil Windley, *Blowing up generators remotely*, Sept. 28, 2007, http://www.zdnet.com/blog/btl/blowing-up-generators-remotely/6451.

70 *See Under Cyberthreat: Defense Contractors*, Bloomberg Businessweek, Jul. 9, 2009.

71 S. Gorman, *Electricity Grid in U.S. Penetrated by Spies*, The Wall Street Journal, Apr. 8, 2009, page A1.

In February 2011 it was reported that Chinese hackers had infiltrated the computer systems of five multinational oil and gas companies, in an attack dubbed "Night Dragon." Security researchers stated that the purpose of the attack appeared to be corporate espionage, as the focus appeared to be on oil and gas field production systems as well as financial documents.[72]

In April 2012, the Department of Homeland Security reported that the U.S.'s water and energy utilities face constant cyber-espionage and denial-of-service attacks against industrial-control systems.[73]

In July 2012, the head of the U.S. National Security Agency stated that there has been a 17-fold increase in attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations.[74]

As noted by the Mandiant Report exposing China's Espionage Units, a major target for such state-sponsored espionage are victims whose compromised systems allow access to infrastructure.[75] Similarly, there have been reports of state-sponsored attacks on U.S. energy companies, as well as other U.S. companies, emanating from the Middle East.[76]

Whether the aim is to steal secrets or to disrupt facilities, utilities are likely remain a target for cyber criminals.[77] Targeting of critical infrastructure remains a serious concern, and was the basis for an Executive Order issued by President Obama in February 2013, announcing that a system would be established for dissemination of information in a voluntary information-sharing program between private and public sector, as well as for the establishment of procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors.[78]

Cyber attacks with physical effects can have substantial financial impact on their targets, including property damage, business interruption and contractual breaches, as well as general third-party claims should the disruption of the target's operations in turn affect its customers and vendors.[79]

Moreover, the increase in cyber attacks and the growing evidence that many are likely state-sponsored, and that cyber attack capabilities are increasingly part of the defense plans of many countries, has led to debates in both government and private sectors as to when a cyber attack becomes cyber warfare. An example of the debate is set forth in a report by independent legal

---

[72] John Markoff, *Hackers Breach Tech Systems of Oil Companies*, The New York Times, Feb. 10, 2011.

[73] Ellen Messmer, *DHS: America's power utilities under daily cyber attack,* Network World, Apr. 4, 2012.

[74] David E. Sanger and Eric Schmitt, *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure*, New York Times, Jul. 26, 2012.

[75] The Mandiant Report, *supra.* See section above on cyber spying.

[76] David E. Sanger and Nicole Perlroth, *Cyberattacks Against U.S. Corporations Are on the Rise*, The New York Times, May 12, 2013.

[77] *See* section above: "Cyber Attacks with Physical Effects or Business Disruption as Focus."

[78] Executive Order, Improving Critical Infrastructure Cybersecurity, Feb. 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[79] Some of these types of incidents may generate claims under different types of insurance coverages than are typically involved in breaches involving Personal Information, depending on the nature of the breach, the damages, the claim, and the type of policy and its terms and exclusions. *See* section on "Potential Insurance Coverage for Data Breaches," *infra*.

experts that recently declared that Stuxnet was an "act of force" under international law. However, expert opinions differed as to whether Stuxnet constituted an "armed attack" that would justify the use of counterforce in self-defense, and trigger the start of international hostilities under the Geneva Convention's laws of war. Simply put, the question of whether certain cyber attacks are acts of warfare is one that will likely be addressed in the not-so-distant future.[80]

Other countries have also been focusing on this increasing risk. International cooperation in identifying and preventing such attacks, and in identifying and stopping the attackers, is increasingly a focus of international forums on cyber security.[81]

4. The Scope of What Constitutes a "Data Breach": Not Just Electronic – Paper Too

Data breach is often thought of only as a cyber risk: a risk associated with electronic processes used for conducting business through computer networks. Most of the attention in the past few years has been on electronic data breaches, particularly on instances of cyber criminals gaining unauthorized access to electronic data maintained by financial institutions, data processors and retailers, and on reports of lost laptops containing confidential information. Often, stories focus on the increasing technical sophistication of cyber criminals (including how thieves can use portable technology to scan credit card information from a card still in the unsuspecting victim's purse or wallet).[82] Many data breaches still happen the old-fashioned way, however, through the improper safeguarding or disposal of paper records. Apparently, "dumpster diving" is still a common way for some to obtain Personal Information and other confidential information for illicit use.

Moreover, many data protection laws and regulations directed at protecting Personal Information are not limited to electronic data, but also require protection and proper disposal of paper records containing Personal Information. Most U.S. data breach notification requirements, however, apply to breaches involving data in electronic format, and do not extend to Personal Information contained in paper documents. In contrast, breaches involving Protected Health Information in any format, including paper photographs or audio recordings can trigger response obligations that are based on the content of the information and not tied to format.

Data breaches regularly result from the improper disposal of paper records. This was demonstrated several years ago when a newspaper reporter found a law firm's old client files in a dumpster in downtown New York City. The files pertained to personal injury lawsuits, and included names and medical information of individuals as well as Social Security numbers and other personal details.

---

[80] Kim Zetter, *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*, Wired, Mar. 25, 2013, http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/. *See* Scott Shane, *Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials*, The New York Times, Sept. 26, 2012, http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all; Elizabeth Bumiller and Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, The New York Times, Oct. 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

[81] *See, e.g.*, Security & Defence Agenda, *International cooperation on cyber-security*, May 10, 2012, http://www.securitydefenceagenda.org/Contentnavigation/Activities/Activitiesoverview/tabid/1292/EventType/EventView/EventId/1119/EventDateID/1125/Internationalcooperationoncybersecurity.aspx

[82] *Electronic Pickpocketing Target Credit Cards With Radio Chip*, News On 6, Dec. 14, 2010, http://www.newson6.com/Global/story.asp?S=13672878.

Reportedly, in preparation for an office move, the law firm had hired a disposal company, but that vendor improperly dumped the records rather than shredding them. This incident and many others involving improper disposal of paper records containing Personal Information demonstrate that the improper disposal of paper files still presents a substantial exposure, and that holders of such documents need to be attentive to their disposal. This includes ascertaining the security practices of any entities to which a company delegates disposal of its records.

Moreover, people still leave paper files on trains and wherever they stop off on the way home, including files with Protected Health Information of individuals. If the person leaving the files worked for an entity subject to the rules governing reporting of breaches of PHI, that loss of paper records can be a data breach requiring mandatory reporting, as discussed below in Section III.2 discussing HIPAA, the HITECH Act, and other federal statutes and regulations governing PHI.

5. Privacy and Data Breach Concerns in Cloud Computing

As technology develops, so do new exposures, and at times they can outpace even the new regulatory requirements. Recently, there has been increasing attention on "cloud computing" and the challenges it presents to those providing it and utilizing it, on assessing its risks as well as its benefits, and in identifying and complying with applicable security standards and laws.[83]

Cloud computing in its most general sense is the practice of sharing information and services on remote servers, rather than on local ones. Often those remote servers are owned and operated by others, who may rent space and usage to a number of other customers, so resources are shared.

The definition of what the "cloud" is may never be agreed upon. Many argue that the cloud is no different from the Internet. Others, however, contend that the cloud represents one of the most important changes in enterprise computing since the invention of the computer itself. Proponents of this view note that there has been a radical change in the way service providers market their IT capabilities to end users; it is now rare to see an IT service offering that doesn't mention the cloud. Regardless of the difference in views, most agree that the cloud presents an opportunity for enterprises to outsource their computing capability to a third party, with the result that servers, storage, applications and services can now be located in multiple jurisdictions, with further growth in use anticipated.

a. In the United States

Although some dispute whether the concept is new, cloud computing is increasingly being used by businesses, government and individuals. In fact, on November 1, 2011, the U.S. Commerce Department's National Institute of Standards and Technology ("NIST") released for public comment a draft "roadmap" designed to foster federal agencies' adoption of cloud computing, support the private sector, improve the information available to decision-makers and facilitate the continued development of the cloud computing model.[84] This could prove to be a significant

---

[83] *See, generally*, Renzo Marchini, *Cloud Computing: A Practical Introduction to the Legal Issues*, Nov. 2010.

[84] NIST Releases Draft Cloud Computing Technology Roadmap for Comments, Nov. 1, 2011, http://www.nist.gov/itl/csd/cloud-110111.cfm.

accelerator of adoption of cloud services. Such increased use of cloud computing has raised significant privacy and data breach concerns.

Cloud computing has been defined as having the following essential characteristics:

On-demand self-service	–	a consumer can self-provision;
Broad network access	–	capabilities are widely available over a network through heterogeneous devices, such as phones, computers and tablets;
Resource pooling	–	a provider's computing resources are pooled to serve multiple consumers (customers) using a multi-tenant model;
Rapid elasticity	–	capabilities can be elastically provisioned and released;
Measured service	–	cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).[85]

NIST defines three ways cloud services are offered:

Software as a Service (SaaS) – the consumer uses the provider's applications running on a cloud infrastructure. Online email and customer relationship applications are examples;

Platform as a Service (PaaS) – the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider;

Infrastructure as a Service (IaaS) – the consumer acquires processing, storage, networks, and other fundamental computing resources from the provider and is able to deploy and run arbitrary software, which can include operating systems and applications.[86]

Each layer of services relies on the services below it. So, when a provider provides SaaS, it is also providing the platform and the infrastructure needed to run the software. Thus, in assessing privacy and data breach concerns "in the cloud," it is important to understand which cloud service model is being used. Consumers and providers will have varying ability to easily control privacy and security concerns depending on which model is deployed. Frequently, the customer generally has no control over, or knowledge of, the exact location of the provided resources.

---

[85] *See generally* Peter Mell and Timothy Grance, *Special Publication 800-145 – The NIST Definition of Cloud Computing*, NIST, Sept. 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[86] *Id.*

Examples of cloud computing abound in our personal lives and include platforms in which users can edit and store documents on remote servers. Such services eliminate the need to license desktop software as well as the need to store information on a local computer.

On a larger scale, businesses use cloud computing to address varying demands for computing resources (*e.g.*, high demand for online shopping during the holiday season), to achieve better cash flow by purchasing computing resources incrementally, and to outsource the operation and maintenance of non-core competencies.

Cloud computing potentially presents both security benefits and risks. On one hand, cloud computing service providers focus on providing computer services and therefore may be able to employ advanced and robust security techniques that would be cost-prohibitive for smaller companies to implement on their own. On the other hand, an entity using such resources inherently relinquishes some control over the data it provides to a cloud computing service provider. Because cloud resources are so easily deployed, IT personnel may not be involved in its use. When that happens, non-IT personnel may not have sufficient knowledge and sensitivity to properly use security features offered by a cloud provider. Moreover, unless limited by law or contract, the service provider can generally move the data from one server to another, which could potentially be in different states or different countries and subject to different data protection requirements from those of the location of the parties entering into the contract. This can result in Personal Information stored "in the cloud" being subject to either less protection or more stringent regulations than in the original jurisdiction.

Security of cloud computing continues to be debated, with at least one study reporting that organizations have improved their security practice around cloud use in the last few years.[87]

b. In the E.U. and Globally

Over the last couple of years Europe has increased its focus on cloud computing and several organisations have been set up to encourage its expansion and increased usage at the EU level.

The European Cloud Computing Strategy [88] was, for example, adopted by the European Commission in September 2012. Aimed at "Unleashing the Potential of Cloud Computing in Europe", the strategy outlines actions which hope to deliver a net gain of 2.5 million new European jobs, and an annual boost of €160 billion to the EU's GDP (around 1%), by 2020, all within the cloud arena. Part of this strategy was the creation of the European Cloud Partnership (**ECP**)[89] , which brings together industry and the public sector to work on common procurement requirements for cloud computing in a transparent way. Cloud for Europe[90] is another project, started in June of last year which supports public sector cloud use as collaboration between public authorities and

---

87 Ponemon Institute LLC, *Security of Cloud Computing Users 2013 Study*, Mar. 2013.

88 http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

89 http://ec.europa.eu/digital-agenda/en/european-cloud-partnership

90 http://www.cloudforeurope.eu/

industry and is co-funded by the European Commission under the Framework Programme for Research and Innovation [91].

Concerns over cloud data security in Brussels have, nevertheless grown following the Snowden affair in 2013. The EU's response in respect of cloud is that it wants to regulate the sector even if that makes its use more complicated.[92] Viviane Reding, the European Commission's justice minister, has even gone so far as to say that she wants to see "the development of European clouds" certified to strict new European standards. EU legislators have moved quickly to pull together regulations for cloud security,[93] but businesses and consumer cloud users are calling for more regulations to make changing cloud service providers easier and the ECP is even calling for a certification of cloud providers.[94]

Amendments have been proposed to the current law such as requiring "all transfers of data" from a cloud in the EU to a cloud maintained in the United States or elsewhere to "*be accompanied with a notification to the data subject of such transfer and its legal effects*" and there has even been talk of barring such transfers unless conditions are met [95]. In addition, lawmakers are also proposing to impose guidelines for handling court orders from countries outside the EU [96].

However, there is concern that these changes will isolate the EU and form a sort of "cyber-barrier" which will restrict trade. Anna-Verena Naether, policy manager for DigitalEurope, has said, "*We have to make sure it doesn't lead to a Fortress Europe approach*." [97] Sophia in 't Veld, a Dutch MEP who sponsored one of the cloud computing amendments, expressed concern over the "*market dominance of a few American players*"while the MEP is against building a fence around Europe, she would like to see very clear rules established and more competition coming out of the Euro Zone."

The current EU data protection regime is not well-suited to the wide-spread adoption of cloud computing [98]. The Commission is, however, working on a replacement of the Data Protection Directive. In November of last year the European Parliament released a report on the changes proposed by the Commission [99], in which it uses the cloud arena as justification for legislative

---

91 *Ibid*.

92 *Europe Aims to Regulate the Cloud,* Danny Hakim, NY Times Online, Published October 6, 2013 at: http://www.nytimes.com/2013/10/07/business/international/europe-aims-to-regulate-the-cloud.html?pagewanted=all&_r=0

93 *How to Regulate Cloud Computing,* Mark O'Conor, Patrick van Eecke & Jessica Turner , The Guardian Online, Thursday 28 March 2013 at: http://www.theguardian.com/media-network/media-network-blog/2013/mar/28/regulation-cloud-computing-data-protection

94 *Ibid.*

95 *Ibid.*

96 *Ibid.*

97 *Ibid.*

98 Roger Bickerstaff, Barry Jennings, and Tessa Finlayson, *Cloud computing: an analysis of the key legal and commercial considerations arising in relation to cloud computing and related agreements*, PLC Practice Note, Maintained.

99 European Parliament Report "*on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*", 22 November 2013: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN

change in more ways than one. In particular, it is aiming to "strengthen the global dimension" and an additional Article 43(a) will be added to address the issue raised by access requests by public authorities or courts in third countries to personal data stored and processed in the EU. The idea is that transfer will only be granted by the data protection authority following verification that the transfer complies with the Regulation and this was drafted with particular regard to the growth of cloud computing. Furthermore, a new Recital (5(a)) also recognises the potential of cloud computing to "transform the European economy" provided adequate safety and data protection measures are implemented. There are several further amendments regarding controllers of data which also consider cloud computing. On 12 March 2014, the European Parliament voted in plenary in favour of the European Commission's draft EU Data Protection Regulation (the "Proposed Regulation"). The Justice and Home Affairs ministers of the Council are to meet in June 2014 in order to finalise its position on the data protection reform ahead of entering final negotiations with Parliament and the Commission. However, there is concern that European elections may delay or even disrupt the adoption of the Regulation. For further information on the Proposed Regulation see Section IV.4.

On the plus side, there seems to be little evidence of cloud data breaches over the past few years. While there have of course been a number of high profile data breaches of great concern in the EU, cyber criminals for the most part have kept their activities earthbound [100]. The risk remains prevalent nevertheless, especially considering the type and in particular the volume of data that cloud platforms can hold; a breach could affect hundreds of thousands individuals. For the moment it seems to be a case of "watch this (cyber) space."[101]

6. Privacy and Data Breach Concerns in Social Media

The growth of social media sites presents another set of privacy and data security challenges.[102] "Social media" refers broadly to online applications that allow users to create and exchange different types of content. In addition to social networking sites like Facebook, LinkedIn, Twitter and Google+, the term encompasses video and photo sharing sites such as YouTube and Instagram, and news aggregator sites such as Fark and Feedly.[103]

Facebook itself has seen explosive growth in its user population in recent years, and the site has over 1 billion active users.[104] The aggregation of so much personal information, and the myriad

---

[100] Russ Banham, *Cloud computing data breaches currently few,* , Business Insurance, 1 April 2014 at: http://www.businessinsurance.com/article/99999999/NEWS070101/399999805

[101] For a guidance on cloud computing and data protection, and the risk analysis check list for businesses wishing to use cloud computing see ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 05/2012 on Cloud Computing, adopted July 1st 2012, http://ec.europa.eu/justice/data-protection/index_en.htm.

[102] According to a recent report, 66% of online adults use social networking websites, as compared to 8% in 2005. Joanna Brenner, *Pew Internet: Social Networking (Full Detail)*, Pew Internet & American Life Project, May 31, 2012, http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx.

[103] Online dating websites such as Match.com and EHarmony are similar to social media websites in many ways in the way they aggregate content and allow online communications between their members.

[104] Facebook statistics as of June 2014, http://newsroom.fb.com/company-info/ . Google+, Google's social media site, launched in June 2011 and now has over 250 million users. *See* Jeff Bullas, *Why You Shouldn't Ignore Google+ Anymore*, http://www.jeffbullas.com/2012/06/28/why-you-shouldnt-ignore-google-anymore/; *see also Google +Surpasses Twitter to Become*

uses to which that information is put by various applications, some of them created by third parties, has led to much discussion about privacy settings on such sites.[105] There have been a number of investigations both by reporters and regulatory agencies concerning the usage of personal information by such sites. Even usages that may have altruistic purposes, such as scanning of postings to thwart criminal activity, have raised privacy concerns.[106]

a. Social Media as Target and Source of Data Breaches

The amount of information about individuals maintained on social media sites has made them targets for those that seek information about individuals, for identity theft or other purposes. Moreover, the lack of security maintained by users of their access credentials, and the informality with which information is transmitted, makes social media susceptible to hacking both by those who want to obtain information about individuals and those who use the sites for dissemination of false information.

The dangers of hacking of social media sites and the damage such hacking can cause was demonstrated on April 22, 2013, when the Associated Press's twitter feed was hacked and a tweet of "Breaking: Two Explosions in the White House and Barack Obama is injured" appeared.[107] Within minutes after the tweet, the Dow Jones average dropped more than 128 points during the span of a few seconds, but after the report was found to be a hoax, the stock market recovered.[108] A group of hackers loyal to Syrian President Bashar Assad claimed responsibility for the hoax.[109] Recently a report was issued by a cyber intelligence firm regarding what it described as a campaign by Iranian hackers to use fake persona on social networking site to gain login credentials and other information from officials in the U.S. and other countries. After obtaining "friend" status, the fake personal reportedly would target their victim with spear phishing emails that introduced malware with capabilities for data exfiltration.[110]

Social media is also a target for more traditional style breaches. Social media websites have reportedly been the subject of several hacking attacks in the last couple of years. In 2012, LinkedIn a Russian hacker claimed to have downloaded over six million passwords from Linked In; although

---

Second Largest Social Network, Search Engine Journal (posted by Michelle Stinson Ross on Jan. 30, 2013, reporting on a study released in December 2012).

[105] According to one report, only one-third of Facebook users believe that Facebook's use of their personal information is "somewhat to very acceptable." Donna Tam, *Facebook Less Trusted than Amazon, Google, Survey Says*, CNET News, Jul. 19, 2012, http://news.cnet.com/8301-1023_3-57476288-93/facebook-less-trusted-than-amazon-google-survey-says/.

[106] *See, e.g.*,; Joseph Menn, *Social Networks Scan for Sexual Predators, with Uneven Results*, Reuters, Jul. 12, 2012, http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712; *Facebook In Privacy Breach*, The Wall Street Journal, Oct. 18, 2010. The privacy concerns regarding Facebook are not just in the United States. *See, e.g.*, David Cohen, *Facebook Privacy Battles Heat Up in Ireland*, All Facebook – The Unofficial Facebook Blog, Jul. 31, 2012, http://allfacebook.com/ireland-odpc-europe-versus-facebook_b95960; David Cohen, *Facebook Privacy Policies Challenged by Austrian Law Student*, All Facebook – The Unofficial Facebook Blog, Oct. 26, 2011, http://allfacebook.com/facebook-privacy-policies_b64632.

[107] David Jackson, *AP Twitter feed hacked; no attack at White House*, USA Today, Apr. 23, 2013.

[108] Jackson, *supra.*

[109] Emily Alpert, *Backers of Syrian president claim credit for AP Twitter hack*, Los Angeles Times, Apr. 23, 2013.

[110] Leon spencer, *Social Media Central to Iranian espionage campaign*, Report, ZDNet, May 30, 2014, http://www.zdnet.com/social-media-central-to-iranian-espionage-campaign-report-7000030028.

the passwords were encrypted, hundreds of thousands of them have reportedly been "cracked" and many posted online.[111] About a week and a half after the breach was reported, a lawsuit seeking $5 million in damages was filed by one of the site's users, leading to extensive motion practice on class certification and what constitutes legally cognizable injuries from a data breach.[112] The same week that the LinkedIn breach was reported, it was reported that the online dating website EHarmony was also the target of a hack and 1.5 million passwords were stolen.[113] More recently, in late 2013, hackers reportedly stole usernames and passwords for nearly two million accounts at Facebook, Google, Twitter, Yahoo and others, reportedly as a result of key logging software maliciously installed on a number of computers around the world and sending them to a server controlled by hackers tracked to the Netherlands.[114]

In May, 2014 there was the discovery of the OAuth and the OpenID or "Covert Redirect" security flaws. Basically, these programs allow the "cyber-attackers" to appear to the user as a standard log-in popup, however, they are anything but. When the user logs-in, all of the information is provided to the hacker, not to the intended website. Among the sites these fake log-in's have reportedly attacked are Facebook, Google+, Linkedin and Microsoft.[115]

Software developers that create content for social media websites have also become targets for data thieves and lawsuits. In one illustrative example, a developer that creates online services and applications for use with social networking sites reportedly suffered a data breach in which (according to allegations contained in a complaint related to the breach) a hacker stole the email and social networking login credentials – *i.e.*, user names and passwords – of approximately 32 million people. The users had been required to provide their login credentials as part of a sign-up process to gain access to the developer's applications. A class action suit followed against the developer, which reportedly settled for minimal payment to the plaintiffs.[116] The U.S. Federal Trade Commission filed charges against the developer over the breach, and that proceeding was reportedly settled as well.[117]

The concern about password theft has increased, as has the threat of phishing attacks. Often users tend to use the same passwords on multiple sites, so that a password stolen from one site, even one

---

111 Zach Whittaker, *6.46 Million LinkedIn Passwords Leaked Online*, ZDNet, Jun. 6, 2012, http://www.zdnet.com/blog/btl/6-46-million-linkedin-passwords-leaked-online/79290.

112 *In Re LinkedIn User Privacy Litigation*, U. S. District Court Northern District of California, San Jose Division, Case No.:5:12-CV-03088-EJD.

113 Salvador Rodriguez, *Like LinkedIn, eHarmony is Hacked; 1.5 Million Passwords Stolen*, Los Angeles Times, Jun. 6, 2012, http://articles.latimes.com/2012/jun/06/business/la-fi-tn-eharmony-hacked-linkedin-20120606.

114 Jose Pagliery, *2 million Facebook, Gmail and Twitter passwords stolen in massive hack*, CNN Money, December 4, 2013, http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/.

115 See *Social Media, Is Covert Redirect Flaw a Big Deal* by Jeffrey Roman, http://www.databreachtoday.com/social-media-c-289 and *Social Media Latest to Feel Security Flaw Impact*, by Jeff Green, http://www.pymnts.com/news/social-commerce/2014/social-media-latest-to-feel-security-flaw-impact

116 *Claridge v. RockYou, Inc.*, No. C 09-6032 PJH (N.D. Ca.). According to reports, RockYou claimed it was financially unable to pay any judgment. Tim Wilson, *RockYou Lawsuit Settlement Leaves Question Marks on Breach Liability*, Security Dark Reading, Nov. 23, 2011, http://www.darkreading.com/insider-threat/167801100/security/privacy/232200192/rockyou-lawsuit-settlement-leaves-question-marks-on-breach-liability.html.

117 John P. Mello Jr., *RockYou Settles Pending Charges for $250K Over Data Breach*, PC World, Mar. 7, 2012, http://www.pcworld.com/article/252725/rockyou_settles_pending_charges_for_250k_over_data_breach.html.

for social use without financial or other protected information, can be used by hackers to try to obtain access to information maintained by a user on other sites.

Social media sites have also become targets for those investigating individuals. Some people examine the content that users make available on their social media website profiles. For example, workers' compensation claim investigators were reportedly examining the profiles of claimants to determine whether they are engaging in physical activity that their claimed injuries should prevent.[118] Social media content is also reportedly being used as evidence in divorce cases – according to one survey, more than one-third of divorce filings in 2012 contained the word "Facebook" and used patterns of behavior that are recorded by Facebook posts, such as those that arguably relate to parenting skills, excessive parenting or disparaging remarks about a spouse. All are admissible in custody and alimony battles.[119]

Others have identified ways to use publicly available information on social media websites to obtain information about the site's users. For example, researchers at Carnegie Mellon University reported that they were able to successfully guess individuals' Social Security numbers based on information on such websites.[120] The researchers also claim to have developed an application for iPhones that can take a photograph of someone and, through the use of facial recognition software, display on-screen that person's name and vital statistics.[121] Additionally, the researchers reportedly looked at photographs of anonymous people (many of whom used pseudonyms) on a dating website and, through facial recognition software and Facebook, were able to identify about 10% of the dating site's members.

b. Social Media as Source of Statutory and Regulatory Violations

Social media can be used to obtain information about individuals for less nefarious reasons than identify theft, but in contexts that can still have an effect on an individual such as in vetting applicants for employment or tracking the activities of employees. This has raised regulators' and legislators' concerns about the incursion on individuals' privacy and generated new and proposed laws regulating their use as well as regulatory scrutiny.

The increased use of social media in the workplace adds another layer of complexity to privacy issues. In 2010, the U.S. Supreme Court decided that a public employee who uses an employer-supplied, text messaging-enabled pager device does have a reasonable expectation of privacy with regard to personal messages sent on the device. The Court ruled, however, that under a Fourth

---

118 Roberto Ceniceros, *Comp cheats confess all on social network sites*, businessinsurance.com, Sept. 6, 2009.

119 Quentin Fottrell, *Does Facebook Wreck Marriages?*, Smart Money, May 21, 2012, http://blogs.smartmoney.com/advice/2012/05/21/does-facebook-wreck-marriages/.

120 *Facebook's Privacy Issues Are Even Deeper Than We Knew*, Forbes, Aug. 8, 2011, http://www.forbes.com/sites/chunkamui/2011/08/08/facebooks-privacy-issues-are-even-deeper-than-we-knew/.

121 *Face-matching with Facebook profiles: How it was done*, C/NET News, Aug. 4, 2011, http://news.cnet.com/8301-31921_3-20088456-281/face-matching-with-facebook-profiles-how-it-was-done/. *See also* Face Recognition Study – FAQ, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/. Facebook's own facial recognition technology has been the subject of various inquiries, including a recent Congressional hearing. Kashmir Hill, *Sen. Al Franken Grills Facebook and the FBI Over Their Use of Facial Recognition Technology*, Forbes Tech Blog, Jul. 18, 2012, http://www.forbes.com/sites/kashmirhill/2012/07/18/sen-al-franken-grills-facebook-and-the-fbi-over-their-use-of-facial-recognition-technology/.

Amendment analysis, the employer's review of two months' worth of the employees' text messages (in order to determine whether they were exceeding their allowable quotas for personal text messages) was justified.[122] Presumably, the Court's holding would also apply to messages shared on social media websites via employer-provided hardware.

In May 2012, the Acting General Counsel of the National Labor Relations Board ("NLRB") issued a report warning that many provisions routinely included in social media polices – such as blanket restrictions on the publication of confidential information and rules requiring a professional tone in online posts – may violate the National Labor Relations Act ("NLRA") by inappropriately restricting protected concerted activity rights.[123]

In September 2012, the NLRB issued its first decision on an employer's social media policy, holding that a general prohibition on what employees can say online violates Section 7 of the NLRA.[124] The NLRB rejected an administrative judge's approval of Costco Wholesale Corp.'s social media policy, determining that Costco's policy prohibiting employees from electronically posting statements that "damage the Company . . . or damage any person's reputation" was impermissible under the NLRA as an unlawful restraint on protected concerted activity rights.[125]

In another instance of the intersection between employment law and social media, in November 2010, the NLRB filed a lawsuit against an ambulance company, alleging that it violated federal labor laws (specifically, an employee's right to engage in protected concerted activities with other employees pursuant to the NLRB[126]) when it fired an employee for posting unflattering comments about her supervisor on a Facebook page.[127] The parties settled in January 2011; the employer agreed, among other things, to amend its social media policy.[128]

In a similar vein, employment background checks can include information from credit reports, employment and salary history, criminal records, and social media.[129] According to the FTC, the same rules that apply to other types of information also apply to social media. For example, the FTC website reports that FTC staff looked at a company selling background information from social media to see if it was complying with the Fair Credit Reporting Act ("FCRA"), and noted

---

122 *City of Ontario, California v. Quon*, 130 S. Ct. 2619, 560 U.S. 746, 177 L. Ed. 2d 216 (Jun. 17, 2010).

123 Lafe E. Solomon, Acting General Counsel of the NLRB, *Report of the Acting General Counsel Concerning Social Media Cases*, Office of the General Counsel – Division of Operation-Management, May 30, 2012.

124 *Costco Wholesale Corp. and United Food and Commercial Workers Union, Local 371*, Case 34-CA-012421 (NLRB Sept. 7, 2012).

125 *Id.*

126 29 U.S.C. § 151 *et seq*.

127 *American Medical Response of Connecticut, Inc. and International Brotherhood of Teamsters, Local 443*, Case No. 34-CA-12576 (NLRB Region 34).

128 *Conn. ambulance co. settles Facebook firing case with Labor Board*, International Business Times, Feb. 16, 2011 (http://www.ibtimes.com/conn-ambulance-co-settles-facebook-firing-case-labor-board-267649).

129 According to some recent reports, approximately 91% of employers use social media during their hiring process. *The Facebook Background Check: Using Social Media to Vet Candidates*, Ohio State Bar Ass'n, https://www.ohiobar.org/ForPublic/Resources/LawYouCanUse/Pages/The-Facebook-Background-Check-Using-Social-Media-to-Vet-Candidates.aspx. *See, e.g.*, Tyra M. Vaughn, *Exclusive: Public safety agencies use social media to check applicants' backgrounds*, Daily Press, Sept. 1, 2012, http://articles.dailypress.com/2012-09-01/news/dp-nws-police-hires-facebook-backgound-checks-0823-20120901_1_social-media-wight-sheriff-mark-marshall-check-job.

that "companies selling background reports must take reasonable steps to ensure the maximum possible accuracy of what's reported from social networks and that it relates to the correct person," as well as comply with other FCRA sections.[130]

Some employers have reportedly been more direct about their review of social media websites and have requested personal social media account login credentials during the job application process in an attempt to gain information about the job applicant. Such requests are now prohibited in some, but not all, states, with varying scope as to what conduct would be permissible for legitimate business purposes such as investigating improper employee downloading of an employer's proprietary information.[131]

Potentially problematic uses of social media have been reported outside the employment context as well. In one reported incident, a physician revealed sufficient information about a patient on a social media site to constitute a breach of patient privacy.[132] Judges and lawyers have been sanctioned for communications through social media,[133] and an Israeli army mission was aborted in 2010 when a soldier revealed the mission on Facebook.[134]

The use of social media is likely to continue to expand. Banks and lenders are expected to incorporate social media conversations into their analysis of credit risk.[135] For example, some online comments may be interpreted by lenders as an indicator that an applicant may be delinquent on a future loan or a possible credit risk. Research is reportedly being conducted to try to create correlations between online (social media) comments and possible credit issues, which could lead to a form of "social media underwriting" in the future.

In addition, schools are now attempting to use posts on Facebook accounts as evidence and for the punishment of students. For instance, a lawsuit filed in March 2014 by the American Civil

---

130 Lesley Fair, *The Fair Credit Reporting Act & social media: What business should know*, FTC Business Center Blog, Jun. 23, 2011 (http://business.ftc.gov/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know); Letter from Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, to Renee Jackson, dated May 9, 2011, http://ftc.gov/os/closings/110509socialintelligenceletter.pdf.

131 According to NCOIL, the National Conference of State Legislatures, states that have enacted such legislation intended to protect the privacy of prospective and current employees (and in some states a student) include, as of May 2014, Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, Maine, New Mexico, Oregon, Utah, Vermont, Washington and Wisconsin, www.ncsl.org. S*ee, e.g.*, California Chapter 618 of 2012; Illinois Public Act 097-0875(2012); Maryland Chapters 233 and 234 of 2012; Michigan Public Act No. 478 (2012), and New Jersey P.L. 2012, C.75. In late May 2014, two additional states passed similar statutes, Oklahoma (Oklahoma Statutes §173.2, of Title 40) and Louisiana (Louisiana Revised Statutes §51:1951-1955). More are likely to follow. Legislation has been reported to be introduced or pending in over two dozen additional states to prevent employees from requesting passwords to personal Internet accounts to get or keep a job. See *www.ncsl.org*. However, a federal version of a password protection statute, the *Password Protection Act of 2012*, did not make it out of committee in the House of Representatives, see H.R. 5684.

132 Chelsea Conaboy, *For doctors, social media a tricky case*, Boston Globe, Apr. 20, 2011, http://www.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/.

133 *See, e.g., Judge resigns amid probe about Facebook friend*, Atlanta Journal-Constitution, Jan. 7, 2010.

134 *Israeli military calls off raid after soldier posts details*, cnn.com. Mar. 3, 2010, available at http://www.cnn.com/2010/WORLD/meast/03/03/israel.raid.facebook/index.html.

135 Ken Lin, *What Banks and Lenders Know About You from Social Media*, Mashable Social Media, Oct. 7, 2011, http://mashable.com/2011/10/07/social-media-privacy-banks/. One UK-based company marketed itself for its utilization of social media profiles when underwriting online retailers. *capExpand Use Social Media to Underwrite Online Businesses*, Jan. 31, 2013, http://www.bloomberg.com/article/2013-01-31/arp4NczdKsjs.html.

Liberties Union of Minnesota alleged that a former student's free speech and privacy rights were violated when the student was unfairly punished for comments posted to her Facebook page. The punishment included detention, suspension and she was forced to turn over passwords to her Facebook and email accounts. The case settled with the Pope County in West Central Minnesota paying $70,000 and the district agreeing to changes in its policies regarding student privacy.[136]

These are just the tip of the iceberg for privacy issues arising from social media. Social media is certain to present increasing challenges to privacy and data security. Concerns about the adequacy of security of individuals' information on social media sites has caught the attention of U.S. regulators. In early May 2014, the U.S. Federal Trade Commission announced a settlement of charges filed against Snapchat Inc., a popular mobile message application, which was charged with deceiving its customers when it promised that photo and video messages on its site would disappear shortly after being sent when there were methods that existed by which a recipient could use tools outside of the application to save photo and video messages indefinitely.[137] There has also been regulatory scrutiny of Google and other large social media companies worldwide, with actions taken against them by regulators not only in the U.S., but in countries around the world who are concerned with the adequacy of privacy controls and the collection of information about individuals.

In the U.S., FTC complaints and settlements with social media giants have led to agreement of 20 years of auditing and fines of eight figures. For example, the FTC brought a complaint against Facebook in 2011, focusing primarily on changes that the company allegedly made to its privacy controls in 2009, which led to the automatic sharing of information and users' pictures even if they previously chose to not share that content.[138] The FTC also contended that Facebook shared its users' personal information with third-party advertisers despite several public assurances from the company that it did not.[139] As part of a settlement reached with the FTC, Facebook agreed to submit to government audits of its privacy practices every other year for the next 20 years and committed to obtaining explicit approval from users before changing the types of content it makes public.[140] Facebook did not, however, admit any wrongdoing as part of the settlement. That settlement and the privacy issues it addressed were the basis for a March 2014 complaint filed by

---

136 Susan Lunneborg, *Facebook lawsuit settled: Minnewaska Area agrees to update student privacy policies to address electronic media*, Western Central Tribune, http://www.wctrib.com/content/facebook-lawsuit-settled-minnewaska-area-agrees-update-student-privacy-policies-address; Susan Lunnenberg, *Western Minnesota student's free speech suit over Facebook comments settled for $70K*, http://www.twincities.com/localnews/ci_25419690/western-minnesota-students-free-speech....

137 Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False, May 8, 2014, www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-*charges-that-promises-of-disappearing-messages-were-false*. *See* Judy Greenwald, *FTC slaps Snapchat for overpromising users on privacy, security*, Business Insurance, May 9, 2014, http://www.businessinsurance.com/article/20140509/NEWS07/140509821?tags

138 *FTC finalizes Facebook privacy settlement*, USA Today, Aug. 10, 2012, http://www.usatoday.com/tech/news/story/2012-08-10/ftc-facebook-privacy/56934670/1.

139 Alan Friel, et al, *Take Heed: Facebook and Google Buzz's Privacy Settlements With FTC Reinforce Need to Audit Privacy Practices and Revisit Statements and Policies*, Digilaw Blog, Dec. 12, 2011, http://digilaw.edwardswildman.com/blog.aspx?entry=3852.

140 The settlement was finalized once the period for public comment ended. Kristin Jones, *FTC: Facebook Finalizes Settlement of Privacy Charges*, The Wall Street Journal, Aug. 10, 2012, http://online.wsj.com/news/articles/SB10000872396390443404004577581150743022604

privacy watchdog groups with the FTC challenging the proposed sale of WhatsApp (a company that offers an instant messaging service) to Facebook, based in part on the issue of whether Facebook's policies toward privacy are incompatible with WhatsApp's "pro-privacy" stance.[141] This has resulted in a statement by the FTC of which social media sites that are buyers or sellers of other sites take note. By letter dated April 10, 2014, the FTC's Bureau Director noted that both companies collect data from consumers but make different promises and statements with regard to consumer's privacy, with WhatsApp promises exceeding the protections currently promised to Facebook users, and that "we want to make clear that, regardless of acquisition, WhatsApp must continue to honor these promises to consumers."[142]

In 2012, Google also reached a settlement with the FTC in which it has agreed to pay $22.5 million to settle charges that it secretly bypassed the privacy settings of millions of users' Apple Safari web browser.[143] The settlement reflects a penalty for a violation of a prior order, which was a consent decree in which Google agreed in October 2011 not to misrepresent its privacy practices to consumers.[144] The FTC alleged that Google used cookies to monitor Safari users' web browsing despite advising the users that they would automatically be opted out of any such tracking. Google, however, did not admit any wrongdoing, which led to an objection to the settlement by FTC Commissioner J. Thomas Rosch as well as a motion filed by Consumer Watchdog in federal court in California that is responsible for approving or rejecting the proposed settlement.[145] The court approved the settlement despite the objection.[146]

Regulatory investigations and actions are likely to increase, as the challenge of balancing innovation and privacy continues.

7. Privacy Issues Arising Out of Behavioral Advertising and Online Tracking

Targeted advertising has become ubiquitous. Digital advertising is a $100 billion industry.[147] Significant privacy concerns have recently been raised by regulators and in a rash of class actions arising from targeted advertising and tracking of consumer behavior by companies that market online and via mobile devices.

---

141 Seth Rosenbaltt, *Privacy groups ask FTC to block Facebook-WhatsApp deal*, CNET, March 6, 2104, http://www.cnet.com/news/privacy-groups-ask-ftc-to-block-facebook-whatsapp-deal/.

142 *FTC Notifies Facebook WhatsApp of Privacy Obligations in Light of Proposed Acquisition*, http://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed

143 Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, FTC, Aug. 9, 2012, http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

144 Jennifer Valentino-Devries, *Google to Pay $22.5 Million in FTC Settlement*, The Wall Street Journal, Aug. 9, 2012, http://online.wsj.com/article/SB10000872396390443404004577579232818727246.html.

145 Consumer Watchdog raises issue with the settlement because it allows Google to deny any wrongdoing. Juan Carlos Perez, *Consumer Watchdog Challenges Google-FTC Privacy Settlement*, PC World, Aug. 22, 2012, http://www.pcworld.com/businesscenter/article/261282/consumer_watchdog_challenges_googleftc_privacy_settlement.html.

146 *United States of America v. Google., Inc.*, Case No. CV12-04177 SI, U. S. District Court, Northern District of California.

147 Ken Doctor, *The newsonomics of GAFA's global reach*, Nieman Journalism Lab, Mar. 21, 2013, http://www.niemanlab.org/2013/03/the-newsonomics-of-gafas-global-reach/.

a. In the United States

i. The FTC Recommendations

The FTC defines Online Behavioral Advertising ("OBA") as a process of "tracking consumers' activities online to target advertising."[148] It often, but not always, includes a review of the searches consumers have conducted, the Web pages visited, the purchases made, and the content viewed, in order to deliver advertising tailored to an individual consumer's interests.

The FTC has taken a strong interest in the privacy issues presented by OBA. In a Final Report released in March 2012, the FTC set forth its Final Framework, which affirmed that the guidance will apply to OBA data that is reasonably linkable to a specific consumer, computer or device, including data not yet linked which may reasonably become so.[149] Among other factors, the FTC referenced two categories of comments that influenced its decision to maintain this definition in the final March 2012 report: (a) ". . . commenters pointed to studies demonstrating consumers' objections to being tracked, regardless of whether the tracker explicitly learns a consumer name, and the potential for harm, such as discriminatory pricing based on online browsing history, even without the use of PII"; and (b) ". . . commenters noted, the ability to re-identify 'anonymous' data supports the proposed framework's application to data that can be reasonably linked to a consumer or device."[150] The final March 2012 Framework responded to businesses' concerns that the "reasonably linkable" definition may be overbroad in practice, by stating that:

> … a company's data would not be reasonably linkable to a particular consumer or device to the extent that the company implements three significant protections for that data. First, the company must take reasonable measures to ensure that the data is de-identified…. Second, a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data…. Third, if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data.[151]

In March 2013, the FTC released updated guidance for mobile and other online advertisers that focused on explaining how to make their disclosures to consumer of their practices clear and conspicuous to avoid charges of deceptive practices (updating guidance initially released in 2000). The updated FTC Guidance is entitled *.com Disclosures: How to Make Effective Disclosures in Digital Advertising.*[152]

---

148 FTC Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* at p. 2, Feb. 2009, http://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles.

149 *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at pp. 18 - 20, March 26, 2012, http://ftc.gov/os/2012/03/120326privacyreportpdf.

150 *Id.* Also noting that commenters to the December 2010 draft report "pointed to incidents, identified in the preliminary staff report, in which individuals were re-identified from publicly released data sets that did not contain PII." *Id.* at p. 18.

151 *Id*. at p. 21.

152 The Guidance is available through the FTC website, www.ftc.gov.

The FTC has initiated enforcement proceedings and announced enforcement consent orders against companies for delivering OBA without consumer consent, generally alleging "deceptive" acts in violation of the FTC Act and imposed ongoing reporting requirements for 20 years.[153] Enforcement actions continue. As noted above, on August 9, 2012, the FTC and Google entered into a consent decree resulting in a $22.5 million fine – the largest awarded ever by the FTC – for Google's alleged use of cookies to circumvent user's privacy settings in Apple's Safari browser. This allegedly caused users who had elected not to receive targeted ads to be served with Google's targeted ads anyway.[154] More recently, in March 2013, the FTC settled charges against Epic Marketplace, an online ad network, that allegedly used "history sniffing" to gather data from millions of consumers across sites they visited and ads they reviewed, including collection of data about sites outside its network relating to personal health conditions and finances.[155]

On May 15, 2014, the FTC testified before Congress on the agency's ongoing efforts to protect consumers from emerging threats related to online advertising and associated tracking of consumers' online activities across websites, and on the agency's continued outlining steps the agency is taking through enforcement actions as well as consumer education.[156] This is part of the FTC's continued aggressive stance in addressing privacy related issues.

ii. Industry Self-Regulation

Faced with increasing regulatory oversight and enforcement actions, the online advertising industry has increased its self-regulation of OBA. [157]

The Digital Advertising Alliance (DAA) has released *Self-Regulatory Principles for Online Behavioral Advertising*, issued in 2009, followed by an implementation guideline for a Self-Regulatory Program in 2010.[158]

Other organizations such as the World Wide Web Consortium Tracking Protection Working Group have also been working on issuing self-regulatory guidelines.[159] The Direct Marketing Association

---

153 *In the Matter of Chitika, Inc.*, the FTC pursued Chitika for having an "opt-out" for behavioral advertising that expired after 10 days, alleging that this was a "deceptive" practice because the opt-out was not meaningful. Chitika now has a 20-year reporting requirement to the FTC. In August 2011, the FTC pursued its first mobile app complaint, resulting in a consent decree against a mobile advertiser that served targeted ads to children under the age of 13 in violation of COPPA. *United States of America, Plaintiff v. W3 Innovations, LLC, also d/b/a Broken Thumbs Apps,* http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm. On November 8, 2011, the FTC entered into a consent order against a digital third-party advertiser, Scanscout, for its alleged due of flash cookies to target advertising.

154 http://www.ftc.gov/os/caselist/c4336/120809googlecmptexhibits.pdf.

155 *Epic Marketplace, Inc.* No. C-4389 (FTC March 2013), see http://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc.

156 See FTC May 15, 2014 press release and the Prepared Statement of The Federal Trade Commission on Emerging Threats in the Online Advertising Industry before the Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, United States Senate, May 15, 2014, http://www.ftc.gov.

157 See Christopher Mickus, *Technology: FTC and self-regulatory frameworks regarding online behavioral advertising*, Inside Counsel, October 18, 2013, http://www.insidecounsel.com/2013/10/18/technology-ftc-and-self-regulatory-frameworks...

158 See www.iab.org website for details, e.g., http://www.iab.net/public_policy/behavioral-advertisingprinciples.

159 See http://www.w3.org/2011/tracking-protection/.

("DMA") has also issued OBA guidelines underscoring several Self-Regulatory Principles set forth by various other advertising organizations and the Better Business Bureau in response to FTC calls for greater transparency knowledge and choice by consumers.[160] The Council of Better Business Bureaus administers the Online Interest-Based Advertising Accountability Program, which includes initiation of formal enforcement of Self-Regulatory Principals for Online Behavioral Advertising, and has endorsed the self-regulatory principles drafted by the Digital Advertising Alliance ("DAA"). Companies agree to voluntarily modify their practices to comply with the Principles.[161]

iii. Do Not Track Class Actions

Consumers are claiming that tracking their activities online or on their mobile devices violates their right to privacy, and generally alleging a variety of state and federal statutory and common law claims and violations. The class action bar filed more than 150 putative class action lawsuits alleging violations of the Electronic Communications Privacy Act ("ECPA"), the Computer Fraud and Abuse Act ("CFAA"), and state laws.

The ECPA prevents access and tracking of user behavior without consent. Initially, primary defenses to the ECPA claims were based on motions to dismiss claiming lack of Article III standing (no injury in fact) and consent. However, starting around June 2012, courts (particularly those in California), held in several cases that plaintiffs had sufficiently alleged harm to avoid dismissal of their complaints, and the U.S. Supreme Court decided not to address whether statutory damages could constitute injury in fact, thus raising issues as to the continued viability of the harm defense to future privacy class actions at least in those jurisdictions.[162] Thus, the focus in the defense is generally on the sufficiency of disclosures and consent provisions on the website and contained in a

---

160 http://www.dmaresponsibility.org/privacy/oba.shtml.

161 See www.bbb.org website.

162 See Section on privacy based litigation below.

the Northern District of California held in the *In re iPhone/iPad Application Consumer Privacy Litigation*, N.D. Cal. Case No. 5:11-md-02250, on June 12, 2012, that Article III harm had been alleged where the plaintiffs identified the specific applications that tracked their behavior and other harm besides just invasion of privacy. This was a reversal of the Northern District's original position finding no Article III harm as it related to the original complaint. In the June 12, 2012 Order, the Northern District stated: "Plaintiffs have articulated additional theories of harm beyond their theoretical allegations that personal information has independent economic value. In particular, Plaintiffs have alleged actual injury, including: diminished and consumed iDevice resources, such as storage, battery life, and bandwidth,… increased, unexpected, and unreasonable risk to the security of sensitive personal information …; and detrimental reliance on Apple's representations regarding the privacy protection afforded to users of iDevice app. Additionally, Plaintiffs have addressed the deficiencies identified in the Court's September 20 Order." (June 12, 2012 Order, Dkt 69, at 10.)

Second, on the heels of the Northern District's decision, the Supreme Court decided not to address the harm threshold issue. As background, in late 2011, the U.S. Supreme Court took up the issue of standing in the case of *First American Financial Corp. v. Edwards*. The Ninth Circuit Court of Appeals had ruled that statutory damages alone are enough to confer Article III standing on a plaintiff under the Real Estate Settlement Procedures Act (RESPA). The high court was expected to address its prior decisions that had held that Article III's "case and controversy" provision required that a plaintiff allege, and eventually prove, that he or she suffered an "actual injury" as a result of a defendant's conduct in order to have standing to sue in federal court. However, after briefing and argument was complete, rather than upholding or overturning the lower court's decision, on June 28, 2012, the Supreme Court simply dismissed the appeal as "improvidently granted." The Supreme Court's decision may be found at http://www2.bloomberglaw.com/public/document/First_American_Financial_Corp._v_Edwards_No_10708_2012_BL_160940_U. Already, at least one court has held, after the *First American Financial Corp*. decision, that plaintiffs had standing to assert claims for privacy violations relating to tracking, and the defendant's motion to dismiss based upon lack of harm ground failed. *See e.g., In re Hulu Privacy Litigation* (Case No. 3:11-cv-03761, Dkt 68, Jul. 28, 2012 Order).

Privacy Policy and Terms of Use), with some courts showing a willingness to infer consent if a consumer has reviewed a privacy policy that discloses tracking. Other defences include focusing on the requirements of ECPA for disclosure of contents of a communication. [163]

The CFAA makes it unlawful to track user browsing behavior if this causes $5,000 in economic loss, and thus the focus in defense is generally on the sufficiency of allegations and evidence of economic loss.[164]

The plaintiffs' bar has also filed lawsuits relying on other privacy statutes, such as the Video Privacy Protection Act ("VPPA"), to pursue claims. For example, *In re Hulu Privacy Litigation* considers whether a provider of online streaming digital video content qualifies as a "video tape service provider" under the VPPA.[165] The *Hulu* court found that Hulu was a "video tape service provider" as defined by the VPPA, even as it pertained to free content on its website that users (plaintiffs) could stream without affirmatively registering for or subscribing to the Hulu service. The court referred to the legislative history of the VPPA as showing Congress's intent to "ensure that VPPA's protections would retain their force even as technologies evolve."[166] The court was also persuaded that Congress intended the VPPA to provide broad protection for consumers' privacy. This decision cleared the way for the plaintiffs to allege statutory damages of $2,500 per violation for millions of page views, assuming the other hurdles identified in the decisions are overcome. Thus, it is likely to be cited by the class action bar.

---

[163] In early 2014, the Ninth Circuit (which hears appeals from federal trial level courts sitting in California) addressed the viability of claims of violation of the ECPA, among other statutory violations in *Zynga Privacy Litigation*, No. 11-18044, 2014 WL 1814029 (Ninth Cir., May 8, 2014) (in which social network and social gaming users brought class actions against a social networking company [Facebook] and social gaming company [Zynga] alleging violations of the Wiretap Act and Stored Communications Act provisions of the ECPA by disclosing user information to third parties; the court concluded that the plaintiffs failed to state a claim for violation of ECPA because they did not allege disclosure of the "contents" of a communication, which it found to be a necessary element of an ECPA claim). See also section below on privacy related litigation which identifies several decisions addressing the issues of standing and what courts have found to be sufficient allegations of harm.

[164] A recent decision discussing such claims under CFAA as well as California state law (and citing to decisions in other jurisdictions) is *In re Google Android Consumer Privacy Litigation*, No. 11-MD-02264, 2014 WL 988889 (N.D. Cal., March 10, 2014). In that decision, Google moved to dismiss claims based on allegations that apps improperly collected personal data from their Android mobile phones and shared this data with Google. The motion to dismiss was based on the argument that plaintiffs lacked standing under Article III of the U.S. Constitution. Plaintiffs in turn argued they had sufficient "injury in fact" based on allegations, among others, that the increased rate at which their batteries discharged based on defendants' conduct. The Court dismissed the CFAA claims, noting that CFAA defines "loss" as "any reasonable cost to any victim…" and concluding that the allegations were insufficient to establish damage or loss. However, the Court did allow to proceed a claim under the state Unfair completion Law, even thought that statute also requires a plaintiff to have lost money or property to have standing to sue, on the grounds that allegations of diminished battery life were sufficient under the state statute. Other causes of action also survived the motion to dismiss, at least at this lower court state of the litigation. See also *In re IPhone Litigation*, No. 11-MD-02250, 2013 WL 6212591 (N.D. Cal. Nov. 25, 2013), dismissing such state law claims on summary judgment on grounds that while a fact issue existed as to whether consumers suffered "injury-in-fact" that was economic in nature, the consumers lacked standing based on their failure to allege specific facts showing (or at least demonstrating a genuine issue of material fact) that they read and relied upon manufacturer's alleged misrepresentations as to its practices and suffered economic injury as a result of that reliance, *i.e.,* causation as well as actual reliance.

[165] *In re Hulu*, No. 3:11-cv-03764-LB (N.D. Cal. Aug. 10, 2012); see also decision on summary judgment motions 2014 WL 1724344 (N.D. Cal. April 28, 2014) (granting Hulu summary judgment on the comScore disclosures which were demonstrated to be anonymous disclosures when sent by Hulu, but denying as to the Facebook disclosures on the ground that there were material issues of fact about whether the disclosure of the video name was tied to an identified user such that it was a prohibited disclosure under the VPPA, and because the record was not developed sufficiently to determine as a matter of law whether Hulu knowingly disclosed information or whether Hulu users consented to the disclosures.

[166] *Id*., August 10, 2012 decision, at 9.

iv. Do Not Track Legislation

Calls for a national "Do Not Track" bill have so far been unsuccessful, although the Obama Administration has supported one and numerous bills have been proposed.

In March 2011, the Obama administration called for a universal privacy bill, and expressly supported the FTC's "Do Not Track" proposals. Legislators initially responded with numerous proposals, with a new effort initiated by Senator Rockefeller in 2013, but so far none have been enacted.[167]

California also proposed a "Do Not Track" bill that contains a private right of action and statutory penalties.[168] Ultimately, in September 2013, California's Governor signed a new privacy law that went into effect January 1, 2014, and requires that businesses that operate a commercial website or online serve and collect "personally identifiable information" (as defined by the law) to disclose how they respond to Web browser "do not track" signals or other mechanisms that provide consumers with the ability to exercise choice over the collection of their PII , and disclose if such information is collected by a clear and conspicuous hyperlink in its privacy policy that links to a description of any protocol the operator follows that offers the consumers the choice to opt out of internet tracking.[169] The law's requirements focus on disclosure, rather than on requiring the honouring of do not tract requests, but of course not following disclosures can be the basis for misrepresentation claims.

On September 15, 2011, the FTC recommended amendments to the Children's Online Privacy Protection Act ("COPPA")[170] which would expand the definition of "personal information" to

---

[167] *See, e.g.*, H.R. Bill Nos. 611, 653 and 654, which recommend "do not track" without consumer consent (introduced by Representatives Bobby Rush and Jackie Speier, respectively, in February 2011. HR 611 was referred to the House Committee on Energy and Commerce in February 2011, where it remained as of August 2011; HR 653 was referred to the House Committee on Financial Services, and HR 654 was referred to the House Committee on Energy and Commerce.) On May 13, 2011, Representatives Markey (D) and Barton (R) co-sponsored HR 1895 "Do Not Track Kids Act of 2011" (proposing amendments to the Children's Online Privacy Protection Act to prohibit mobile tracking of children under the age of 13). The Senate is also considering its own behavioral advertising bills. Also, Senators John Kerry and John McCain introduced legislation on the Senate side. See Commercial Privacy Bill of Rights Act (introduced Mar. 2011) at http://thomas.loc.gov/cgi-bin/query/C?c112:./temp/~c1129yzKOm. Senator Rockefeller introduced the Do-Not-Track Online Act of 2011 as SB 913 (which would create a "universal legal obligation" for companies to honor users' opt-out requests on the Internet and mobile devices). This bill was referred to the Senate Committee on Commerce, Science and Transportation. In 2013, Senator Rockefeller tried again, introducing in the Senate S.418, the Do-Not-Track Online Act of 2013 (which would require the FTC to promulgate regulations that establish standards for implementation of a mechanism by which an individual can indicate if he or she prefers to have personal information collected by providers of on line services, including providers of mobile applications, and prohibit collection of personal information on individuals who have expresses a preference not to have such information collected, and which would also allow for collection and usage of such information notwithstanding the expressed preference if necessary to provide a service requested by the individual so long as identifying particulars are removed or information deleted on provision of the service, or the individual receives clear, conspicuous, and accurate notice and consents to such use and collection).

[168] See, SB 761, introduced by state Senator Alan Lowenthal on February 18, 2011. It was amended four times, with the last amendment on May 10, 2011, and included a requirement that the state attorney general issue regulations that would require Web companies to notify state residents about online data collection and allow them to opt out, and contained a private right of action and a statutory penalty of $1,000 per violation.

[169] Cal. Bus. & Prof . Code §§22575-22578.

[170] Children's Online Privacy Protection Rule 16 C.F.R. § 312, http://www.ftc.gov/os/2011/09/110915coppa.pdf. Also, on November 8, 2011, the FTC issued its new guidance regarding consumers and cookies. *See* http://onguardonline.gov/articles/0042-cookies-leaving-trail-web.

include OBA information. Comments were received and the FTC proposed further revisions. On November 13, 2013, Senator Edward Markey (D-Mass) and Rep. Joe Barton (R- Texas) introduced an updated version of their 2011 proposed legislation, the "Do Not Track Kids Act of 2013.[171]

On February 23, 2012, the Obama Administration issued a comprehensive framework for consumer privacy protection entitled "Consumer Data Privacy In A Networked World: A Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy (the "President's Privacy Framework").[172] The document outlines a vision for consumer privacy and provides guidance, particularly in the areas of behavioral advertising and mobile media. It also includes a definition of "personal data" that includes information that is used to deliver targeted marketing (*e.g.*, mobile unique identifiers). The President's Privacy Framework consists of: 1) a Consumer Privacy Bill of Rights; 2) a multi-stakeholder process to develop enforceable codes of conduct; 3) enhanced enforcement by the FTC and safe harbours for companies that adopt codes of conduct; and (4) a commitment to increase intraoperability with the privacy frameworks of international partners. On February 24, 2014, the second anniversary of the issuance of the framework, 40 organizations signed a letter to the President urging that he work with congress to pass legislation applying this "Consumer Bill of Rights" to commercial sectors not subject to existing Federal data privacy laws.[173]

b. E.U. Positions on Online Behavioral Advertising

Effective May 25, 2011, countries in the E.U. were required to implement regulations to obtain explicit consent before companies collect OBA information. On December 13, 2011, the UK's Information Commissioner's Office (the ICO) advised that opt-in consent will be necessary to collect OBA.[174] The UK announced that it would begin enforcement actions to ensure compliance starting May 25, 2012.[175] In May 2012, the ICO published revised guidance on the rules on use of cookies and similar technologies. The 2012 guidance is identical in almost all respects to the revised guidance published in December 2011, with the exception of the ICO's advice on the use of implied consent. The guidance now states that the provider can rely on implied consent, but only on the understanding that: it is specific and informed and there is some action on the part of the user from which consent can be inferred.[176]

Further, on 4 February 2013 a new set of OBA rules came into effect, aiming to secure transparency and control for web users and enforced by the Advertising Standards Authority (the ASA). These

---

[171] Their respective versions are S. 1700 and H.R. 3481. As of May 2014, it is still in Committee. See also Section on COPPA below.

[172] *See* Dominique R. Shelton, *Takeaways From Obama's New Consumer Privacy Framework,"* Daily Journal, Mar. 2, 2012, available at http://www.edwardswildman.com/files/upload/Edwards%20Wildman%20(DJ%203%202%2012)%20e-p.pdf.

[173] See http://wepic.org/privacy/white_house_consumer_privacy_bill_of_rights.

[174] *Must Try Harder on Cookie Compliance Says ICO,* Information Commissioner's Office News Release, Dec. 13, 2011,http://www.ico.gov.uk/news/latest_news/2011/must-try-harder-on-cookie-compliance-says-ico-13122011.aspx.

[175] See Edwards Wildman Palmer LLP Client Advisory, *25 May Deadline for UK Website Providers,* Apr. 2012, http://www.edwardswildman.com/Edwards-Wildman-Client-Advisory---Cookie-Transparency-25-May-Deadline-for-UK-Website-Providers-04-18-2012/.

[176] The ICO 2012 guidance is available at http://ico.org.uk/news/blog/2012/updated-ico-advice-guidance-e-privacy-directive-eu-cookie-law. (This link provides video guidance the ICO released and a link to the pdf guidance

rules supplement existing opt in and transparency rules for cookies under the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (Regulations) enforced by the ICO. There is some overlap between the ASA's guidance and the cookie consent opt in legal requirements under the Regulations.

The ASA rules require[177]:

- Notifying consumers - third parties delivering ads to web users using OBA must give a "clear and comprehensive" notice to web users about the collection and use of web viewing behaviour data. This notice must be given on the third party's own website and either in or around the advertisement delivered by OBA.

- Consumer choice - the notice must also inform users of how to opt out of OBA and must include a link to a relevant mechanism that allows them to opt-out.

- Explicit consent if all info captured - third parties that use technology to collect and use information about all or substantially all websites visited by web users on a particular computer must obtain explicit consent. This rule is aimed at "deep packet inspection" OBA, typically conducted at an ISP level.

- No targeting the under 12s - third parties delivering OBA must also not create "interest segments" specifically designed for the purpose of targeting children aged 12 or under.

8. Mobile/Apps as a Growing Exposure

In light of the importance of digital advertising revenue to businesses has led to an increase in both private litigation and regulatory scrutiny not only of Online Behavioral Advertising and tracking as discussed above, but of the usage of mobile apps in particular and the challenges those present in providing transparency and adequate disclosures to consumers increasingly utilizing apps on the small screens of smart phones and other mobile devices. Regulators in both the US and EU have recently issued guidelines for mobile app developers, and indicated they will scrutinize how developers address privacy concerns.[178]

In the US, the heighted scrutiny accorded mobile/apps has been led by the FTC on the federal level, and California on the state level, both of which have issued guidances, and instituted enforcement actions against mobile app operators.

As discussed above, in March 2013, the FTC updated an earlier guidance on disclosures to take into account the developments in technology, and released an updated guidance for mobile and other online advertisers directed at explaining how to make their disclosures to consumer of their

---

[177] The ASA Codes are available at http://www.cap.org.uk/Advertising-Codes/Non-broadcast-HTML/Appendix-3-Online-Behavioural-Advertising.aspx

[178] See *Regulators Are Expressing Heightened Interest in Mobile Apps and Privacy Enforcement: Is Your Company Prepared?*, Edwards Wildman, April 2013, http://www.edwardswildman.com/Regulators-are-Expressing-Heightened-Interest-in-Mobile-Apps-and-Privacy-Enforcement--Is-Your-Company-Prepared-4-02-2013/

practices clear and conspicuous to avoid charges of deceptive practices, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising.*[179]

The FTC is not the only federal agency scrutinizing mobile app developers. Agencies overseeing specific industries are also entering the fray. The U.S. Food & Drug Administration ("FDA"), for example, is scrutinizing mobile medical apps. The FDA has apparently been hesitant in the past to take actions that would chill innovation of tools for monitoring medical conditions remotely, many of which methodologies are available for smartphones and tablets. However, in May 2013, it issued its first publically announced enforcement action against a mobile app developer by issuing a letter to an India-based developer that had been the subject of complaint because it was selling its app on Apple Inc.'s App Store to screen for diabetes and urinary tract infections without first seeking the FDA's blessing as required for medical devices.[180] On September 25, 2013, the FDA issued its final Guidance for Industry and Food and Drug Administration Staff on Mobile Medical Applications, containing "nonbinding recommendations" with the stated goal set forth in the Introduction that it is to "inform manufacturers, distributors, and other entities about how the FDA intends to apply it regulatory authorities to select software applications intended for use on mobile platforms…" [181] While the regulatory issue that triggered this was not privacy, the final Guidance does refer readers to the FDA's Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. [182]

The U.S. National Institute of Standards and Technology ("NIST") is also involved in developing guidelines for organizations to address security issues in the use of mobile devices, including providing recommendations for implementing centralized management technologies. In July 2012 it issued draft Guidelines for Managing and Securing Mobile Devices in the Enterprise.[183] In June 2013, these were superseded by NIST Special Publication 800-124, Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise.[184]

In January 2013, the California Attorney General issued a report entitled *Privacy on the Go: Recommendations for the Mobile Ecosystem*, making it clear that mobile privacy will be an enforcement priority for its newly created Privacy Enforcement and Protection Unit. The report outlines best practices for mobile consumer privacy, including summary disclosures of key privacy practices that are more accessible on small screens, minimizing use of device identifiers, and limiting data collection and use to what is necessary to effect the functionality a consumer has elected to receive.[185]

---

[179] The Guidance is available through the FTC website, www.ftc.gov.

[180] http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm; see Jeff Overlay, *FDA Shows Deft Touch With 1st Mobile App Enforcement*, Law360, May 22, 2013, http://www.law360.com/articles/443997/print?section=lifesciences.

[181] See the Guidance, available on http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

[182] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm).

[183] Available at http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

[184] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890048

[185] A copy of the report is available at http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.

In the EU, the Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy, adopted on 27 February 2013, its Opinion 02/2013 on apps on smart phones.[186] Its stated goal was "to clarify the legal framework applicable to the processing of personal data in the development, distribution and usage of apps on smart devices, with a focus on the consent requirement, the principles of purpose limitation and data minimisaton, the need to take adequate security measures, the obligation to correctly inform end users, their rights, reasonable retention periods and specifically, fair processing of data collected from and about children.[187]

9. The Importance of Privacy Policies

Increasingly, regulatory agencies investigating a company, often after such company has disclosed that it sustained a breach or the agency has otherwise learned of the breach,[188] will request and review the privacy policies of that company, scrutinize its compliance with regulatory requirements and review the accuracy of its privacy statements when evaluating whether to issue a fine, and, if so, the amount. Similarly, lawsuits by consumers and other third parties affected by a data breach often focus on representations as to data security made by the breached company in their privacy policies and on their websites. Thus, a compliant privacy policy is a critical factor in mitigating exposures arising from data breaches.

Moreover, legislative and regulatory requirements increasingly focus on the content of privacy policies, and whether they adequately disclose to consumers the company's practices in the collection and use of information about individuals, as demonstrated by California. As with many statutory requirements, failure to follow them has provided fodder for class action attorneys to try to certify classes and obtain statutory penalties that are often calculated on a per-violation basis.

a. The California Example

In the U.S., California has often led the way in privacy statutory requirements, and continues to do so in the area of required privacy policies for companies that collect and use consumer information for marketing purposes and through online applications.

i. California's Shine the Light Law

California's Shine the Light Act[189] requires certain businesses to disclose their collection and usage of consumer information, and provide consumers with the ability to opt out. It requires certain businesses and non-profits with 20 or more employees that have an established business relationship with a consumer to either:

> Adopt a Privacy Policy of not disclosing certain information of its customers (defined as personal information, but which under this Act is a term that is far broader in scope than its typical use, and includes certain demographic information) to third parties for

---

186 Available on http://ec.europa.eu/justice/data-protection/index_en.htm.

187 Guidance at p. 2.

188 *See*, Section III.d, below.

189 CA Civil Code § 1798.83.

> that third party's marketing purposes without the advance consent of its customers, or give its customers the option of "opting out" of such disclosures, and must publicly disclose the policy or option (for example, in its website Privacy Policy), or
>
> Annually, upon request, identify the categories of personal information disclosed regarding its users during the previous year, and the names and addresses of any third parties to whom such information was disclosed, together with information sufficient to identify the nature of the third parties' businesses.

The Act applies to both online and offline collection and disclosures and there are specific requirements for online and brick-and-mortar notices. There are nuances as to the businesses the Act applies to, which are exempt, what reports consumers are entitled to receive, and how various terms such as "third party" are applied. Failure to comply with the intricacies of the Act led to the filing of multiple class action lawsuits against online retailers and publishers in 2013.

ii. California's Online Privacy Protection Act

California also has specific statutory requirements for privacy policies of entities that collect PI of California residents through the Internet. The California Online Privacy Protection Act (**"**OPPA**"**) requires "an … online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial website or online service … [to] conspicuously post [a] … privacy policy…."[190]

OPPA has specific requirements as to how the privacy policy must be noticed, including the form of notice and the link on site or application home page. In March 2012, the California Attorney General pointed to studies indicating that only 19% of the top 340 mobile applications post privacy policies and only 5% of all mobile apps do so. She gave notice that OPPA's requirements applied to mobile apps and that failure to comply could lead to actions under California's Unfair Competition Law[191] (which also permits class actions by consumers). She also recently brought an action against Delta Airlines for failure to have a privacy policy posted on its mobile apps in compliance with OPPA. In May 2013, Delta succeeded in obtaining a dismissal of that case on federal preemption grounds, based on federal laws prohibiting state regulation of airlines. Those grounds would not apply to other industries, and the California Attorney General has appealed the decision.[192]

As of January 1, 2014, an amendment to OPPA went into effect which now requires web site and online services to make certain disclosures regarding online tracking and targeted advertising. Prior to the amendment, OPPA required a website and online service operator to disclose in its privacy policy: (1) categories of personal information gathered; (2) parties with whom such information is shared; (3) if the operator maintains a process for consumers to review and change such information; (4) a description of the process by which the operator notifies users of changes to its

---

190 CA Bus & Prof. Code Sec. 22575.

191 Codified at Cal. Bus. Prof. Code § 17200.

192 *The People of the State of California v. Delta Airlines, Inc.*, Case No. 12-526741, Superior Court for the State of California, City and County of San Francisco. The decision is on appeal.

privacy policy; and (5) the effective date of the policy. After the amendment, in addition to the foregoing, OPPA requires the operator to: (1) disclose how the operator responds to "Do Not Track" signals or other mechanisms giving consumers the ability to exercise choice over the collection of personal information over time and across third-party websites or online services, if the operator engages in the collection of such information; and (2) disclose whether other parties may collect such information over time and across different Web sites when a consumer uses the operator's site or service.

iii. California's Social Eraser Law

California passed a new law with respect to Privacy Rights for California Minors in the Digital World.[193] The law will amend California Business and Professions Code by adding Sections 22580 -22582 to it.

The law will prohibit websites from advertising certain items to minors if the "marketing or advertising is specifically directed to that minor based on information specific to that minor." Among the prohibited items are alcoholic beverages, firearms, ammunition, spray paint, tobacco and cigarettes, fireworks, tattoos, drug paraphernalia, and obscene material.

In addition to the foregoing advertising restrictions, the new law also implements what has been described as a "Social Eraser."

This provision requires operators of websites directed to minors or with actual knowledge that minors are using the website (1) to permit registered users who are minors to remove, or request removal of, content posted by the user (but not third parties); (2) provide notice that the information may be removed; (3) provide clear instructions as to how to remove; and (4) provide notice that such removal mechanisms do not ensure complete or comprehensive removal.

The operator however does not have to erase or remove content if: (1) federal or state law requires its retention; (2) it was posted by a third party; (3) it is anonymous data; (4) the minor does not follow the instructions provided by the website regarding how to remove or request removal; or (5) the minor received compensation for the content.

Lastly, the operator is deemed to be in compliance if (1) it renders the information no longer visible to third parties (even if still on the server); or (2) if even after making invisible, it remains visible because a third party has copied or reposted the content.

This law is scheduled to go into effect on January 1, 2015, and will be another potential source for class actions and regulatory enforcement proceedings.

10. New Technologies Bring New Risks

As corporations and consumers embrace new technology, cyber criminals adapt their tactics to take advantage of new opportunities for data theft. Sales of smartphones and tablet computers have now eclipsed sales of PCs, and cyber criminals are beginning to shift more of their attention to trying to

---

[193] California Senate Bill 568 available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568

exploit security holes in the ubiquitous mobile devices. At the same time, more and more organizations are embracing a bring your own device ("BYOD") to work culture (or at least allowing use of them for work). In fact, bringing your own device was just a first step to a culture of bring your own anything and everything ("BYOx"), from usage of personal clouds (BYOC, including personal usage of cloud service or storage providers, rather than one with whom a business has entered into a contractual relationship or otherwise sanctioned) to devices, applications and wearables of all kinds. Increasingly, everyday devices are linked to the internet for monitoring and control, ranging far beyond computers to include a wide range of home appliances and monitoring mechanisms, medical devices, vehicles – in what has become popularly referred to as the Internet of Things. It is now estimated that more things are connecting to the Internet than people — over 12.5 billion devices in 2010 alone, with predictions that 25 billion devices will be connected by 2015, and 50 billion by 2020. [194]

Interconnectedness, however, while providing positive advantages including efficiency and connectivity between distant operations and operators, also brings with it vulnerabilities to unauthorized access and related network and data security concerns, as well as increases privacy issues.

III. The U.S. Regulatory and Statutory Landscape: Obligations Under Data Privacy and Security Laws and Regulations

The regulatory and statutory landscape related to data privacy and security has changed significantly in the past decade in response to increasing concerns about information privacy, identity theft, and fraud. State, federal, industry, and international requirements impose new and evolving obligations on companies to protect the Personal Information they collect, store, maintain, transfer or use, whether such information relates to customers, employees or others, as well as notification requirements in the event of a data breach. There has been increasing scrutiny of the usage of Personal Information, and increasing enforcement of disclosure obligations as to companies' collection and use of information about individuals. Non-compliance with applicable requirements exposes companies to the risk of government investigations, fines and penalties, as well as the risk of litigation by individuals and classes of individuals alleging non-compliance with privacy and data security requirements, including following a data breach. Although laws and regulations concerning data privacy and security often do not create a private right of action, the failure to comply with such requirements is often asserted in third-party lawsuits as evidence of inadequate security, particularly when the company's privacy notice represents that it is in compliance with applicable legal and regulatory requirements.

1. State Data Privacy and Security Requirements

In an effort to protect individuals' privacy and to reduce the risk of identity theft, many states have enacted laws and many state regulatory bodies have promulgated regulations imposing obligations on entities that obtain and/or maintain Personal Information. These laws and regulations are intended to protect Personal Information and, in the event of a breach, to require notification to

---

[194] Cisco Visualization, T*he Internet of Things*, http://share.cisco.com/internet-of-things.html

government agencies and to individuals whose Personal Information has been or may have been subject to unauthorized access or acquisition.

a. Restrictions on Collection of Personal Information

In recognition of both privacy considerations and the data breach risks inherent in companies' collection of large amounts of information about individuals, regulatory and legislative scrutiny (and that of class action lawyers) has increasingly focused on the business practices of collection of information about individuals. As discussed above with regard to the California example, that has meant increased focus on the disclosure of practices regarding the collection and usage of Personal Information. There are also statutory restrictions in several states that limit not only the usage and disclosure of Personal Information, but also the right to collect that information in the first place.

Collection of customer information by retailers in connection with credit card transactions (usually for marketing uses) has become a focus of attention by courts as well as legislatures. Numerous states have statutes that restrict the right of retailers to record information such as addresses and telephone numbers of customers in connection with credit card transactions, if that information is not required by the credit card companies or otherwise necessary for, *e.g.*, shipping or installation.[195] Recently, the highest appellate courts of California and Massachusetts held those states' statutes to restrict the right of retailers to collect ZIP codes of customers in connection with credit card transactions under certain circumstances and subject to certain exceptions.[196]

Other states have even greater restrictions on collection of information obtained during credit card transactions, as that data is so often the target of breaches. Minnesota law, for example, prohibits companies transacting business in Minnesota from retaining security codes, PIN verification numbers, or the full contents of any track of magnetic stripe data following authorization of a credit card transaction, and for longer than 48 hours following authorization of a PIN debit transaction.[197]

Companies collecting credit card information are also subject to collection and retention restrictions imposed by card brand regulations, such as Visa and MasterCard, and pursuant to PCI-DSS (as discussed below).[198]

In addition, a number of states restrict collection of Personal Information through scanning or swiping of the magnetic stripe or bar code of a state-issued identification card or driver's license under certain circumstances and subject to certain exceptions.[199] Personal Information obtained through such means is also subject to use restrictions under the laws of certain states.[200]

b. Protection of Social Security Numbers

---

195 *See, e.g.*, Cal. Civ. Code §1747.08(b).

196 See section on The Expanding Definition of Personal Information, *supra.*

197 *See* Minn. Stat. 325E.64.

198 See section on Industry Standards, *infra*.

199 *See, e.g.*, Ga. Code Ann. § 40-5-120(5); Haw. Rev. Stat. § 487J-6.

200 *See, e.g.*, Haw. Rev. Stat. § 487J-6.

Social Security numbers have become a prime target of data thieves. Unlike debit and credit card numbers, Social Security numbers are difficult to change and can be used to obtain additional documentation for identity theft purposes potentially far more profitable for the thief and damaging to the victim than a discrete number of fraudulent transactions. Hackers are reportedly focusing on the Social Security numbers of children, which are generally not yet in use by the holders to obtain credit and thus are not associated with a tarnished credit history.[201] Breaches involving Social Security numbers are also of concern to law enforcement agencies charged with state and national security, due to their potential use as identification for nefarious purposes including evading law enforcement and national security authorities, and gaining entry to the U.S. under assumed identities.

Many states impose specific requirements governing the handling of Social Security numbers. For example, a Connecticut law requires any person or entity that collects Social Security numbers to create a protection policy specifically related to Social Security numbers.[202] The company policy, which must be published or publicly displayed (such as on the company's website), must protect confidentiality, prohibit unlawful disclosure, and limit access to Social Security numbers.

New York has also enacted legislation limiting the disclosure, transmission and printing of Social Security numbers.[203] The law limits the collection of Social Security numbers and restricts the ability of private entities to require an individual to provide his or her Social Security number or any number derived from that number (with certain exceptions, such as if "requests for purposes of employment," for confirming the individual's age to allow him or her access to a marketing program restricted to individuals of a certain age, or by a banking institution). While the statute is fairly detailed, there are still unanswered questions as to the scope of its application. Other states have also enacted laws and regulations to protect the Social Security numbers and other Personal Information of their residents.[204]

c. Record Disposal Requirements

Many states also regulate the disposal of records containing Personal Information. For example, under Massachusetts and New York law, records containing Personal Information must be redacted, burned, pulverized, shredded or destroyed in some other way that will render the data unreadable. In Massachusetts, if third parties are contracted to dispose of such records, they must implement policies and procedures that prohibit unauthorized access to or use of Personal Information during collection, transport and disposal. Both states impose fines for noncompliance.[205]

Companies that dispose of records containing Personal Information also need to consider whether they are subject to disposal requirements imposed by federal law. The Fair and Accurate Credit Transactions Act of 2003, for example, requires businesses and individuals that use consumer

---

201 *Thieves target children's Social Security numbers*, Chicago Sun-Times, Aug. 3, 2010; *see also, Federal Trade Commission, Child Identity Theft*, available at http://www.consumer.ftc.gov/articles/0040-child-identity-theft.

202 Conn. Gen. Stat. § 42-471.

203 N.Y. Gen. Bus. Law § 399-ddd.

204 *See, e.g.*, Cal. Civ. Code § 1798.85; Mich. Comp. Laws § 445.84; Or. Rev. Stat. § 646A-620; Tex. Bus. & Com. § 501.

205 Mass. Gen. Law ch. 93I § 2; N.Y. Gen. Bus. Law § 399-h.

reports, such as lenders, insurance companies, employers, landlords, car dealers, and debt collectors, to properly dispose of those consumer reports.[206]

d. Data Breach Notification Requirements

In the event of a data breach involving unauthorized access to Personal Information, state laws and regulations in most U.S. jurisdictions mandate notice of the breach to affected individuals, and some states also require reporting to regulatory agencies and state attorneys general. Vast numbers of individuals may be involved in a single breach, and large breaches frequently affect residents of many jurisdictions.

Fifty-one U.S. jurisdictions, including 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted data breach notification laws.[207] These laws specify the steps that a company must take in response to a breach that affects its residents. Although the data breach notification laws of each of the 51 jurisdictions are similar, they are not identical. Upon a breach or potential breach of data security, the affected company must carefully review the requirements of each applicable jurisdiction to determine its obligations in that particular jurisdiction.[208] As further discussed below, the various laws purport to apply based on the residence of the individual whose data was compromised, and are not limited by the company's place(s) of business.[209] Often, even most "local" businesses find that they collect data from residents of multiple jurisdictions.

In addition to such state data breach notification requirements, companies in certain industries, such as banking,[210] credit unions,[211] insurance,[212] telecommunications,[213] and health care,[214] are also subject to industry-specific breach notification requirements, while still other industry regulators

---

206 15 U.S.C. § 1681w(a)(1); *see also* 69 Fed. Reg. 68690-01 (Nov. 24, 2004), codified at 16 C.F.R. § 682.

207 As of Apr. 30, 2014, the states that do not yet have such notification laws are Alabama, New Mexico and South Dakota.

208 A list of jurisdictions and links to their data breach notification laws is available at http://www.ncsl.org/research/telecommunications-and-information-technology/2014-security-breach-legislation.aspx#1

209 The Texas breach notification statute requires companies that conduct business in Texas to notify residents of other states that do not require notice. *See* Tex. Bus. & Com. Code Ann. § 521.053.

210 *See, e.g.*, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notices, issued by the Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; and Office of Thrift Supervision, Treasury, interpreting section 501(b) of the Gramm-Leach-Bliley Act and Interagency Guidelines Establishing Information Security Standards.

211 Guidelines for Safeguarding Member Information promulgated by the National Credit Union Administration (12 C.F.R. 748 and Appendices).

212 *See, e.g.*, Connecticut Insurance Department Bulletin IC-25, Aug. 18, 2010.

213 47 C.F.R. § 64.2011.

214 *See* federal Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") (42 U.S.C. § 201 et seq.), the Health Information Technology for Economic and Clinical Health ("HITECH") Act, as amended, and implementing regulations, requiring notice to affected individuals, the U.S. Department of Health and Human Services ("HHS"), and in some cases, the media, in the event of a breach of protected health information ("PHI"); *see also* Federal Trade Commission (the "FTC") Health Breach Notification Rule, 16 C.F.R. Part 318, requiring notification to affected individuals, the FTC and in some cases, the media, by vendors of personal health records ("PHR") and PHR-related entities in the event of a data breach involving PHR. Such requirements are discussed further in Section III(2)(f) below. In addition, certain states impose specific notification requirements upon health care providers in addition to the general state breach notification requirements (*see* Cal. Health Safety Code § 1280.15, requiring agency and individual notice within five days of discovery).

have issued guidance relating to breach response.[215] The definitions of a reportable incident under these requirements often differ from the general data breach notification requirements, requiring additional levels of analysis and response in the event of an incident. U.S. federal and state governmental entities are subject to separate data breach notification requirements for breaches of data in their possession or databases.

In the event of a data breach, an initial and major task is to identify which jurisdictions' requirements apply. Entities often find themselves subject to the different, sometimes conflicting, requirements of multiple jurisdictions. A single data breach incident may have only one location at which the entity's data security was breached. Nevertheless, the individuals affected by the breach may reside in many different jurisdictions that impose data breach notification requirements, some of which may not be limited to companies doing business in the jurisdiction. For example, if a laptop stolen from an office in Florida contains the Personal Information of residents of Maine, Massachusetts, New Hampshire and Vermont, then the data breach laws of all those states, as well as Florida, may be triggered. In the event of a breach of a database or loss of computerized records containing information of individuals residing in different locations, the notification requirements of all U.S. states and other jurisdictions with such requirements are potentially triggered.

Typically, the applicability of notice requirements of a given jurisdiction depends on several factors:

- whether the type of information that has been lost, stolen or misplaced falls within the jurisdiction's definition of "Personal Information";
- whether there has been a "breach of the security of the system" (or similar defined term) under the jurisdiction's definitions and requirements;
- whether the incident meets the jurisdiction's threshold of harm or likelihood of harm, if any; and
- whether any threshold number (often one) of individuals whose Personal Information was accessed are residents of the jurisdiction.

Not all jurisdictions have the same definitions or triggers. For example, some jurisdictions define a "breach" that requires notification to include unauthorized "access" to Personal Information, while others may require notification in the event of unauthorized "acquisition" or "misuse" of Personal Information. Further, certain jurisdictions only require notice where a specific harm threshold has been met, while others do not have any threshold for harm or likelihood of harm.

The data breach notification statutes of each relevant jurisdiction must be analyzed to determine whether:

- Residents of the jurisdiction must be notified;

---

[215] *See, e.g.*, U.S. Department of Education Data Breach Response Checklist, September 2012, providing guidance for educational agencies and institutions, available at http://ptac.ed.gov/document/checklist-data-breach-response-sept-2012.

- Notices to affected individuals must contain specific content (or are prohibited from containing certain information, such as in Massachusetts, which prohibits notices from including the nature of the breach, while others require the disclosure of such information);

- State attorneys general and other state agencies must be notified and, if so, whether those notices must include specific content and/or be provided in advance of notification to affected individuals; and

- Credit reporting agencies, such as Experian, TransUnion and Equifax, must be notified.

Certain states require that notices to affected individuals include specific content, such as:

- A general description of the breach;

- The type of Personal Information exposed;

- Contact information for the major credit reporting agencies;

- The company's contact information; and

- Advice to remain vigilant by reviewing account statements and credit reports.

In contrast, Massachusetts *prohibits* the disclosure of the nature of the breach.

Time is of the essence with regard to such notifications, which may be required as early as five days following discovery of a breach.[216] Many breach notification statutes do not specify a fixed number of days by which notice is required, but instead require notice "as soon as practicable and without unreasonable delay" (or similar language). Affected individuals frequently identify timeliness of notification as a significant factor in their assessment of a breached entity's response to a data security incident. Governmental agencies may impose fines for delays, and certain states, such as Florida, outline specific penalties up to $500,000 where notice is not provided to affected individuals within 45 days, as required by Florida law.[217]

The California Attorney General filed and reportedly settled a lawsuit against Kaiser Foundation Health Plan, Inc. in early 2014, alleging that Kaiser failed to issue breach notification to affected individuals "in the most expedient time possible and without unreasonable delay" in violation of Cal. Civ. Code § 1798.82 (which does not specify a fixed number of days by which notice is required) where Kaiser had identified a portion of the affected group in December 2011, continued to investigate and identify additional individuals through February, and ultimately issued notices in

---

[216] *See* Cal. Health Safety Code § 1280.15; Connecticut Insurance Department Bulletin IC-25, Aug. 18, 2010.

[217] *See* Fla. Stat.§ 817.5681, requiring notice to affected individuals no later than 45 days following determination of a breach, and imposing a fine of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days, with a maximum fine of $500,000.

March 2012. According to the complaint, Kaiser had sufficient information to identify and notify at least some individuals affected by the breach between December 2011 and February 2012.

e. Data Security Requirements: Massachusetts Remains at the U.S. Forefront

Massachusetts, through its Office of Consumer Affairs and Business Regulation ("OCABR"), has promulgated one of the most comprehensive U.S. regulatory schemes for data privacy and security. The regulation, which went into effect March 1, 2010, set a new U.S. state standard for data protection.

The Massachusetts data security regulation (201 C.M.R. 17.00, the "Massachusetts Regulation") applies to any individual or company, regardless of type, size or location, that owns or licenses Personal Information of Massachusetts residents. Under the Massachusetts Regulation, Personal Information includes the name of a Massachusetts resident together with his or her Social Security number, or driver's license, financial account, or credit card number (with or without PIN). Any entity, including insurance companies, producer entities and service providers, that uses or stores the Personal Information of Massachusetts residents, whether of employees, customers, insureds, or others, is subject to the Massachusetts Regulation.[218]

The Massachusetts Regulation establishes the most rigorous state data security requirements in the U.S. to date. To comply, companies that own or license the Personal Information of Massachusetts residents are required to adopt a comprehensive written information security program (referred to as a "WISP") that satisfies specific requirements, including the following:

- Identify and evaluate internal and external risks;
- Regularly monitor employee access to Personal Information;
- Prevent terminated employees from accessing documents, devices and other records that contain Personal Information;
- Take reasonable steps to select and retain third-party service providers that are capable of compliance with the Massachusetts Regulation;
- Review security measures annually, and update the WISP when there is a material change in business operations;
- Develop and maintain a procedure for actions to take in response to any breach of security;
- Train employees about and discipline employees for violation of the policy; and
- Designate one or more employees to maintain, supervise and implement the WISP.

[218] The extraterritorial authority of the OCABR and the Massachusetts Attorney General to enforce the Massachusetts Regulation against companies located outside Massachusetts borders is yet to be fully tested.

The WISP must also address the establishment and maintenance of a detailed computer security program as to Personal Information of Massachusetts residents, including, to the extent technically feasible:

- Encryption of all transmitted records and files containing Personal Information that are stored on laptops and other portable devices and/or will travel across public networks or wirelessly;

- User-authentication protocols and access-control measures, including control over user identifiers, passwords and access;

- A system for monitoring unauthorized use; and

- Up-to-date firewalls, anti-virus definitions and anti-malware programs.

In an effort to ease the burden imposed on small businesses, the Massachusetts Regulation makes clear that its requirements are risk-based in both implementation and enforcement, stressing that there is no one-size-fits-all WISP. The Massachusetts Attorney General will judge compliance on a case-by-case basis, taking into account the following factors: (i) the size, scope and type of business handling the information; (ii) the amount of resources available to the business; (iii) the amount of data stored; and (iv) the need for security and confidentiality of both consumer and employee information.

This risk-based approach brings the Massachusetts Regulation in line with both the enabling legislation and applicable federal law, including two rules promulgated by the FTC: (i) the Red Flags Rule that requires creditors and financial institutions to have a written Identity Theft Prevention Program to detect warning signs of identity theft and fraud; and (ii) the Gramm-Leach-Bliley Safeguards Rule (16 C.F.R. Part 314), which requires financial institutions to have a security plan to protect personal consumer information (both discussed below).

The Massachusetts Regulation also requires that companies oversee their third-party vendors by:

(i) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such Personal Information consistent with these regulations and any applicable federal regulations; and

(ii) Requiring by contract that such third-party service providers implement and maintain such appropriate security measures for Personal Information.

Contracts with third-party service providers entered into prior to March 1, 2010 are required to have been amended by March 1, 2012 to satisfy the Massachusetts Regulation.

In Frequently Asked Questions ("FAQs") published in November 2009,[219] the OCABR made the encryption requirement imposed by the Massachusetts Regulation flexible. Consistent with the risk-based approach of the Massachusetts Regulation, the encryption requirement is technology-neutral in that it does not require specific encryption technology.

The FAQs clarify other important issues as well, including the following:

- A bank or credit card account is a "financial account" which, when accompanied by the name of a Massachusetts resident, is subject to the Massachusetts Regulation.

- An account that is not clearly a financial account is considered a financial account if unauthorized access could result in an increase of financial burden or a misappropriation of monies, credit or other assets.

    - An insurance policy number is a financial account number if it (i) grants access to a person's finances, or (ii) could result in an increase of financial burden, or a misappropriation of monies, credit or other assets.

    - Compliance with HIPAA does not eliminate a company's obligation to comply with the Massachusetts Regulation if the company owns or licenses Personal Information of a Massachusetts resident.

Companies, especially small businesses that are subject to the Massachusetts Regulation, have voiced concerns about the burden and cost of compliance. The OCABR, however, has taken the position that the importance of protecting residents' Personal Information outweighs the financial burden on even small businesses that may need to retain outside consultants to help them institute the required procedures.

The Massachusetts Attorney General's Office has signaled that it will be taking a hardline approach to enforcement of its consumer protection and privacy and data security requirements. In May 2012, the Massachusetts Attorney General reported resolving a suit it had filed against a hospital that reportedly shipped several boxes of unencrypted back-up tapes containing individuals' names, Social Security numbers, financial account numbers and health information to a service provider, which then were reported missing. The suit alleged violation of both the Massachusetts Consumer Protection Act and HIPAA. A consent judgment, announced in May 2012, included a $750,000 payment, including a $250,000 civil penalty, a $225,000 payment for an educational fund to be used by the Attorney General to promote education concerning the protection of Personal Information and Protected Health Information, and a credit of $275,000 to the hospital to reflect security measures it took subsequent to the breach. The Attorney General reported that the hospital also agreed to take a variety of steps, including a review and audit of security measures. This case also demonstrates the importance placed by the Massachusetts Attorney General on both data security

---

[219] The FAQs and other guidance related to the Massachusetts Regulation are available at: http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf.

procedures in place prior to the breach and responsiveness in addressing issues resulting from a breach.[220]

Significantly lesser fines have issued in situations where there was no evidence of unauthorized access to Personal Information, but fines were nonetheless issued where information was unencrypted in violation of the Massachusetts Regulation.

The Massachusetts Attorney General has also indicated that it will scrutinize an entity's response to a breach and will consider whether the breached entity complied with the Payment Card Industry Data Security Standards if there has been a breach of credit card numbers. In March 2011, it announced that the owner of a group of popular restaurants in Massachusetts agreed to pay a $110,000 fine in connection with a data breach that allegedly affected over 125,000 credit and debit card holders. The Attorney General's focus was on the reported fact that a forensic investigator was not engaged until three weeks after the restaurant was informed by credit card processors of a potential breach, and that the restaurant continued to accept credit and debit cards for several weeks after it allegedly knew or had reason to know that its security had been breached. The complaint also alleged that the restaurant had failed to comply with Payment Card Industry Data Security Standards and that it did not have other necessary data security precautions in place to protect its customer data.[221]

f. New Trends in State Regulation: Social Media

Social media is an increasing source of concern to regulators, both as a source of information about individuals that can be culled by employers and other businesses investigating individuals, and as a target for hackers.

Out of concern that applicants and employees will be required to provide access to their social media accounts, several states have recently enacted legislation regulating access by employers and/or educational institutions to individuals' social media accounts, with similar legislation pending in over two dozen others.[222] For example, effective January 1, 2013, California law restricts companies from requesting or requiring that current or potential employees provide their social media account login credentials, access personal social media in the presence of the employer, or divulge any personal social media.[223] California law also imposes similar restrictions upon public and private colleges and universities located in the state with regard to social media of current or potential students,[224] and requires that private colleges and universities post their social

---

220 *South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations*, Press Release of Attorney General Martha Coakley, May 24, 2012, http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html.

221 See Edwards Wildman Palmer LLP Client Advisory, *Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?* Apr. 2011, http://www.edwardswildman.com/newsstand/detail.aspx?news=2322.

222 As discussed above in Section on Social Media, according to NCOIL, the National Conference of State Legislatures, as of May 2014, states that have enacted such legislation intended to protect the privacy of prospective and current employees (and in some states a student) include, as of May 2014, Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, Maine, New Mexico, Oregon, Utah, Vermont, Washington and Wisconsin, www.ncsl.org.

223 Cal. Lab. Code § 980.

224 Cal. Educ. Code § 99120.

media privacy policies on the college or university's website.[225] Such restrictions are subject to limited exceptions, such as where social media is reasonably believed to be relevant to an investigation of allegations of employee misconduct, so long as the social media is used solely for purposes of that investigation or related proceedings.[226] (See discussion above entitled Social Media as Source of Statutory and Regulatory Violations for a discussion of pertinent case law, and federal as well as state scrutiny of employer and university requirements that applicants, employees and/or students provide access to their social media accounts; see also examples of data breaches involving social media.)

2. Federal Requirements

In addition to state laws and regulations, entities may also be subject to federal rules and regulations mandating privacy and protection of Personal Information, and requiring that certain steps be taken in the event of a data breach. The FTC currently asserts broad authority to regulate unfair or deceptive acts or practices relating to privacy and data protection.[227] Financial institutions are subject to specific federal requirements and, for these purposes, the term "financial institutions" is defined very broadly. Public companies may also need to disclose cyber risks and incidents as part of their mandated disclosure of material information to potential investors. A number of federal acts and regulations, such as the Fair Credit Reporting Act ("FCRA"),[228] also require protection of consumer information, depending on the nature of the entity involved, the type of information disclosed, and the circumstances. Health information is also subject to federal protections under HIPAA and the HITECH Act, as further discussed below.

a. FTC Regulation of Privacy and Data Protection

Section 5 of the Federal Trade Commission Act, which applies to almost all companies engaged in interstate commerce in the United States, prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC has brought numerous privacy and data security enforcement actions against companies pursuant to such authority for (i) failure provide appropriate data security to reasonably protect customer information, which the FTC has interpreted to constitute an "unfair act or practice;" and/or (ii) non-compliance with the companies' privacy policies or representations regarding security, which the FTC has interpreted to constitute a "deceptive act or practice."

The FTC has brought such enforcement actions against, e.g., software vendors (Microsoft[229] and Guidance Software[230]), consumer electronics companies (Genica and Computer Geeks),[231] mobile

---

225 Cal. Educ. Code § 99122.

226 *See, e.g.*, Cal. Lab. Code § 980(c).

227 See Edward F. Glynn, Jr. and Lisa Simmons, *Edwards Wildman Client Advisory- Court Finds FTC Has Section 5 Unfairness Authority to Bring Enforcement Action Against Hotel Chain Victimized By Cyber Intrusion*, April 9, 2014, http://www.edwardswildman.com/court-finds-ftc-has-section-5-unfairness-authority-04-09-2014/

228 FCRA (15 U.S.C. §1681, et seq.) regulates "Credit Reporting Agencies" and imposes certain restrictions and notice requirements on the production and use of consumer reports. The FTC found in January 2013 that an app developer offering criminal record searches for the cost of downloading a 99 cent app was a Credit Reporting Agency subject to FCRA and charged the developer with three violations of that law. In the Matter of Filiquarian Publishing, LLC, No. 112 3195, Federal Trade Commission, Agreement Containing Consent Order (Jan. 10, 2013).

229 FTC v. Microsoft (Consent Decree, Aug. 7, 2002), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm

app developers (Delta Airlines),[232] clothing retailers (Guess![233] and Life Is Good[234]), music retailers (Tower Records),[235] animal supply retailers (PetCo),[236] general merchandise retail stores (BJs Wholesale,[237] TJX companies,[238] and Sears[239]), shoe stores (DSW),[240] entertainment establishments (Dave & Busters[241]), social media sites (Twitter[242] and Facebook[243]), and hotels (Wyndham).[244]

Two cases winding their way through the courts challenge the FTC's authority to regulate privacy and data protection pursuant to Section 5 of the FTC Act. The first arises from a complaint that the FTC filed against Wyndham Worldwide Corporation in 2012, in which the FTC charged that Wyndham violated the FTC Act's prohibition on unfair and deceptive practices by failing to secure customer information according to Wyndham's privacy policy.[245] Wyndham argued that the FTC lacks the authority to regulate data security, and that it failed to satisfy fair notice principles because it had not issued any regulations concerning data security before bringing it unfairness claim. In April 2014, a federal court sitting in New Jersey rejected Wyndham's arguments when it denied Wyndham's motion to dismiss the FTC complaint and permitted the FTC's case against Wyndham

---

230 In the Matter of Guidance Software (Agreement Containing Consent Order, FTC File No. 062 3057, November 16, 2006), available at www.ftc.gov/opa/2006/11/guidance.htm

231 In the Matter of Genica Corporation, and Compgeeks.com, FTC File No. 082-3113 (Agreement Containing Consent Order, February 5, 2009), available at http://www.ftc.gov/enforcement/cases-proceedings/082-3113/gencia-corporation-compgeekscom-also-dba-computer-geeks

232 See, "California Attorney General Sues Delta Air Lines for Failing to Have a Mobile App Privacy Policy," at http://bit.ly/W11J4T

233 In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260**,** June 18, 2003), available at www.ftc.gov/os/2003/06/guessagree.htm

234 *In the Matter of* Life is good, Inc. (Agreement Containing Consent Order, FTC File No. 072 3046, January 17, 2008), available at www.ftc.gov/os/caselist/0723046

235 In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209**,** Apr. 21, 2004), available at www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf

236 In the Matter of Petco Animal Supplies, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 7, 2004), available at http://www.ftc.gov/enforcement/cases-proceedings/032-3221/petco-animal-supplies-inc-th-matter

237 In the Matter of BJ's Wholesale Club, Inc. (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), available at www.ftc.gov/opa/2005/06/bjswholesale.htm

238 In The Matter of The TJX Companies, Inc., FTC File No. 072-3055 (Agreement Containing Consent Order, March 27, 2008), available at www.ftc.gov/os/caselist/0723055

239 In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Agreement Containing Consent Order, September 9, 2009), available at http://www.ftc.gov/os/caselist/0823099/index.shtm

240 In the Matter of DSW Inc., (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), available at www.ftc.gov/opa/2005/12/dsw.htm

241 In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153 (Agreement Containing Consent Order, March 25, 2010), available at http://www.ftc.gov/os/caselist/0823153/index.shtm

242 In the Matter of Twitter, Inc., FTC File No. 092 3093 (Agreement Containing Consent Order, June 24, 2010; Decision and Order, March 11, 2011), available at http://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation

243 In the Matter of Facebook, Inc., File No 092 3184 (Agreement Containing Consent Order, November 29, 2011), available at http://ftc.gov/os/caselist/0923184/index.shtm

244 *FTC v. Wyndham Hotels*, (PENDING Lawsuit filed 6/26/2012 http://www.ftc.gov/opa/2012/06/wyndham.shtm)

245 FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information, Federal Trade Commission, Press Release, June 26, 2012, http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect

to move forward.[246] The second case, involving LabMD, began as an enforcement action by the FTC on similar grounds, and by 2014 had generated challenges by LabMD to the FTC's authority in several administrative and court proceedings. While challenges to the FTC's authority to bring enforcement actions based on issues of adequacy of a company's privacy and data security procedures have so far been largely unsuccessful, LabMD did obtain one victory over the FTC in a May 2014 decision by an administrative law judge ordering the FTC to provide deposition testimony as to what data security standards, if any, that the FTC has published and intends to rely upon at trial to demonstrate that LabMD's data security practices were not reasonable or appropriate and in violation of Section 5 of the FTC Act. [247]

b. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") was enacted in 1999 to reform the financial services industry and address concerns relating to consumer financial privacy. Title V of GLBA establishes a minimum federal standard of privacy for consumer non-public personal information and applies to financial institutions, including companies that were not traditionally considered to be financial institutions, such as insurance companies.[248] Prominent among the privacy requirements of the GLBA and the regulations promulgated thereunder are requirements that financial institutions (i) develop and adopt privacy and information security policies and practices, and (ii) send annual privacy notices to customers.

GLBA required the state and federal governmental agencies that regulate financial institutions to promulgate regulations to effectuate GLBA.[249] Thus, a number of agencies issued privacy and data security regulations pursuant to GLBA, applicable to financial institutions subject to their

---

246 *Federal Trade Commission v. Wyndham Worldwide Corp.*, 13-cv-01887, U.S. District Court, District of New Jersey (Newark). *See* Edwards Wildman Palmer LLP Client Advisory, *Court Finds FTC Has Section 5 Unfairness Authority To Bring Enforcement Action Against Hotel Chain Victimized By Cyber Intrusion*, April 2014, http://www.edwardswildman.com/Court-Finds-FTC-Has-Section-5-Unfairness-Authority-04-09-2014/

247 *In the Matter of LabMD, Inc.*, FTC Matter/File No. 102-3099, FTC Docket No. 9357, see May 1, 2014 order. *See LabMD, Inc. v. Federal Trade Commission*, 1:12-cv-3005-WSD, United States District Court for the Northern District of Georgia, Atlanta Division; *LabMD Inc. v. Federal Trade Commission*, Case No. 3-15267, United States Court of Appeals for the Eleventh Circuit. The FTC suit against LabMD was scheduled to go to trial in May 2014. *See also LabMD challenges FTC data security action in new lawsuit, Grant Gross*, PC World, Mar. 21, 2014, http://www.pcworld.com/article/2110840/labmd-challenges-ftc-data-security-action-in-new-lawsuit.html; Allison Grande, *11th Circ. Blow Prompts LabMD to Drop FTC Fight for Now*, Law360, February 25, 2014, http://www.law360.com/articles/513110/print?section=appellate; Allison Grande, *FTC Told to Reveal Data Security Expectations In LabMD Suit*, Law360, May 2, 2014, http://www.law360.com/articles/534075/print?section=health; Allison Grande, *LabMD Ruling Puts FTC in Driver's Seat on Data Security*, Law360,May 13, 2014, http://www.law360.com/articles/537543/print?section=corporate.

248 *See http://www.ftc.gov/privacy/privacyinitiatives/glbact.html* on the applicability of Title V of GLBA to insurance companies.

249 15 U.S.C. § 6801-6809.

jurisdiction, including banks,[250] registered investment advisors and broker dealers,[251] credit unions,[252] insurance companies,[253] and others.[254]

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") transferred rulemaking authority over privacy provisions of GLBA from the following regulatory agencies to the newly created Consumer Financial Protection Bureau (the "CFPB") effective July 2011: the FTC, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of Currency, and Office of Thrift Supervision.[255] The SEC, the Commodity Futures Trading Commission, and state insurance departments continue to regulate GLBA with respect to the financial institutions subject to their jurisdiction, and the FTC retains limited jurisdiction with respect to GLBA.

In light of the transfer of GLBA privacy rulemaking authority to the CFPB, the CFPB published an interim final rule in December 2011 establishing a new Regulation P (Privacy of Consumer Financial Information), combining content of existing regulations previously promulgated by the FTC and banking regulators, and including technical and conforming changes to reflect the transfer of authority to CFPB and certain other changes made by the Dodd-Frank Act.[256]

On May 6, 2014, the CFPB issued a proposed amendment to Regulation P that would allow financial institutions that do not engage in certain types of information-sharing activities to stop mailing an annual privacy notice to consumers if they post the annual notices on their websites and meet certain other conditions.[257]

i. Regulation S-P and SEC Enforcement of Privacy, Data Protection and Cybersecurity

Regulation S-P, promulgated by the SEC pursuant to the GLBA, implements the privacy and data protection requirements of the GLBA with respect to financial institutions subject to SEC jurisdiction, including registered investment advisers and broker-dealers.[258] Subject to limited exceptions, Regulation S-P requires such entities to issue privacy notices to consumers regarding their privacy policies and practices and include the categories of information collected and disclosed; to whom information might be disclosed; an explanation of the consumer's right to opt

---

250 *E.g.*, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" dated March 30, 2005 issued jointly by the five member agencies of the Federal Financial Institutions Examination Council – the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of Currency, and Office of Thrift Supervision.

251 SEC Regulation S-P, 17 C.F.R. Part 248.

252 National Credit Union Administration regulations, 12 C.F.R. Part 748.

253 Most state insurance departments have promulgated regulations implementing GLBA with respect to their licensees that are subject to GLBA, in most cases based upon model regulations issued by the National Association of Insurance Commissioners.

254 *E.g.*, FTC Privacy Rule (16 C.F.R. Part 313) and Safeguards Rule (16 C.F.R. Part 314).

255 Pub. L. No. 111-203, section 1061(a)(1).

256 12 C.F.R. Part 1016.

257 CFPB statement and proposed amendment available at http://www.consumerfinance.gov/newsroom/cfpb-proposes-rule-to-promote-more-effective-privacy-disclosures/

258 17 C.F.R. Part 248.

out of certain disclosures; and policies and practices for protecting the confidentiality, security, and integrity of nonpublic personal information. Regulation S-P also requires registered investment advisers and broker-dealers regulated by the SEC to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information, and impose requirements for secure disposal of consumer reports, as defined by the Fair Credit Reporting Act. Related SEC Regulations S-AM and S-ID impose limitations on affiliate marketing, and impose duties regarding the detection, prevention and mitigation of identity theft pursuant to the Red Flags Rule.

In April 2011, the SEC announced that it had, for the first time, assessed financial penalties against individuals charged solely with violations of Regulation S-P.[259] According to the SEC, the fine was assessed pursuant to an SEC investigation that found that while a broker-dealer was winding down its business operations in 2010, its former president and former national sales manager violated customer privacy rules by improperly transferring customer records to another firm. The SEC also found that the former chief compliance officer failed to ensure that the firm's policies and procedures were reasonably designed to safeguard confidential customer information.

Following a Cybersecurity Roundtable held by the SEC in late March 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced that it will be conducting examinations of more than 50 registered broker-dealers and investment advisors. In a Cybersecurity Initiative Risk Alert issued by OCIE in connection with the announcement, OCIE stated that its investigations will be designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats. OCIE included in the Risk Alert a sample request for information and documents.[260]

ii. SEC Guidance Regarding Public Company Obligations to Disclose Cyber Security Risks and Incidents to Investors

Public companies need to assess their exposure to cyber risks and the procedures they take and costs they incur in preventing cyber incidents as part of their overall assessment of matters that can have a material effect on their company's operations or financial condition.

In October 2011, the Division of Corporation Finance of the Securities and Exchange Commission (the "SEC") issued guidance that identifies cyber risks and incidents as potential material information to be disclosed under existing securities law disclosure requirements and accounting standards (the "Disclosure Guidance").[261] While the Disclosure Guidance states that it represents the views of the Division of Corporation Finance and is "not a rule, regulation or statement of the

---

[259] The SEC press release is available at: http://www.sec.gov/news/press/2011/2011-86.htm.

[260] The Cybersecurity Initiative Risk Alert is available here: http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf

[261] Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity, Oct. 13, 2011, available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. *See also* Edwards Wildman Palmer LLP Client Advisory, *Public Companies May Need to Disclose their Exposure to Material Cyber Risks According to New Guidance Issued by SEC Division of Corporation Finance*, http://www.edwardswildman.com/newsstand/detail.aspx?news=2634.

Securities and Exchange Commission," public companies can now expect the SEC to review their filings to determine whether cyber risks and incidents are adequately disclosed.

Federal regulations and guidance issued by other agencies in recent years have largely focused on identifying data security risks that would affect consumers. This Disclosure Guidance, however, is directed at protecting investors and encouraging companies to assess their risks of cyber incidents and review the adequacy of their disclosures as to those risks and their impact on a company's operations, liquidity and financial condition. A broad range of factors are identified in the Disclosure Guidance for consideration, including prior cyber incidents, business operations and outsourced functions that have material cyber risks and potential costs and consequences, and relevant insurance coverage purchased by the company to address its exposures. Public companies now have a blueprint for assessing their cyber risk exposures, and for determining their reporting obligations as to material exposures, along with the context for evaluating such disclosures.

The Disclosure Guidance was promulgated following a May 11, 2011 letter to the SEC from five members of the Senate, including John D. Rockefeller IV, Chairman of the U.S. Senate Committee on Commerce, Science, and Transportation. That letter expressed concern that "a substantial number of companies do not report their information security risk to investors," and that "once a material network breach has occurred, leaders of publicly traded companies may not fully understand their affirmative obligation to disclose information . . . ." As a result, the Senators requested that the SEC "publish interpretative guidance clarifying existing disclosure requirements pertaining to information security risk . . . ."[262]

The Disclosure Guidance was drafted to assist companies preparing disclosures required under U.S. federal securities laws (such as registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934) to assess whether they have a cyber risk exposure that should be disclosed.

Companies are increasingly reporting cyber attacks and risks in their SEC filings, but even those with breaches reportedly often include statements that there were no material financial losses. [263]

c. Federal Trade Commission "Red Flags" Rule

The FTC and other federal agencies that regulate financial institutions, including the Federal Reserve Board, National Credit Union Administration, Office of the Comptroller of Currency and Securities and Exchange Commission, have issued regulations to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").[264]

---

[262] Senator Rockefeller sent a similar letter on April 9, 2013 asking the SEC to elevate the cybersecurity guidance to the Commission level, rather than the staff level (as noted, the current guidance was issued by the Division of Corporation Finance), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51.

[263] See, Chris Strohm, Eric Engleman, Dave Michaels, *Cyberattacks Abound Yet Companies Tell SEC Losses Are Few*, Bloomberg, Apr. 3, 2013, http:// www.bloomberg.com/news/print/2013-04-04/; Eamon Javers, *Cyberattacks: Why Companies Keep Quiet*, CNBC Washington Reporter, Feb. 25 2013, www.cnbc.com/id/100491610.

[264] Pub. Law 108-59, codified at 15 U.S.C. § 1681 *et seq.*

FACTA is federal legislation directed at protecting consumers against identity theft as well as enhancing the accuracy of consumer report information. It prohibits businesses from printing out more than five digits of a credit card number, and allows consumers to obtain a free credit report every 12 months from each of the nationwide credit reporting agencies.

The regulations, which are commonly referred to as the Red Flags Rule (the "Rule"),[265] require covered entities to develop and implement a written Identity Theft Prevention Program to detect the warning signs – the "red flags" – of identity theft in order to prevent and mitigate identity theft. The Rule applies to "financial institutions" and "creditors" that maintain "covered accounts," as those terms are defined by the Rule. The FTC's enforcement of the Rule was effective December 31, 2010 with regard to all covered entities.

On April 10, 2013, however, the SEC and Commodity Futures Trading Commission ("CFTC") jointly adopted rules and guidelines to transfer responsibility for promulgating and enforcing the Red Flags rule from the FTC to the SEC and the CFTC with respect to the entities they regulate. This includes SEC-registered investment advisers, broker-dealers, or mutual funds and CFTC regulated futures commodity merchants, commodity trading advisers, and commodity pool operators.[266] This transfer of jurisdiction became effective in November 2013. (See Section III.2.b. above on Gramm-Leach-Bliley Act).

i. Affected "Financial Institutions" and "Creditors"

The Rule applies to "financial institutions" and "creditors" that maintain "covered accounts," as those terms are defined by the Rule. "Financial institution" is defined as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account . . . belonging to a consumer."[267]

As initially enacted, the Rule's definition of the term "creditor" was very broad, causing concern that the Rule would extend to entities other than traditional financial institutions that engage in regular forbearance in the collection of debts or bills or permit multiple or extended payments. On December 18, 2010, President Obama signed the Red Flag Program Clarification Act of 2010 into law, amending the Fair Credit Reporting Act's definition of the term "creditor" to narrow the scope of the Rule. The revised definition of "creditor" specifically excludes those who advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person. As a result, many professionals who had challenged the scope of the Rule, including lawyers, accountants and healthcare professionals, are not subject to its requirements.[268]

---

[265] 16 C.F.R. § 681.

[266] *See* Edwards Wildman Client Advisory – *Identity Theft Red Flag Rules Adopted by SEC and CFTC*, Apr. 2013, http://www.edwardswildman.com/newsstand/detail.aspx?news=3737.

[267] 15 U.S.C. § 1681a(t).

[268] The FTC amended its regulations to update its definition of "creditor" to match that in the Red Flag Program Clarification Act of 2010. 16 C.F.R. Part 681. The FTC's amended rules went into effect on February 11, 2013. 77 Fed. Reg. 72712-15.

The Rule now defines "creditor" as used in the Rule as follows:

> "(A) means a creditor, as defined in section 702 of the Equal Credit Opportunity Act[269] (15 U.S.C. 1691a), that regularly and in the ordinary course of business
>
> > (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;
> >
> > (ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or
> >
> > (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person;
>
> (B) does not include a creditor described in subparagraph (A)(iii) that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person; and
>
> (C) includes any other type of creditor, as defined in that section 702, as the agency described in paragraph (1) having authority over that creditor may determine appropriate by rule promulgated by that agency, based on a determination that such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft."[270]

The December 18, 2010 amendment limited the definition of a creditor to cover only creditors who regularly, and in the ordinary course of business, carry out the following functions:

- Obtain or use consumer reports in connection with a credit transaction;
- Furnish information to consumer reporting agencies in connection with a credit transaction; or
- Advance funds to – or on behalf of – someone, except for funds for expenses incidental to a service provided by the creditor to that person.[271]

ii. Covered Accounts

Significantly, the definition of "covered accounts" under the Red Flags Rule is also broad. It has two parts:

---

269 "Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." 15 U.S.C. § 1691a.

270 15 U.S.C. § 1681m(e).

271 *See also* http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.[272]

The second part of this definition extends the scope to any account for which there is a foreseeable risk of identity theft.

The Rule is designed to be risk-based and to take into account the burden that the Red Flags Rule could impose upon an entity that has only a small risk of identity theft. The FTC makes clear that higher-risk entities should have a more comprehensive Identity Theft Prevention Program, and low-risk entities are permitted to have a less complex program, but all entities covered by the Rule are required to establish a program.

In recognition of the burden that compliance with the Red Flags Rule may impose on certain entities, the FTC released a "Do-It-Yourself" Red Flag program for entities that are at low risk for identify theft.[273]

d. Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002 ("FISMA")[274] is a United States federal law enacted as Title III of the E-Government Act of 2002, an act focused on the importance of information security to the economic and national security interests of the U.S. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[275]

e. HIPAA Privacy and Security Rules

The U.S. Department of Health and Human Services ("HHS") has issued Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[276]

---

272 16 C.F.R. § 681.2(b)(3).

273 Available at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm.

274 44 U.S.C. § 3541, *et seq.*

275 http://csrc.nist.gov/groups/SMA/fisma/overview.html.

276 42 U.S.C. § 201 *et seq.* (HIPAA), 45 C.F.R. Part 160 and Subparts A and E of Part 164 (Privacy Rule).

The Privacy Rule governs the use and disclosure of an individual's protected health information ("PHI") by entities covered under HIPAA. The Privacy Rule also sets standards for an individual's right to understand and control some aspects of how his or her PHI is used and disclosed. It applies to health plans, healthcare clearinghouses, and to any healthcare provider who engages in electronic data interchange using one or more of the "standard transactions" as defined by HIPAA regulations governing electronic data interchange (collectively referred to as "covered entities"). The Privacy Rule includes a requirement that a covered entity mitigate, to the extent practicable, any harmful effect that is caused by an improper disclosure of PHI of which it becomes aware. Under the HITECH Act, discussed below, the Privacy Rule also applies directly to business associates of covered entities, although the privacy obligations of business associates are generally limited to compliance with their business associate agreements.

The Privacy Rule was amended by the omnibus amendments to the HIPAA Privacy, Security, Health Breach Notification and enforcement rules released on January 25, 2013 (the "Omnibus Final Rule"). The Omnibus Final Rule implemented most of the privacy amendments mandated by the HITECH Act. Enforcement of the amendments incorporated in the Omnibus Final Rule will commence on September 23, 2013. The business associate provisions of the Omnibus Final Rule will also be effective as of that date, except that business associate agreements in effect prior to January 25, 2013 need not be brought into compliance until the earlier of September 22, 2014, or the first date that the agreement is amended.

The Omnibus Final Rule amended the HIPAA Enforcement Rule, which governs the process by which the Office of Civil Rights ("OCR") investigates and resolves alleged violations of the HIPAA Privacy, Security and Health Breach Notification Rules. Once a violation is identified, the range of penalties that can potentially be imposed and the enforcement discretion of OCR vary significantly based on OCR's determination of the knowledge and intent of the violator. If OCR determines that a violation does not involve willful disregard of the regulations or intentional misconduct, it may waive or significantly reduce penalties. If OCR finds willful misconduct, it must impose a civil penalty, and has the discretion to impose significant penalties for violations that impact many individuals or that continue for long periods of time.

A second major component of HIPAA is the Security Rule, which is directed at PHI in electronic form. The Security Rule sets forth required security standards for protecting electronically stored and transmitted PHI, including administrative safeguards (written procedures and protocols, along with business associate agreements), physical safeguards (limitations on physical access to hardware, media, and software containing PHI), and technical safeguards (protective controls for information systems and networks). The HITECH Act also applied the Security Rule to business associates, making business associates directly accountable for civil monetary penalties under the HIPAA Enforcement Rule.

The HITECH Act greatly increased the civil monetary penalties that could be imposed on covered entities and business associates for violations of the Privacy Rule, the Security Rule or the Health Breach Notification Rule. It also vested limited enforcement power in state Attorneys General to enforce HIPAA's requirements. The HITECH Act and the rules promulgated under it also create additional requirements regarding notification to individuals of a data breach involving health information applicable to HIPAA covered entities or business associates of HIPAA covered entities.

Moreover, as held by the Eleventh Circuit, HIPAA preempts contrary state laws that impede the purpose and objective of HIPAA in keeping an individuals' PHI strictly confidential.[277] However, state laws that create additional privacy protections for individuals are not pre-empted. Thus, state laws that protect privacy (such as laws governing the disclosure of the results of HIV tests or genetic tests) also must be considered.

f. The HITECH Act and Health Breach Notification Rules

The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") under Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, also known as the Economic Stimulus Plan, directed the FTC and HHS to issue regulations with respect to data breaches involving protected health information.

Specifically, the FTC was directed to promulgate regulations requiring vendors of personal health records ("PHR") and related entities to notify consumers when the security of their health information has been breached, and HHS was directed to promulgate a rule requiring (i) HIPAA covered entities, such as hospitals, doctors' offices, and health insurance plans, to notify individuals of a security breach and (ii) business associates of HIPAA covered entities to notify such HIPAA covered entities in the event of a security breach.

i. FTC Health Breach Notification Rule

The FTC's final Health Breach Notification Rule,[278] effective September 24, 2009 and enforced beginning February 22, 2010 (the "FTC Rule"), applies to a different group of entities than HIPAA. It applies to foreign and domestic vendors of PHR, PHR related entities and third-party service providers that maintain the information of U.S. citizens or residents. The FTC Rule does not apply to HIPAA covered entities or any other entity that engages in activities as a business associate of a HIPAA covered entity; these entities are covered by the separate rules issued by HHS, discussed below.

The HITECH Act recognizes the new types of web-based entities that collect consumers' health information, such as vendors of PHR and Internet applications that interact with PHR. A PHR related entity means an entity, other than a HIPAA covered entity or any entity to the extent that it engages in activities as a business associate of a HIPAA covered entity, that:

(1) Offers products or services through the website of a vendor of PHR;

(2) Offers products or services through the websites of HIPAA covered entities that offer individual PHRs; or

(3) Accesses information in a PHR or sends information to a PHR.

---

[277] *Opis Management Resources v. Secretary Florida Agency For Health Care Administration*, Docket No. 4:11-cv-00400-RS-CAS, Apr. 9, 2013 (in which the Florida Agency for Health Care Administration issued citations to nursing facilities for violating Florida law when they refused to release a deceased's medical records to a spouse and certain others on the grounds that they were not "personal representatives" under the relevant provisions of HIPAA).

[278] 16 C.F.R. Part 318. Published in the Federal Register, available at http://www.ftc.gov/healthbreach/.

PHR related entities include, for example, web-based applications that help consumers manage medications and websites offering online personalized health checklists.

Under the FTC Rule, PHR vendors, PHR related entities and third-party service providers that experience a breach in the security of unsecured PHR identifiable health information must notify the FTC, as well as individuals whose information was breached. PHR in this context means "an electronic record of PHR identifiable health information that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual." "Breach of security" means acquisition of unsecured PHR identifiable health information of an individual in a PHR without authorization of the individual. "Unsecured" means PHR identifiable information that is not protected through the use of a technology as recommended by HHS in its guidance discussed below, that renders PHR identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals.[279]

Notice must be provided pursuant to the following requirements:

- Timeliness of Notice: Notice must be provided without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach of security. If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, notice to the FTC must be provided no later than 10 business days after the date of discovery. If the breach involves fewer than 500 individuals, the entity may instead maintain a log of the breach and must submit it annually to the FTC no later than 60 calendar days following the end of the calendar year.

- Method of Notice: Notice to an individual affected by the breach may be sent in any of the following ways:

    - First-class mail to the individual's last known address;

    - Email if the individual did not choose to receive first-class mail; or

    - Substitute notice, if the contact information for 10 or more individuals is insufficient or outdated, by conspicuous posting on the home page of the entity's website for a period of 90 days or in major print or broadcast media, including in the areas where the affected individuals likely reside. The notice must include a toll-free phone number, which must remain active for at least 90 days, that individuals can call to learn whether they are affected by the breach.

- Media Notice: If 500 or more residents of a state or jurisdiction are, or are reasonably believed to be, affected by the breach, the entity must provide notice to prominent media outlets in the state or jurisdiction.

---

[279] 16 C.F.R. § 318.2.

- Content of Notice: The notice must contain the following:
  - A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
  - A description of the types of unsecured PHR identifiable health information involved in the breach;
  - Steps that individuals should take to protect themselves from potential harm resulting from the breach;
  - A brief description of what the entity is doing to investigate the breach, mitigate harm, and protect against future breaches; and
  - Contact information for individuals to ask questions or obtain additional information, including a toll-free number, email address, website, or postal address.

The FTC has issued a standard form to make it easier for companies to report a breach to the FTC.[280]

ii. The HHS Breach Notification Rule for HIPAA Covered Entities and Business Associates

HHS issued an interim final rule on the Breach Notification for Unsecured Protected Health Information for HIPAA covered entities and business associates of those entities, effective September 23, 2009 (the "HHS Rule").[281] The HHS Rule was updated by the Omnibus Final Rule issued on January 25, 2013, with an effective date of March 26, 2013.

Under the HHS Rule, as amended, covered entities must notify individuals whose unsecured protected health information ("PHI") has been, or is reasonably believed to have been, accessed, acquired, used or disclosed following a breach of that unsecured PHI. Covered entities must also notify HHS, and under certain circumstances must also notify the media. The HHS Rule also requires that business associates notify the HIPAA covered entity of the breach. Significantly, the rule requires covered entities to notify individuals and the Secretary of HHS within 60 days of discovery of the breach.

The HHS Rule is similar to the FTC Health Breach Notification Rule. Its provisions regarding timeliness of notification, method of notification, and notice to the media are identical to those of the FTC rule. There are several important differences, however, including the following:

- Instead of notifying the FTC, the HHS Rule requires covered entities to notify the Secretary of HHS;

---

[280] The form is available at http://www.ftc.gov/healthbreach/.

[281] 74 Fed. Reg. 162, Aug. 24, 2009.

- Notices are required to be in plain language;
- If the breach affects more than 500 individuals of a particular state or jurisdiction, notice must be made to HHS contemporaneously with the notification to affected individuals and notice must also be provided to the media; and
- If the covered entity believes that there is possible imminent misuse of unsecured PHI, the covered entity may provide information to individuals by telephone or other appropriate means in addition to written notice.
- If the covered entity lacks sufficient contact information to contact 10 or more individuals directly, it may need to provide substitute notice by publishing the notice of the breach in a major media outlet and on its website.

The Omnibus Final Rule made an important change to the Health Breach Notification Rule by narrowing the basis for not providing notification of a health data breach. Under the original interim final rule, a covered entity was permitted to determine that certain breaches of PHI did not create a sufficient risk of harm to the individual so as to justify notification. This exception to the notification requirement was eliminated, and replaced with a more objective test of whether PHI was "compromised" by the data breach. It is likely that as a result of this change, almost all breaches of PHI will result in notification.

On April 17, 2009, HHS issued a revised version of its *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for the Purposes of the Breach Notification Requirements under the HITECH Act* (the "Guidance").[282] Covered entities and business associates are not required to follow the Guidance. However, if HIPAA covered entities and business associates secure PHI in accordance with the Guidance, the PHI is deemed to be secure and thus a breach of the secured PHI would not be not subject to the notification requirements. The Guidance does not impose any obligation on covered entities to encrypt all PHI, but lists encryption as one of the two ways in which PHI may be rendered unusable, unreadable or indecipherable. The other method is destruction of the media on which the PHI is stored.[283]

The push toward digitalization of medical records provided by the new legislation has raised concerns about a corresponding increase in risk of data breaches as medical information is increasingly maintained in electronic form. The increased risk is likely to result in further efforts to ensure compliance with the security requirements of the legislation.

Moreover, the issue of compliance with the privacy protection requirements of HIPAA and HITECH is also likely to be a component of third-party lawsuits against companies subject to the new rules that sustain data breaches. Lack of compliance with such regulatory safeguards is often a

---

[282] 45 C.F.R. Parts 160 and 154.

[283] Both the interim final HHS Rule and the Guidance are available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html.

basis for claims of negligence in the security procedures of companies that sustain a breach.[284] Lack of compliance may also subject an entity to a suit brought by a state attorney general, as HITECH authorizes an attorney general to pursue an action against an entity that is subject to HIPAA when the attorney general "has reason to believe that an interest of one or more of the residents of [a] state has been or is threatened or adversely affected by any person who violates a [privacy or security provision under HIPAA]."[285]

iii. HIPAA and HITECH Act Enforcement

2013 and 2014, OCR has made it clear that it is concerned that many covered entities, especially providers, have not completed a comprehensive risk assessment as required by the Security Rule. OCR has expressed the intention of seeking daily fines for these violations, which could amount to hundreds of thousands or even millions of dollars in civil penalties for violations of the Security Rule. Moreover, it has reinforced repeatedly that it expects those entities subject to HIPAA and HITECH to be aware of and fulfill their obligations, with amounts of assessments for non-compliance increasing. Thus, May 2014 marked the announcement of one of the largest assessments yet, when OCR announced a settlement with two large medical institutions involving payments of $4.8 million, arising from an investigation following the institutions' submission of a joint data breach report in 2103 regarding the disclosure of PHI of 6,800 individuals.[286] Indicating the focus of OCR investigations on pre-breach security practices as well as post-breach response, the Resolution Agreements focus large on the medical institutions' alleged failures to assess and monitor IT equipment, applications and data systems utilizing PHI, including data systems linked to hospital patient data bases, and includes corrective action plans.

Small breaches as well as large are subject to OCR scrutiny. The year 2013 had begun with HHS announcing its first HIPAA breach settlement involving fewer than 500 patients, in which a hospice agreed to pay $50,000 to settle potential violations of the Security Rule in connection with a breach of unsecured electronic protected health information (ePHI) arising from theft of an unencrypted laptop.[287]

This followed a year of "firsts" in HIPAA and HITECH Act enforcement, signaling what became a trend of heightened enforcement. Enforcement fines also increased in size, as the new Omnibus Final Rule greatly increased the potential penalties for violations of the HIPAA Privacy, Security

---

284 *See Amborgy v. Express Scripts, Inc. et al*., Civil Docket #4:09-VC-00705-FRB, filed in May 2009 in the U.S. District Court, Eastern District of Missouri. This lawsuit was commenced as a class action against an entity that provided pharmacy services and drug formulary management services to member groups including managed care organizations, insurance carriers and employer and union-sponsored health plans. It received an extortion demand by persons who had gained access to its customers' confidential Personal Information. The plaintiffs based their complaint on, among other things, the company's alleged failure to comply with HIPAA in a purported breach of assurances of compliance in its Privacy Notice.

285 42 U.S.C. § 1320d-5(d).

286 New York and Presbyterian Hospital agreed to pay OCR $3,300,000 to settle potential violations of HIPAA Privacy and Security Rules and to adopt a corrective action plan to evidence their remediation of OCR's findings, and Columbia University (CU) has agreed to pay a $1,500,000 monetary settlement and corrective action plan to address deficiencies in its HIPAA compliance program. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html; See *Data Breach Results in $4.8 Million HIPAA Settlements*, May 7, 2014, Advisen, http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

287 U.S. Department of Health & Human Services, *HSS announces first HIPAA breach settlement involving less than 500 patients*, Jan. 2, 2013, www.hhs.gov/news/press/2013pres/01/20130102a.html.

and Health Breach Notification Rules.[288] In January 2012, in the first state HIPAA enforcement action against a business associate, Minnesota Attorney General Lori Swanson filed a civil lawsuit[289] against Accretive Health, Inc., a provider of debt collection and other services for hospitals. The lawsuit, which alleged multiple HIPAA violations as well as inappropriately aggressive debt collection practices, was settled in July when Accretive agreed to pay $2.5 million to the State of Minnesota to establish a restitution fund to compensate affected patients. Accretive was also required to stop doing business in Minnesota for two years, which will cost the company approximately $25 million in projected annual revenues.

In March 2012, in the first enforcement action resulting from a breach self-report under the HITECH Act's breach notification rule, Blue Cross Blue Shield of Tennessee (BCBST) agreed to pay the OCR $1.5 million and to enter into a corrective action plan in order to avoid civil monetary penalties for HIPAA violations. BCBST claimed to have spent more than $17 million in corrective actions relating to the breach, which involved the theft of hard drives that contained patient information.

In April 2012, HHS signaled that small practices as well as large are subject to significant assessments, when it reached a $100,000 settlement agreement with Phoenix Cardiac Surgery, a small, four-physician practice, after a whistleblower tip prompted an HHS investigation. HHS found that the practice had committed various HIPAA violations, including the use of an unsecured publicly accessible, Internet-based calendar service. The group had also failed to implement proper policies and procedures to ensure the privacy and security of patient information or to train its employees, and failed to enter into business associate agreements with its service providers to ensure that they were properly handling PHI.

In June 2012, in the first HIPAA enforcement action by HHS against a state agency, the Alaska Department of Health and Social Services (DHSS) agreed to pay HHS $1.7 million to settle alleged violations of the Security Rule. The DHSS had filed a breach report stating that a portable USB drive that possibly contained PHI was stolen from the vehicle of a DHSS employee. In its investigation, OCR also discovered that the DHSS did not have adequate policies and procedures in place to safeguard PHI.

These are just a sample of the enforcement actions taken against in recent years, indicating that entities that sustain a breach will be undergoing close scrutiny of their pre-breach data security assessments and practices as well as of their post breach response.

g. Additional Data Privacy Requirements for Educational Institutions

In the United States, any school or institution that provides educational services or instruction and receives funds under any program administered by the U.S. Department of Education (DOE) is subject to the privacy requirements of the Family Educational Rights and Privacy Act ("FERPA").[290] Subject to certain limited exceptions, FERPA gives students (or in some cases their

---

[288] See Edwards Wildman Client Advisory, *HIPAA Enforcement Rule Sets Standards for Penalties: Will Your HIPAA Compliance Program Stand Up?*, Mar. 14, 2013, http://healthcare.edwardswildman.com/blog.aspx?entry=4655.

[289] *Minnesota v. Accretive Health, Inc.* (No. 12-145), D. Minn., Jan. 19, 2012.

[290] 20 U.S.C. §1232g; 34 C.F.R. Part 99.

parents) the right to inspect and challenge the accuracy of a student's own education records, while prohibiting schools from disclosing those records, or any personally identifiable information about a student contained in those records, without the consent of the student or, in the case of a minor, the student's parent. In December 2011, the DOE issued several amendments to its implementing rules that made considerable changes to information-sharing among subject entities, the scope of entities subject to enforcement by the DOE.[291]

The consent provisions and protection of "personal information" under FERPA differ significantly from other privacy laws. Personally Identifiable Information (PII) is defined as (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's Social Security number, student number, or biometric record; (e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.[292]

However, FERPA also contains a category of data, called "Directory Information," which significantly overlaps with PII but is excepted from the prohibition against sharing PII without consent. FERPA permits schools to make directory information publicly available without prior consent, so long as parents or students over 18 are informed what data that particular school is classifying as directory information and given an opportunity to opt out of the sharing. This exception is typically used by schools to offer a school directory or yearbook without obtaining the otherwise required consents for publicly disclosing students' names, addresses, birthdates, degrees, etc. Prior to the 2011 amendments, schools were only permitted an all-or-nothing approach to directory information, where anything classified as directory information was publicly available for any purpose. The 2011 amendments permit, but do not require, schools to limit the use or disclosure of directory information and give parents or students the option to opt out of some, but not other, uses.

The 2011 amendments expand another exception to the privacy protections of FERPA, by increasing the opportunities for disclosure under the "audit or evaluation" and "studies" exceptions. These allow covered entities to share student records with third parties for the purposes of audits, evaluations, or longitudinal studies of their education programs, when certain privacy protections, including written agreements with those third parties, are in place. Finally, the 2011 amendments clarify that FERPA may be enforced even against entities that do not have students in attendance, such as state education agencies, and third parties who contract with a school to provide services and receive education records, but do not receive direct DOE funding. There is no private right of action under FERPA.[293]

---

291 76 Fed. Reg. 75604-60

292 34 C.F.R. § 99.3

293 *Gonzaga University et al. v. Doe*, 122 S. Ct. 2268, 536 U.S. 273 (2002).

Aside from FERPA, several states have passed laws that govern the collection of information not covered by FERPA, such as social media account information. See Section III.2.g above. Moreover, if an educational institution is also an arm of municipal or state government, its records may be subject to privacy laws governing state agency records.

h. Further Protection for Minors

Additional statutory protection is afforded children under 13 by the Children's Online Privacy Protection Act of 1998 ("COPPA").[294] COPPA and its related rules regulate the online and mobile collection and release of personal information from children under 13. The FTC has authority to issue regulations and enforce COPPA, and has done so vigorously. For instance, on May 12, 2011, the FTC announced an agreement settling claims that Playdom, Inc., a leading publisher of social games and virtual worlds, violated the COPPA Rule and Section 5 of the FTC Act in connection with the operation of a number of online virtual world games. The settlement announced included a $3 million fine. Other fines, while not as large, have been substantial.[295]

COPPA also includes a self-regulatory provision that allows industries or other entities to apply for approval of a "safe harbor" program, under which companies agree to be subject to the compliance review and disciplinary procedures of the program in lieu of FTC enforcement. The most recent such program was approved in February 2014.[296]

In September 2011, the FTC proposed revisions to COPPA, in part to address mobile and new technology. After receiving over 350 public comments, on August 1, 2012 the Commission published a Supplemental Notice of Proposed Rulemaking in which it changed several aspects of its proposed revisions that continued the effort to balance the interest of protecting children with the practicalities and challenges of operating within an online or mobile environment, while also acknowledging the importance and benefits of the Internet, and invited comments.[297]

Finally, in December 2012, after a two-year process, the FTC introduced a new rule that went into effect July 1, 2013. In this new rule, the FTC changed course on many of its original proposals and adopted many industry suggestions that recognize that COPPA is aimed at protecting children from inappropriate contact without parental knowledge, and not aimed at preventing advertising to children. The new rule retained "email plus," which allows operators to obtain parental consent to collection of children's personal information for certain internal purposes (but not third party commercialization or marketing) by means of an email from a parent along with a reasonable form of follow-up confirmation. The definition of "personal information" was expanded for purposes of COPPA and its requirement for verified parental consent for collection of such information, and includes persistent identifiers (with some exceptions), geolocation information, photographs and videos of children. The new rule also includes provisions affecting mixed-use or family-oriented

---

294 15 U.S.C. §§6501-6506. *See* related rules at 16 CFR Part 312.

295 *See, e.g., Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books – Company also Will Pay $800,000 for Allegedly Collecting Kids' Personal Information without their Parents' Consent*, FTC Release, Feb. 1, 2013, http://www.ftc.gov/opa/2013/02/path.shtm.

296 http://www.business.ftc.gov/content/safe-harbor-program.

297 *See* Edwards Wildman Palmer LLP Client Advisory, *Not Kidding About Protecting Kids' Data – FTC Puts Forth More Changes to Proposed Children's Privacy Rules,* Aug. 2012, http://www.edwardswildman.com/newsstand/detail.aspx?news=3013.

sites as well as general audience sites (such as social media plug ins), and numerous other provisions. As stated by the FTC in its announcement of the new rule:

> It requires that operators of website or online services that are either directed to children under 13 or have actual knowledge that they are collecting personal information from children under 13 give notice to parents and get their verifiable consent before collecting, using or disclosing such information, and keep secure the information they collect from children. It also prohibits them from conditioning children's participation in activities on the collection of more personal information that is reasonably necessary for them to participate. The Rule contains a "safe harbor" provision that allows industry groups or other to seek FTC approval or self-regulatory guidelines."[298]

Though "email plus" was retained in some capacity, the FTC detailed various other methods of obtaining verifiable parental consent and the situations for which each method would be applicable. In addition to these, the new rule opened the door for applications for new methods of obtaining verifiable parental consent. The first such new method, "knowledge-based authentication" was approved in December 2013 on an application by Imperium, Inc.[299]

Recently, in April 2014, the FTC revised its Guide for Complying with COPPA, including Frequently Asked Questions which are stated to be intended to supplement the compliance materials available on the FTC Website.[300]

i. Telecommunications

Entities regulated by the Federal Communications Commission ("FCC") may be subject to several privacy provisions contained in the Communications Act, including a prohibition on disclosing the contents or even existence of the communications they carry.[301]

The most prominent of the Communications Act's privacy rules are those concerning Customer Proprietary Network Information ("CPNI"), which requires that providers of telephone service – including Voice over Internet Protocol (VoIP) providers that connect to the public switched telephone network – limit use, disclosure of, and access to information such as phone numbers dialed, length of calls, services purchased by a customer, and charges incurred to the provision of

---

298 *FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule*, released Dec. 19, 2012, www.ftc.gov/opa/2012/12/coppa.shtrm; see also Alan Friel, *New COPPA Rule a Middle Ground – Broadens and Clarifies Children's Privacy Obligations of On line and Mobile Companies, But Backtracks on Many Previously Proposed Changes That Would Have Disrupted The Advertising and Publishing Industries*, Digilaw, Dec. 19, 2012, http://digilaw.edwardswildman.com/blog.aspx?entry=4485.

299 *See* Edwards Wildman Palmer LLP Client Advisory, *Edwards Wildman Client Advisory: New Ways to Get Parental Consent to Collect Data From Children Emerging Under COPPA*, February 2014, http://www.edwardswildman.com/Edwards-Wildman-Client-Advisory-New-Ways-to-Get-Parental-Consent-to-Collect-Data-From-Children-Emerging-Under-COPPA-02-13-2014/

300 "Complying with COPPA: Frequently Asked Questions – A Guide for Business and Parents and Small Entity Compliance Guide (revised April 2014)," available at www.business.ftc.gov.

301 47 U.S.C. § 605.

telephone service and certain related services.[302] Unlike some other privacy laws, this does not include "Subscriber List Information," the names, telephone numbers, and addresses of subscribers that the telephone carrier publishes in a directory.[303] This exception allows for the publication of telephone directories.

In 2013, the FCC extended the CPNI rules to cover information collected by a mobile device that meets the definition of CPNI, when the mobile carrier directs that collection and has access to the information collected, including data regarding customers' use of the network and data collected through and about preinstalled apps.[304]

The Communications Act also includes customer notice and data protection requirements for cable[305] and satellite[306] providers. Under these rules, cable and satellite providers must give annual notice to their subscribers of their personally identifiable information collected; how that information will be used, disclosed, and maintained; and how a subscriber may access the information held. The law also limits the possible uses and disclosures that can be made without customer consent, and requires that the data be destroyed if it is no longer necessary for the purpose for which it was collected.

Other laws and regulations affecting communications companies include the cybersecurity framework developed by NIST, which identifies the communications sector as critical infrastructure (see Section II.2.k. on Critical Infrastructure below); and EU data breach notification regulations, which requires telecommunications companies to provide notice to regulators and subscribers in the event of a data breach (see Section IV below). Various states in the U.S. may also have data breach notification laws that affect communications companies (see Section III. 1 on State Data Privacy and Security Requirements, above).

j. Telephone Consumer Protection Act

The Telephone Consumer Protection Act ("TCPA") presents a major privacy-related risk for companies in a wide array of industries which use faxes, text messages, artificial or pre-recorded voice messages, and automated dialing technologies to reach customers.[307] While the TCPA is not directed at data security, it is privacy related in that it was enacted in response to consumer complaints about the intrusion into consumer privacy of unsolicited telemarketing. The TCPA provides a private cause of action to recipients of certain unauthorized telephone calls and faxes and affords damages of $500 for each violation.[308] Courts in their discretion may also award up to treble damages if plaintiffs show defendants violated the TCPA "willfully" or "knowingly."[309]

---

302 47 U.S.C. § 222.

303 *Id.*

304 *In the Matter of Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, FCC 13-89 (June 27, 2013).

305 47 U.S.C § 551.

306 47 U.S.C. § 338(i).

307 *See generally* 47 U.S.C. § 227.

308 *Id.*, § 227(b)(3).

309 *Id.*

Because these statutory damages can become substantial (even staggering) when aggregated, an increasingly active plaintiffs' bar has filed hundreds of class action lawsuits seeking millions of dollars in damages for alleged TCPA violations. In addition to claims under the TCPA, these plaintiffs also frequently assert claims based on state consumer protection statutes and common law claims for conversion, which can increase a defendant's exposure.

Subject to various exceptions, the TCPA outlaws five practices.

First, the Act makes it unlawful to use an automatic telephone dialing system ("ATDS") or an artificial or prerecorded voice message (sometimes called "robocalls"), without the prior express consent of the called party, to call any emergency telephone line, hospital patient, pager, cellular telephone, or other service for which the receiver is charged for the call, with certain exemptions.[310] The TCPA authorizes the FCC to exempt from this provision calls to a number assigned to a wireless service that are not charged to a consumer, subject to conditions the Commission may prescribe to protect consumer privacy rights.[311] Courts have held that only the current subscriber of the phone may provide the requisite "consent."[312] Under the TCPA, an ATDS is "equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."[313] Courts have held that simply using a computer (or iPhone or modem) that could be, but was not, paired with software that would enable it to act as an ATDS was not enough to satisfy the "capacity" requirement.[314] Courts have treated

---

310 *Id.*, § 227(b)(1)(A).

311 *Id.*, § 227(b)(2)(C). As of March 2014, 24 petitions seeking clarification concerning how to interpret the TCPA were pending before the FCC. Addressing these petitions, FCC Commissioner Michael O'Reilly wrote in a blog post that it was "time to provide clarity" for companies that rely on the TCPA and stated: "[i]t is very troubling that legitimate companies feel they have to ask the government for its blessing every time they need to make a business decision in order to avoid litigation," and "[t]hat is why the FCC needs to address this inventory of petitions as soon as possible." Commissioner Michael O'Reilly, *TCPA: It is Time to Provide Clarity*, FCC Blog (Mar. 25, 2014), www.fcc.gov/blog/tcpa-it-time-provide-clarity. See *In the Matter of Cargo Airline Assoc'n* Petition for Expedited Declaratory Ruling; Rules and Regulations Implementing the Tel. Consumer Prot. Act of 1991, 2014 FCC LEXIS 1072 (Mar. 27, 2014) (summarizing conditions specified by the FCC for this exemption).

312 *See Osorio v. State Farm Bk.*, No. 11-cv-61880, 2014 U.S. App. LEXIS 5709, *14-18 (11th Cir. Mar. 28, 2014); *Soppet v. Enhanced Recovery Co., LLC*, 679 F.3d 637, 639-40 (7th Cir. 2012). Some courts have evaluated whether the subscriber gave consent using principles established in common law. *Osorio*, 2014 U.S. App. LEXIS 5709 at *18-25. Other courts, drawing from fourth amendment principles, have held that consent can be provided by a person with "common authority" over the cellular telephone. *Gutierrez v. Barclays Group*, No. 10-cv-1012, 2011 U.S. Dist. LEXIS 12546, *6-9 (S.D. Cal. Feb. 9, 2011) dismissed on other grounds, 2012 U.S. Dist. LEXIS 190049 (S.D. Cal Mar. 12, 2012). Most recently, the FCC seemed to question these holdings, stating it found "inapposite" comments "that there is well-developed body of law addressing intermediary consent, including in the context of the Fourth Amendment where consent to a police search may be obtained from a third party who possesses either actual or apparent authority." *Cargo Airline Ass'n*, 2014 FCC LEXIS 1073, *18 (March 27, 2014). The FCC has issued an order providing that "autodialed . . . calls to wireless numbers that are provided by the called party to a creditor in connection with an existing debt are permissible as calls made with the 'prior express consent' of the called party." *In re Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991*, 23 F.C.C. Rcd. 559, 559 (2007). The FCC has also issued an order clarifying that "neither the TCPA nor [its] implementing rules and orders require any specific method by which a caller must obtain such prior consent for non-telemarketing calls to wireless phones, and [concludes] that the TCPA does not prohibit a caller from obtaining consent through an intermediary." *In the Matter of GroupMe, Inc/*Skype Communications S.A.R.L. petition for Expedited Declaratory Ruling; Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 2014 FCC LEXIS 1073, at *17-18 (Mar. 27, 2014).

313 47 U.S.C. § 227(a)(1); *see also Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 951 (2009) ("system need not actually store, produce, or call randomly or sequentially generated telephone numbers, it need only have the capacity to do so").

314 *Gragg v. Orange Cab Co., Inc.*, No. 12-cv-0576, 2014 U.S. Dist. LEXIS 29052, at *3 (W.D. Wash. Feb. 28, 2014); *see also Dominguez v. Yahoo!, Inc.*, No. 13-cv-1887, 2014 U.S. Dist. LEXIS 36542, at *18 (E.D. Pa. Mar. 20, 2014) (system was not an ATDS where plaintiff did not offer evidence it had capacity to randomly or sequentially generate telephone numbers, as opposed to simply storing telephone numbers); *but see Hunt v. 21st Mort. Corp.*, 2014 U.S. Dist. LEXIS 13469, *13-17 (N.D. Ala. Feb. 4, 2014)

text messages the same as recorded and autodialed calls to cell phones.,[315] although at least one FCC Commissioner expressed "hesitation on the applicability of the TCPA to text messages," noting that the TCPA was enacted in 1991 – before the first text message was ever sent.[316] Some courts have held that consumers who "opt out" of text messages may be sent a single text message confirming receipt of the "unsubscribe" request.[317] In addition, effective October 16, 2013, "prior express written consent" is required for telemarketing calls to cell phones.[318]

Second, the TCPA forbids using artificial or prerecorded voice messages to call residential telephone lines without prior express consent,[319] again subject to certain exemptions.[320] Effective October 16, 2013, all telemarketing robocalls are prohibited unless the consumer has given express *written* consent.[321] In addition, all such calls must include an interactive opt-out mechanism at the beginning of the message, and when a consumer chooses to opt-out, the number must be added to the caller's do-not-call list and the call must be immediately disconnected.[322]

Third, the TCPA prohibits sending "unsolicited advertisements" to fax machines.[323] An "advertisement" is "any material advertising the commercial availability or quality of any property, goods, or services."[324] The TCPA provides a safe harbor for such transmissions where three elements are met: (1) the sender and recipient have an established business relationship; (2) the recipient voluntarily shared its fax number within the context of the established business relationship or the recipient voluntarily made its fax number available for public distribution (e.g.,

---

(question of fact whether defendant's system was ATDS where defendant allegedly destroyed system when it knew of plaintiff's claim making it impossible to determine, as a matter of law, whether enabling software was installed or could easily have been installed).

315 *See, e.g.*, *Dominguez*, 2014 U.S. Dist. LEXIS 36542 at *n. 310 ("[f]ederal courts have made clear that the TCPA applies to text messages as well as voice calls"), *citing Gager v. Dell Fin. Servs., LLC*, 727 F.3d 265, 268 (3rd Cir. 2013) (citing In the Matter of Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 27 F.C.C. Rcd. 15391 (2012) and *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 954 (9th Cir. 2009)). On the other hand, courts have held § 227 does not apply to e-mails. *Prukala v. Elle*, No. 14-cv-92, 2014 U.S. Dist. LEXIS 41887 (M.D. Pa. Mar. 28, 2014), *citing Aronson v. Bright-Teeth Now, LLC*, 824 A.2d 320, 323 (Pa. Super. Ct. 2003) ("that Plaintiff received the alleged e-mails on the same device that she uses as a telephone does not bring [them] under the reach of the TCPA); *see also* In re Rule & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 18 F.C.C.Rcd. 14014, 14133 (2013) (§ 227(b)(1)(C) (prohibition does "not extend to facsimile messages sent as email over the internet").

316 *Cargo Airline Ass'n*, 2014 FCC LEXIS at *26-27 (Cmr. O'Reilly, concurring).

317 *Ibey v. Taco Bell Corp.*, 2012 U.S. Dist. LEXIS 91030 (S.D. Cal. June 18, 2012); *Ryabyschuck v. Citibank (South Dakota) N.A.*, 2012 U.S. Dist. LEXIS 156176 (S.D. Cal. Oct. 30, 2012).

318 47 C.F.R. § 64.1200(a)(2).

319 47 U.S.C. § 227(b)(1)(B).

320 See 47 C.F.R. § 64.1200(a)(2)(iv) and § 64.1200(f)(5).

321 *Id.*, § 64.1200(a)(2) & (a)(3); § 64.1200(b)(2) & (b)(3).

322 *Id.*, § 64.1200(a)(7) & (b)(3). Debt collection calls to a landline are not considered telemarketing calls. *Meadows v. Franklin Collection Serv.*, 2011 U.S. App. LEXIS 2779, *11-12 (11th Cir. 2011) (debt collector "did not violate the TCPA because . . . [it] had an established business relationship with the intended recipient of its prerecorded calls")

323 47 U.S.C. § 227(b)(1)(C).

324 *Id.* § 227(a)(4). Courts have found that even faxes offering services which are ostensibly free may have a qualifying commercial element if the sender intended to induce the recipient to take advantage of the commercial availability or quality of goods and services offered by the sender. *In re Rules and Regulations Implementing the Tel.Consumer Protection Act of 1991 and the Junk Fact Prevention Act of 2005*, 21 F.CC.Rcd.3787, 3814 (Apr. 2006); *G.M. Sign. Inv. V. MFC.com, Inc., No. 08-cv-7106*, 2009 WL 1137751*2 (N.D. Ill. Apr. 24, 2009). An advertisement is "unsolicited" if it "is transmitted to any person without that person's prior express invitation or permission." 47 &U.S. C. §227(b)(1)(D).

by submitting the fax number to a website or directory); and (3) the fax contained an opt-out notice as required by the statute and applicable FCC regulations.[325] In addition, courts have held this prohibition protects lessees of fax machines, as well as owners.[326]

Fourth, the TCPA bans using automatic telephone dialing systems to engage two or more of a business's telephone lines simultaneously.[327]

Fifth, the TCPA was amended in 2010 to make it unlawful to "knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value," except for law enforcement purposes or pursuant to court order.[328]

The TCPA also provides one of the statutory bases for the "National Do Not Call Registry."[329] Under FCC regulations, "[n]o person or entity shall initiate any telephone solicitation to . . . a residential telephone subscriber who has registered his or her telephone number on the national do-not-call registry."[330] The regulations, however, do not prohibit calls to persons with whom the seller has "an established business relationship," unless the recipient has previously made a specific do-not-call request to that caller.[331] Once the recipient made a do-not-call request, then the caller must honor it within a reasonable time, not exceeding thirty days, from the date such request was made.[332]

The TCPA authorizes plaintiffs to sue to enjoin violations, or to recover actual monetary losses or statutory damages of $500 per violation, whichever is greater, or both.[333] In addition, if a court finds that defendant "willingly" or "knowingly" violated the TCPA or its regulations, then it may increase the damages amount to not more than 3 times the amount of damages awarded.[334] A

---

325 *Id.* § 227(b)(1)(C) & (b)(2)(D); 47 C.F.R. § 64.1200(a)(4). Courts have confronted questions relating to the extent to which the Hobbs Act (28 U.S.C. sec. 2342) prohibits a party from challenging the validity of the FCC rules in the context of a private TCPA action. The Hobbs Act provides that federal appellate courts have exclusive jurisdiction to review and determine the validity of FCC orders. Some Circuits have broadly held the Hobbs Act "generally precludes our court from holding the contested regulation invalid outside the statutory procedure mandated by Congress." *Nack v. Wahlburg*, 715 F.3d 680, 686 (8th Cir. 2013). At least one Circuit Court of Appeal seems to disagree with this expansive reading of the Hobbs Act, suggesting the Hobbs Act does not bar challenges to FCC rules as unconstitutional or ultra vires. *Leyse v. Clear Channel Broadcasting, Inc*., 2013 U.S. App. LEXIS 22770, *832-38 (6th Cir. Nov. 5, 2013) (petition for certiorari pending).

326 *Chapman v. Wagener Equities, Inc.*, 2014 U.S. App. LEXIS 5962 (7th Cir. Mar. 19, 2014) ("whether or not the user of the fax machine is an owner, he may be annoyed, distracted, or otherwise inconvenienced if his use of the machine is interrupted by unsolicited faxes"), *criticizing Compressor Eng. Corp. v. Mfgs. Fin'l Corp.*, 292 F.R.D. 433, 448 (E.D. Mich. 2013) (finding ownership requirement because Congress's concern was with the cost of the paper and ink incurred by the owner of the fax machine and the fax machine's owner's loss of the use of the machine").

327 47 U.S.C. § 227(b)(1)(D).

328 *Id.*, § 227(e).

329 *Id.*, § 227(c).

330 47 C.F.R. § 64.1200.

331 *Id.*, § 64.1200(f)(5)i), (f)(14)(ii).

332 *Id.*, § 64.1200(d)(3).

333 *Id.*, § 227(b)(3).

334 There is currently a split of authority as to what constitutes a knowing and willful violation. *See In re: Monitronics Int'l, Inc., Tel. Consumer Prot. Litig.*, No. 11-cv-90, 2014 U.S. Dist. LEXIS 10028, *17-19 (N.D. W.Va. Jan. 28, 2014). Some courts have

different private right of action provision governs "do not call" violations. A person who has received "more than one telephone call within any 12-month period by or on behalf of the same entity in violation of the regulations prescribed" by the FCC may bring suit for actual damages or "up to $500 in damages for each such violation."[335] In addition, if the court finds that a defendant "willfully or knowingly" violated the regulations under this subsection, the court may award treble damages.[336]

Statutory damages under the TCPA can become extensive when aggregated, and plaintiffs frequently pursue such TCPA claims through class actions. Although many courts have denied certification due, e.g., to a lack of commonality, predominance or superiority under Rule 23 or state law counterparts,[337] litigation and settlement classes have been certified,[338] and some class actions have settled for millions of dollars. In many of these cases, plaintiffs have settled with defendants for millions of dollars on the condition that plaintiffs will only seek satisfaction of the judgment from the defendants' insurance policies even if a court determined the insurers did not owe defendants coverage.[339] In turn, defendants have assigned their claims against and rights to payments from their insurers to the class.[340] (See Section on Privacy Related Litigation, below)."[341]

Numerous lawsuits have also been filed seeking coverage for underlying TCPA violations. (See Section on Potential Insurance Coverages, below).

k. Critical Infrastructure – The NIST Cybersecurity Framework

By Executive Order in 2013, President Obama directed the National Institute of Standards and Technology (NIST) to work with the private sector to develop a voluntary Framework – based on

---

held that a defendant must have known its actions violated the TCPA. *Id.*, at *17 (citing cases). Other courts have held that knowledge of the TCPA is not necessary. *Id.*, at *17-18 (citing cases).

[335] 47 U.S.C. § 227(c)(5).

[336] *Id.*

[337] *See, e.g., Wolfkiel v. Intersections Ins. Servs. Inc.*, No. 13C 7133, 2014 U.S. Dist. LEXIS 28276 (N.D. Ill. Mar. 5, 2014) (striking class allegations where court would have to conduct class-member-specific inquiries to determine whether each class member revoked consent to defendants' telemarketing calls); *see also Local Baking Prods. v. Kosher Bagel Munch, Inc.*, 23 A.3d 469, 474-77 (Sup. Ct. N.J. 2011) (surveying TCPA cases and finding "lack of uniformity as to approach and result" on question of certification; concluding "class action suit is not a superior means of adjudicating a TCPA suit" because "Congress has presented an aggrieved party with an incentive to act in his or her own interest without the necessity of class action relief"); *see also Bank v. Independence Energy Group*, 736 F.3d 660, 661 (2nd Cir. 2013) (even though New York statute prohibits class action claims for statutory damages, Rule 23 – not state law – governs when TCPA suit is filed in federal court).

[338] *Hawk Valley, Inc. v. Taylor*, No. 13-cv-1807, 2014 U.S. Dist. LEXIS 45700, at *42-52 (E.D. Pa. Mar. 31, 2014) (surveying cases where plaintiffs pursued TCPA unsolicited-fax advertisement classes; concluding that individualized issues did not predominate where no evidence suggested anyone sought or received express permission from the fax recipients and only small percentage had done business with defendant); *Ira Holtzman, C.P.A., & Associates Ltd. v. Turza*, 728 F.3d 682, 684 (7th Cir. 2013) ("[c]lass certification is normal in litigation under § 227 because the main questions . . . are common"); *Gene and Gene LLC v. BioPay LLC*, 541 F.3d 318, 328 (5th Cir. 2008) (violations of § 221(b)(1)(C) "are not *per se* unsuitable for class resolution" but depend on factual circumstances of each case).

[339] *See, e.g., Standard Mut. Ins. Co. v. Lay*, 989 N.E.2d 591, 594-95 (Ill. 2013).

[340] *Id.*

[341] *Id.* at *6-7, *citing* FCC Ruling, 28 FCC Rcd 6574 at ¶ 46 (consumers may acquire evidence of relationship between telemarketer and seller through discovery if they are not independently privy to such information).

existing standards, guidelines, and practices -- for reducing cyber risks to the nation's critical infrastructure. The resulting Cybersecurity Framework[342] was released in February 2014.

The Cybersecurity Framework was created through collaboration between industry and government,[343] and "provides a consensus description of what's needed for a comprehensive cybersecurity program." It references several generally accepted domestic and international security standards, and collates such practices into a framework of activities that arguably establishes a set of requirements for the development of "reasonable" security practices. It is generally agreed by the participants to constitute best practice for cybersecurity,[344] and carries the weight of being a government-issued framework that was the result of a year-long collaboration between industry and government to develop a voluntary "how to" guide for organizations to enhance their cybersecurity.[345]

Technically, the Cybersecurity Framework was written only for businesses in the 16 critical infrastructure sectors,[346] but it is neither industry-specific, nor country-specific. Consistent with existing law, the Framework adopts a risk-based approach to managing cybersecurity risk. As such, it appears to fit quite well with the approach of existing legal requirements for cybersecurity obligations. It provides generic approaches and activities to address cybersecurity for all businesses.

Created through collaboration between government and the private sector, the Framework uses a common and simplified language to address and manage cybersecurity risk. It provides a common language for understanding, managing, and expressing cybersecurity risk, and thus provides a non-technical tool for aligning policy, business and technological approaches to managing risk.

The Cybersecurity Framework outlines a standardized approach – a process – for companies to identify, describe, address, and communicate their cybersecurity measures and risks. In doing so, the Framework provides organization and structure to the multiple existing approaches to cybersecurity by assembling references to standards, guidelines, and practices that are working effectively in industry today. Most of those standards are internationally recognized. Thus, the Framework provides guidance to an organization on how to manage its cybersecurity risk.

---

342 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

343 The "framework is the culmination of a year-long effort that brought together thousands of individuals and organizations from industry, academia and government." Press release "NIST Releases Cybersecurity Framework Version 1.0," February 12, 2014, available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

344 "Over the past year, individuals and organizations throughout the country and across the globe have provided their thoughts on the kinds of standards, best practices, and guidelines that would meaningfully improve critical infrastructure cybersecurity. The Department of Commerce's National Institute of Standards and Technology (NIST) consolidated that input into the voluntary Cybersecurity Framework that we are releasing today." White House Press Release, Launch of the Cybersecurity Framework, February 12, 2014, available at http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework.

345 http://www.nist.gov/cyberframework

346 According to Presidential Policy Directive 21 (PPD-21), the 16 critical infrastructure sectors are: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation, and water and waste water systems.

The Framework allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.[347]

At present, the Cybersecurity Framework has no legal standing. It is neither a law nor a regulation, and thus does not impose on any business a legal duty to provide data security or constitute a legally-binding standard to follow. However, it may well become the legal standard for defining reasonable security in the near future. The key part of the Framework is referred to as the Core. The Framework Core sets out a process that a business can follow to determine how to address its own unique cybersecurity needs. It is an approach similar in concept to the WISP, is consistent with the process-oriented risk-based approach of the WISP, and essentially incorporates all of the elements of the WISP concept. Thus, it may well become the standard of care going forward.

The activities outlined by the Framework Core set forth, at a very high level, activities that are likely to come to be viewed as basic requirements (i.e., best practices) for the data security processes businesses should be following. The level of detail starts at the very general (Functions), progresses to more detail (Categories within Functions), and then ultimately to the lowest of the three levels of detail (Subcategories within Categories). Those five Functions and the corresponding categories can be summarized as follows:

> Identify Function. This function involves developing the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. It is fundamental to all data security activities, and includes the following Categories:
>
> - Asset Management Category: Identification of all assets to be protected (physical devices, software, data flows, etc.);
> - Business Environment Category: Identification of business environment, including the organizations role in the supply chain and critical infrastructure;
> - Governance Category: Identification of governance policies, procedures and processes to manage and monitor the organizational, regulatory, legal, risk, environmental, and operational requirements;
> - Risk Assessment Category: Risk assessment – *i.e.*, identification of the threats, vulnerabilities, and impact thereof on the organization;
> - Risk Management Strategy: Identification of risk management strategy – *i.e.*, the organizations priorities, constraints, risk tolerances, and assumptions.
>
> Protect Function. Once the assets to be protected and the risks they face have been identified, the next step is to put in place the processes, procedures, and security measures to provide such protection – *i.e.*, to implement appropriate safeguards. This includes the following categories:
>
> - Access Control Category: Access control processes and procedures should limit access to processes, devices, and data to authorized users;

---

[347] See press release "NIST Releases Cybersecurity Framework Version 1.0," February 12, 2014, available at http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

- Awareness and Training Category: Appropriate education and training should be provided for employees and business partners regarding security-related duties and responsibilities;
- Data Security Category: Security measures, processes, and procedures should be implemented to protect data at rest, data in transit, data integrity and to protect against data leaks;
- Information Protection Processes and Procedures Category: Security measures should be implemented to manage the protection of information systems and assets;
- Maintenance Category: Address maintenance and repairs of control systems and information system components consistent with policies and processes;
- Protective Technology Category: Manage technical security solutions to ensure the security and resilience of systems and assets (e.g., audit logs, removable media, and communications & control networks).

Detect Function. Processes, procedures, and policies should be in place to detect the occurrence of cybersecurity events. These include the following categories:

- Anomalies and Events Category: The ability to detect anomalous activities in a timely manner and understand the potential impact of events;
- Security Continuous Monitoring Category: Continuous security monitoring of information systems and assets to identify cybersecurity events and verify the effectiveness of protective measures;
- Detection Processes Category: and procedures to ensure timely and adequate awareness of anomalous events.

Respond Function. Processes and procedures should be in place to properly and promptly respond to detected cybersecurity events. These include the following:

- Response Planning Category: Implement response processes and procedures designed to ensure timely response to detected cybersecurity events;
- Communications Category: Coordinate response activities with internal and external stakeholders, including law enforcement agencies;
- Analysis Category: Ensure adequate analysis (including forensics) is conducted to ensure adequate response and support recovery activities;
- Mitigation Category: Perform activities to prevent expansion of an event, mitigate its effects, and eradicate the incident; and
- Improvement Category: Ensure that organizational response activities are improved to incorporate lessons learned from current and previous detection/response activities.

Recover Function. Processes and procedures should be in place to recover from security incidents, and to restore any capabilities or services that were impaired. These include the following:

- Recovery Planning Category: Ensure execution of recovery processes and procedures to ensure timely restoration of systems affected by cybersecurity events;

- Improvements Category: Recovery planning and processes should be improved by incorporating lessons learned;
- Communications Category: Restoration activities should be coordinated with internal and external parties.

l. On the Horizon

In light of a series of major data breaches and other cyber attacks against major institutions, businesses, and entities that are part of critical infrastructure, there has been increasing recognition on the federal level of the growing risk of cyber attacks from both domestic and external sources, and the resultant exposures and disruptions to business, government operations and individuals' interests. Thus, over the last several years, the White House and federal agencies have issued policy frameworks and initiatives, and members of Congress have proposed numerous bills, in an effort to address privacy, data security and cyber security issues and risks and institute federal standards.

i. Proposed Federal Privacy, Data Security and Cyber Security Legislation

Numerous federal bills have been proposed with the goals of increasing consumer privacy and data security, combating breaches and theft from company and government computer networks, and imposing national breach notification requirements. While Washington policymakers and Congress had earlier seemed poised to enact legislation in this area, none of the recent proposals have gained sufficient momentum or bipartisan support, and there has been continuing debate on the balance between national security needs and individual privacy concerns that are sought to be addressed in many of the proposals.

The goals of the currently pending bills and the current White House legislative proposal vary, but most would impose information security program requirements upon certain types of entities, particularly those in the industrial and public sectors, and many would replace state data breach notification requirements with federal requirements. Summaries of certain more significant bills currently under consideration, as well as the White House legislative proposal, are provided below.

In an indication of the increasing attention that data and cyber security risks are generating from federal policymakers, there were a number of bills on the subject introduced in Congress in every session since 2011, with more expected until legislation, in some form, is passed.

(1) White House Proposals

Cybersecurity: In May 2011, the White House unveiled a comprehensive legislative proposal[348] for increased cyber security measures and standardization of notification of breach obligations. The Administration's proposal includes provisions for: (i) creating a national notification standard; (ii) synchronization of penalties for computer crime with other types of crime, including mandatory minimum penalties for cyber intrusions into critical infrastructure, enabling the Department of

---

[348] *See* fact sheet issued by the White House, available at http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf.

Homeland Security to help and collaborate with private sector entities in responding to a cyber intrusion; (iii) voluntary sharing of information of new cyber threats but with privacy oversight to ensure that such actions do not adversely affect civil liberties or individual privacy; and (iv) formalizing the Department of Homeland Security's role in managing cyber security and the Federal Information Security Management Act.

This was followed on February 12, 2013, by President Obama issuing an Executive Order titled "Improving Critical Infrastructure Cybersecurity,"[349] which formally acknowledged that "[t]he cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."[350] The President directed federal agencies to develop their own voluntary cybersecurity standards for critical parts of the private sector. The Order also requires federal agencies to produce unclassified reports of threats to U.S. companies and to share them in a timely manner. Additionally, the Order instructs federal agencies to ensure that privacy and civil liberties protections are incorporated into their activities. The Executive Order ultimately led to the development of the Cybersecurity Framework by the National Institute of Standards and Technology (see Section on Critical Infrastructure - The NIST Cybersecurity Framework, above) and President Obama renewing his call for Congressional action to enact cyber security legislation.

Surveillance Reform: In light of the revelations by Edward Snowden of the data monitoring and collection practices of the NSA, in March of 2014, President Obama announced a proposal to end the federal government's bulk telephone metadata collection program. President Obama proposed a new program in which among other reforms (1) the government will not collect telephone records in bulk, but rather the records would remain at the telephone companies; (2) the government would obtain such phone records only pursuant to individual orders from the Foreign Intelligence Surveillance Act ("FISA") Court that approve the use of specific phone numbers for searching; and (3) telephone companies would be compelled to provide technical assistance to ensure that the records provided to the government can be searched in a usable format.

Other Proposals. On January 23, 2014 the White House launched a 90 day review of "big data" and privacy that culminated in a set of policy recommendations on May 1, 2014.[351] The goal of the review was to analyze the ways in which big data would "affect the way we live and work; the relationship between government and citizens; and how public and private sectors can spur innovation and maximize the opportunities and free flow of this information while minimizing the risks to privacy."[352] The White House asked for comments from the public and has held public workshops around the country on questions including:

- What are the public policy implications of the collection, storage, analysis, and use of big data?

---

[349] Available at http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[350] *Id.*

[351] Big Data and the Future of Privacy, John Podesta, Jan. 23, 2014, http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy.

[352] Id.

- What types of uses of big data could measurably improve outcomes or productivity with further government action, funding, or research?

- What technological trends or key technologies will affect the collection, storage, analysis and use of big data?

- How should the policy frameworks or regulations for handling big data differ between the government and the private sector?

- What issues are raised by the use of big data across jurisdictions, such as the adequacy of current international laws, regulations, or norms?[353]

The report published by the White House's working group on big data at the end of this review highlighted six recommendations:

- Consumer Privacy Bill of Rights. The Department of Commerce solicit public comment on a Consumer Privacy Bill of Rights, based on Fair Information Practice Principles, with the ultimate goal of drafting proposed legislation.

- National Data Breach Notification Law. Congress should pass a law that established a national standard for data breach notification.

- Privacy Act of 1974. The Office of Management and Budget should apply the protections of the Privacy Act of 1974, which protects personal information held by the federal government, to non-U.S. persons where practicable.

- Education Data. The federal government should consider modernizing the Family Educational Rights and Privacy Act and Children's Online Privacy Protection Act to ensure data collected in schools is not misused, but also encourage innovation in educational technologies and methods.

- Expand Technical Expertise to Stop Discrimination. The several federal agencies that protect consumers and civil rights, including the Consumer Financial Protection Bureau and the Equal Employment Opportunity Commission should expand their technical expertise so that they may identify how big data analytics might have discriminatory impacts and develop plans for investigating and resolving such discrimination cases.

- Amend the Electronic Communications Privacy Act ("ECPA"). ECPA provides different levels of protection when the government seeks to access electronic communications held by third parties (such as an email provider) depending on how long the email has been stored - requiring probably cause and a search warrant for electronic communications that have been held for less than 180, but only a subpoena or similar court order for communications held for more than 180 days. The working group recommends Congress amend the law to

[353] Government ''Big Data''; Request for Information, Office of Science and Technology Policy, 79 Fed. Reg. 12251, 12251-52 (Mar. 4, 2014).

remove this distinction and "ensure the standard of protection for online, digital content is consistent with that afforded in the physical world."

(2) Congressional Proposals

Cybersecurity: In February 2012, members of the House Energy and Commerce Committee held a hearing in which they expressed bipartisan support for legislation addressing cyber threats. The Committee members agreed on several points, including the need for a national standard for data breach notification and the need to regulate Internet Service Providers ("ISPs"). Significantly, the members also stated that the government should give consideration to implementing reinsurance programs to help underwrite the development of cyber security insurance programs. They noted that such a government reinsurance program could be phased out as insurance markets gained experience with cyber security coverage. Meanwhile, however, government-sponsored reinsurance would be a means to help insurers and their insureds protect themselves from potentially enormous exposures.

On April 26, 2012, the House passed the Cyber Intelligence Sharing and Protection Act ("CISPA").[354] Although it passed in the House, this initial version of CISPA was the subject of controversy and the White House reportedly threatened to veto it unless changes were made to increase consumer privacy. CISPA would provide immunity to ISPs from privacy lawsuits for voluntarily disclosing customer information to the government about cybersecurity threats. Additionally, CISPA would allow ISPs to bypass privacy laws and share data with each other in an attempt to promptly stop a cyber attack. Although various companies such as Microsoft, Facebook, AT&T and Verizon supported the bill, privacy groups such as the ACLU, as well as President Obama, voiced disapproval with that version of CISPA on the basis that Americans' private data should not be shared with the military and that data sent to the government should be provided in a method that makes it anonymous, to protect privacy.[355]

Then on July 19, 2012, three Democratic Senators (Senators Feinstein, Rockefeller, and Carper), one Republican Senator (Senator Collins), and one independent Senator (Senator Lieberman) introduced a revised version of their Cybersecurity Act of 2012, in an attempt to obtain the bipartisan support needed for passage. The revised Act no longer had mandatory minimum security standards, but instead created a voluntary system under which private companies would adhere to best practices in exchange for incentives, such as federal assistance on cyber issues and immunity after a cyber attack.[356] The revised Act also:

- Requires designated critical infrastructure (systems that if attacked could cause catastrophic consequences) to report significant cyber incidents.

---

[354] David Kravetz, *House Passes Controversial Cybersecurity Measure CISPA*, Wired, Apr. 26, 2012, http://www.wired.com/threatlevel/2012/04/house-passes-cispa/.

[355] Executive Office of the President – Office of Management and Budget, *Statement of Administration Policy*, Apr. 25, 2012, http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf; Ateghah Khaki, *House of Representatives Passes Privacy-Busting CISPA*, American Civil Liberties Union, Apr. 26, 2012, http://www.aclu.org/blog/technology-and-liberty-national-security/house-representatives-passes-privacy-busting-cispa.

[356] *See* S. 3414. *See also Senators Unveil Revamped, Obama-Backed Cyber-Security Bill*, PC Magazine Online, Jul. 20, 2012.

- Allows the owners of critical infrastructure to participate in a voluntary cybersecurity program.

- Requires the government to improve the security of federal civilian cyber networks via reform of the Federal Information Security Management Act.

- Allows private industry to develop and recommend to a National Cybersecurity Council, chaired by the secretary of Homeland Security, various voluntary cybersecurity practices to mitigate cyber risks.

The Cybersecurity Act of 2012 received much press attention prior to the Congressional recess in July 2012, partly because of an op-ed article written by President Obama in which he urged the Senate to pass the bill.[357] The bill, however, fell eight votes short of the necessary 60 votes to pass the Senate.[358] Many Senators, led by Senator McCain, opposed the bill, based on concerns that such security standards would impose unfair costs on businesses.

CISPA was re-introduced in the House, and was passed in the House in a controversial vote on April 18, 2013 by a vote of 288-127.[359] As of April 2014, it still had not been voted on in the Senate, and a vote may be unlikely.

The President's senior advisors publicly stated on April 16, 2013 that they would recommend that the President veto the bill if it is presented to him for signature.[360] According to public statements, the Administration agrees that there is a need for cybersecurity legislation to clarify the application of existing laws to remove legal barriers for the appropriate sharing of cybersecurity information among the private sector.[361] The Administration, however, voiced concern about the broad scope of CISPA, on the basis that the law should not immunize a failure to take reasonable measures to prevent harm when and if the private sector entity knows that such inaction would cause damage or otherwise injure or endanger other entities or individuals. Further, the Administration stated that it believes that information sharing is one piece of a larger set of legislative requirements to provide the private sector, federal government and law enforcement "with the necessary tools to combat the current and emerging cyber threats facing the Nation."[362] The Administration has also noted that

---

357 Barack Obama, *Taking the Cyberattack Seriously*, The Wall Street Journal, Jul. 19, 2012, available at http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html. President Obama wrote that it "would be the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries."

358 *Cyber Security Law Fails to Pass Senate Before Month-Long Break*, Huff Post Tech, Aug. 2, 2012, http://www.huffingtonpost.com/2012/08/02/cyber-security-law_n_1733751.html.

359 Govtrack.us, http://www.govtrack.us/congress/votes/113-2013/h117. CISPA was amended in various forms before it was voted upon but many believe that the amendments did not make any substantive changes. For example, one proposed amendment would have designated the Department of Homeland Security ("DHS") as the central agency for receiving company data in an effort to limit the scope of government sharing. The amendment, however, was modified before the vote in the House, and the final version of the Amendment merely stated that DHS would be the primary point of contact for reporting by companies. Adi Robertson, *House passes revamped CISPA cybersecurity bill amidst warnings of 'digital bombs'*, The Verge, Apr. 18, 2013, http://www.theverge.com/2013/4/18/4234096/house-of-representatives-passes-cispa-2013.

360 Statement of Administration Policy, Executive Office of the President – Office of Management and Budget, Apr. 16, 2013, located at http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf.

361 *Id.*

362 *Id.*

Congress should incorporate safeguards for privacy and civil liberties into cybersecurity legislation that:

(1) strengthens the Nation's critical infrastructure's cybersecurity by promoting the establishment and adoption of standards for critical infrastructure;

(2) updates laws guiding Federal agency network security;

(3) gives law enforcement the tools to fight crime in the digital age; and

(4) creates a National Data Breach Reporting requirement.[363]

Additionally, the White House recently responded to an anti-CISPA online petition (collecting over 117,000 signatures) and confirmed that any "cybersecurity legislation must not violate Americans' right to privacy."[364]

In the year since passage in the House, the Senate has not voted on CISPA, and reportedly will not do so.[365] Particularly in light of the revelations by Edward Snowden about U.S. surveillance programs, the authors of the House bill have since deemed it unlikely that CISPA will pass in anything resembling its current form.[366]

Surveillance Reform: On May 7, 2014 the House Judiciary Committee voted unanimously to advance an amended USA Freedom Act that would outlaw bulk collection of phone records by the federal government and does not require phone companies to maintain phone records longer than they would in the normal course of business. Critics argue that the bill does not go far enough as it was amended to allow for collection of phone records (and the metadata of those two degrees of separation from the suspect) in certain cases. Also, the bill does not include a special advocate to represent the privacy interests of the subject of the investigation before the FISA courts, where the subject would not be present. The House Intelligence Committee then unexpectedly passed this same bill out of committee on May 8, 2014 rather than its own competing bill that had been scheduled for consideration that day.

Data breach Notification. In the meantime, several senators have (again) proposed nationwide data breach notification laws to address the growing patchwork of state laws and several high profile data breaches. Republican Senator Patrick Toomey introduced one such bill in June 2013, which would require reasonable measures to protect electronic data containing personal information and require either written, electronic, or telephonic notification of data breaches.[367] In early January 2014, Democrat Senator Patrick Leahy introduced the Personal Data Privacy and Security Act of

---

363 *Id.*

364 Official White House Response by Todd Park and Michael Daniel to the Stop CISPA Petition, Apr. 30, 2013, https://petitions.whitehouse.gov/petition/stop-cispa-cyber-intelligence-sharing-and-protection-act/19sQhBpy.

365 *Senate Won't Vote on CISPA, Deals Blow to Controversial Cyber Bill*, Huff Post Tech, Apr. 25, 2013, http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html.

366 *CISPA author Rogers: Snowden 'hurt our chances' for cyber bill*, The Hill, Sept. 25,2013, http://thehill.com/blogs/hillicon-valley/technology/324539-surveillance-leaks-hurt-cybersecurity-talks-but-legislation-still-needed-cispa-author-says.

367 S. 1193, 113th Cong. (2013).

2014, the fifth time he has introduced such legislation since 2005.[368] This bill would apply to businesses that "compile, access, use, process, license, distribute, analyze or evaluate" personally identifiable information on 10,000 or more U.S. persons and would require notification of a breach within 60 days of discovery, but does not preempt states from adding specific information that must be included in data breach notices.[369] Just a few days after introducing this bill, Democrat Senator Tom Carper introduced the Data Security Act of 2014, which would apply more broadly than Senator Leahy's bill, but entirely preempt state law.[370]

ECPA Reform: Legislation pending in both houses of Congress would amend ECPA as recently proposed by the White House's big data working group. In the Senate, the proposed Leahy-Lee Electronic Communications Privacy Act Amendments Act would extend the warrant requirement to all stored data and requires that the government notify the individual whose account was disclosed. This has already been passed out of Committee on April 25, 2013. In the House, the Email Privacy Act does the same. As of May 9, 2014, the bill is in Committee and cosponsored by 208 Representatives from both sides of the aisle. One potential roadblock in passing either of these bills is that the Securities and Exchange Commission has been pushing Congress for an exception in any ECPA reform that would allow it to obtain emails with subpoenas rather than warrants in its enforcement investigations.

ii. Federal Agency Privacy Frameworks

In addition to the NIST Cybersecurity Framework referenced above, the Federal Trade Commission and the Department of Commerce have both unveiled privacy frameworks outlining policy recommendations, which are expected to be influential in shaping forthcoming legislation. The Securities and Exchange Commission (SEC) is in the process of evaluating what role it can play in mitigating cybersecurity risks.

(1) Federal Trade Commission

In March 2012, the FTC issued a report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*,[371] which sets forth a framework of best practices for how companies should protect consumers' privacy, and is intended to inform policymakers as they develop solutions, policies and potential laws governing privacy. The report is also intended to guide and motivate the business community as it develops more robust and effective best practices and self-regulatory guidelines.

The proposed framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device. A preliminary version of the report recommended that the framework would apply to all such entities but the final report concludes that the framework should not apply to companies that collect and do not transfer only non-sensitive data from fewer than

---

368 S. 1897, 113th Cong. (2014).

369 *Id.*

370 S. 1927, 113th Cong. (2014).

371 Available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

5,000 consumers each year, a change borne out of recognition of the potential burden on small businesses.

Among the guidelines outlined in the proposed framework are: (i) building privacy protection into everyday business operations and at every stage in product development; (ii) providing choices to consumers about their data practices in a simpler, more streamlined way and providing a "Do Not Track" option; (iii) making data practices more transparent to consumers; (iv) providing consumers with reasonable access to the data that companies maintain about them; and (v) undertaking a broad effort to educate consumers about commercial data practices and the choices available to them.

The FTC also recommends that Congress consider general privacy legislation, data security and breach notification legislation, and data broker legislation. It also urges individual companies and self-regulatory bodies to accelerate the adoption of the principles contained in the framework, and recommends that data brokers who compile consumer data for marketing purposes should explore the creation of a centralized website where consumers could get information about their practices and options for controlling the use of the data.

Over the first half of 2014, the FTC is hosting a "Seminar Series on Emerging Consumer Privacy Issues" that will ultimately result in staff reports on the topics discussed.[372] The first of these seminars tackled mobile device tracking[373] and the second addressed alternative scoring products to determine consumers' access to products and offers.[374] The final seminar, is on "Consumer Generated and Controlled Health Data" in May 2014.[375]

The FTC has been very active in enforcing privacy and data security. (See Section III.2. on FTC Regulation of Privacy and Data Protection, above; see also Section III.c. on Federal Trade Commission "Red Flags" Rule, above).

(2) U.S. Department of Commerce

The U.S. Department of Commerce Internet Policy Task Force issued a green paper entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (the "2010 Green Paper") in December, 2010.[376] The 2010 Green Paper detailed initial policy recommendations aimed at promoting consumer privacy online while ensuring that the Internet remains a platform that spurs innovation, job creation, and economic growth. Key recommendations set forth in the 2010 Green Paper include: (i) consider establishing fair information practice principles comparable to a "Privacy Bill of Rights" for online consumers; (ii) consider developing enforceable privacy codes of conduct in specific sectors with stakeholders; (iii)

---

[372] FTC to Host Spring Seminars on Emerging Consumer Privacy Issues, Federal Trade Commission, Dec. 2, 2013, http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues

[373] Spring Privacy Series: Mobile Device Tracking , Feb. 19, 2014, http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking

[374] Spring Privacy Series: Alternative Scoring Products, March 19, 2014, http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products

[375] Spring Privacy Series: Consumer Generated and Controlled Health Data, May 7, 2014, http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data

[376] Available at http://www.commerce.gov/node/12471.

create a privacy policy office in the Department of Commerce; (iv) encourage global interoperability to spur innovation and trade; (v) consider how to harmonize disparate security breach notification rules; and (vi) review the Electronic Communications Privacy Act for the cloud computing environment.

In June 2011, the Department of Commerce issued another green paper, entitled *Cybersecurity, Innovation and the Internet Economy* (the "2011 Green Paper"), addressing the economic importance of strengthening cybersecurity protection and preserving consumer trust in the Internet.[377] The Task Force recognized that the threat of cybersecurity attacks has grown as Internet business has grown. Key recommendations in the 2011 Green Paper include: (i) the establishment of nationally recognized but voluntary codes of conduct to minimize cybersecurity vulnerabilities; (ii) the development of incentives to combat cybersecurity threats;[378] (iii) the improvement of the public understanding of cybersecurity vulnerabilities through education and research; and (iv) the enhancement of international collaboration on cybersecurity best practices to support expanded global markets for U.S. products.

In March 2013, as part of an effort to prepare a report identifying ways to incentivize companies and organizations to improve their cybersecurity, the Department of Commerce issued a series of inquiries for public response.[379] Forty-five different entities, including energy companies, technology companies, governmental agencies and consultants, provided responses.[380] This ultimately led to a series of recommendations[381] that were instrumental in NIST's development of the Cybersecurity Framework. (See Section on Critical Infrastructure – The NIST Cybersecurity Framework, above).

(3) Securities and Exchange Commission

In March 2013, the SEC proposed Regulation SCI, which would require certain market participants to have policies and procedures in place to protect their electronic systems.[382] Despite a comment deadline in May 2013, the SEC has not yet adopted its proposed rules. Rather, the SEC has continued to solicit input from industry and other stakeholders on its proper and most effective role in reducing the risks that the financial industry faces from cyber attacks. On March 26, 2014, the SEC held a roundtable discussion on this topic, and related topics, including disclosures of cyber

---

377 Available at http://www.commerce.gov/sites/default/files/documents/2011/june/cybersecurity_green_paper_finalversion_0.pdf.

378 According to the 2011 Green Paper, these incentives could include the reduction of cyber insurance premiums for companies that adopt best practices and openly share details about cyber attacks for the benefit of other businesses.

379 A Chance to Comment on Commerce's Report on Cybersecurity Incentives, Mar. 28, 2013, http://www.commerce.gov/blog/2013/03/28/chance-comment-commerce%E2%80%99s-report-cybersecurity-incentives. Notice of Inquiry available at http://www.ntia.doc.gov/federal-register-notice/2013/notice-inquiry-incentives-adopt-improved-cybersecurity-practices.

380 Responses are available at http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi.

381 Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program, Department of Commerce, Aug. 8, 2013, http://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf.

382 Regulation Systems Compliance and Integrity, Release No. 34-69077; File No. S7-01-13, https://www.sec.gov/rules/proposed/2013/34-69077.pdf

risk and data breaches, the role of boards of directors with regard to cyber risk, and simulations to identify problem areas and improve defenses.[383] (See Section on Regulation S-P and SEC Enforcement of Privacy, Data Protection and Cybersecurity, above; see also Section on SEC Guidance Regarding Public Company Obligations to Disclose Cyber Security Risks and Incidents to Investors, above).

iii. Additional Federal Developments

Cyber security in all senses is clearly a growing concern of the federal government, as demonstrated by both the legislative and agency developments discussed above, and additional Obama administration initiatives.

(1) Office of the Cyber Czar

Shortly after taking office, President Obama announced the creation of the office of "Cyber Czar" – a national cyber security chief to oversee the security of the U.S. communications networks and electronic infrastructure, in May 2009. On April 15, 2011, through the Cyber Czar, the Administration issued its final National Strategy for Trusted Identities in Cyberspace guidelines, aimed at establishing identity solutions and privacy-enhancing technologies that will make the online environment more secure and convenient for consumers.[384]

(2) Government Accountability Office Reports

In early 2013, the U.S. Government Accountability Office ("GAO") issued a report titled "Cybersecurity – National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented" (the "GAO Report")[385] in which it summarized several key challenge areas in the federal government's approach to cybersecurity. The GAO stated that the increase in risks is demonstrated by the "dramatic increase in reports of security incidents" and the ease of obtaining and utilizing hacking tools as well as the advances in the effectiveness and sophistication of the attack technology. The GAO also recognized that cyber attacks could have a potentially devastating impact on the nation's computer systems and networks and could disrupt government and business operations as well as the lives of individuals.

The GAO Report focuses on the increasing threat to sensitive information at risk that has potentially serious impacts on federal and military operations and critical infrastructure. According to the GAO Report, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team increased by 782% from 2006 to 2012.

According to the GAO Report, the many continuing cyber security challenges that are faced by the federal government identify the need for a clearly defined oversight process to ensure that individual agencies are held accountable for implementing effective information security programs.

---

383 *SEC Holds Cybersecurity Roundtable*, Digilaw Blog, March 31, 2014, http://digilaw.edwardswildman.com/blog.aspx?entry=5317.

384 Additional information regarding the NSTIC Initiative is provided on its website, http://www.nist.gov/nstic/index.html.

385 United States Government Accountability Office, Cybersecurity – National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, GAO-13-187, Feb 14, 2013.

However, the Report recognizes that until there is a national cyber security strategy that addresses all of the necessary key elements, progress is likely to remain limited.

The GAO recommends that the White House develop an overarching federal cyber security strategy. Additionally, the GAO recommends that the strategy ensure that federal agencies are held accountable for making significant improvements in cyber security and that Congress consider legislation to better define roles and responsibilities for implementing and overseeing federal information security programs.

On November 15, 2013, the GAO released another report entitled *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*.[386] In this report, the GAO noted that self-regulation has thus far been inadequate at protecting consumer privacy and recommended federal legislation to provide such protection. This legislation, the GAO suggested, should generally give consumers the right to access and correct information held about them by private companies, and align with Fair Information Practice Principles. However, the GAO stopped short of recommending specific laws, and acknowledged the challenge in providing sufficient protection to individuals, without stifling innovation and commerce, which bring their own benefits to consumers.[387]

3. PCI -The Payment Card Industry Standards for Protection of Credit Card Information

The Payment Card Industry Security Standards Council is an international organization founded by American Express, Discover Financial Services, JCB International, MasterCard, Visa Inc. and Visa Europe (referred to as the "Brands"). It was started to develop and manage certain credit card industry standards for credit, debit and other payment cards (including store and company purchasing cards carrying the label of a PCI Brand member).

a. PCI-DSS

The Payment Card Industry Security Standards Counsel has developed Payment Card Industry Data Security Standards (generally referred to as "PCI-DSS"). The standards are periodically updated incorporated into the contractual agreements binding the various entities involved in the chain of payment card processing, and are enforced by fines and other assessments imposed through those agreements. 2014 is the tenth year of PCI DSS, and it has recently instituted what it refers to as PCI 3.0 version of its standards.[388]

PCI-DSS is a set of industry standards created and periodically updated to help protect the security of electronic payment card transactions that include Personal Information of cardholders, and

---

386 Nov. 15, 2013, http://www.gao.gov/products/gao-13-663.

387 Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace, at 46, http://www.gao.gov/assets/660/658151.pdf.

388 The effective date of the version 3.0 of the standards is January 1, 2014, but existing PCI DSS 2.0 compliant vendors reportedly have until January 1, 2015 to move to the new standard. See https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=padss

operate as an industry requirement for security for organizations utilizing credit card information. PCI-DSS applies to all entities that store, process or transmit cardholder data.[389] It imposes requirements upon those entities for security management, policies, procedures, network architecture, software design, and other critical measures that help to protect customer credit and debit card account data. As a large number of malicious data breaches are targeted at obtaining electronically transmitted, collected or stored payment card information, PCI-DSS compliance is often one of the first aspects investigated when a breach occurs involving payment card information. The effectiveness of the PCI-DSS requirements for minimizing the risk of data breach is a subject of some debate; however, compliance with existing PCI-DSS is still "a major issue" with research showing that only one in ten organizations were fully compliant at the time of their baseline assessment, [390] with organizations that suffered a data breach less likely to be PCI-DSS compliant at the time of their breach – even if compliant at the time of their last annual assessment – than the average of companies assessed.[391]

Merchants and service providers are categorized according to the number of credit card transactions they process in a 12-month period, and compliance obligations differ depending on such designations. For example, a Level 1 designation indicates that the merchant is among those with the largest number of transactions and the greatest level of security required. Level 1 merchants process more than six million credit card transactions annually, across all channels, including the Internet, and must perform an on-site PCI data security assessment on an annual basis and network scans on a quarterly basis.

The brands' regulations and their agreements with card association members generally provide for the imposition and collection of fines and penalties against organizations that fail to comply with PCI-DSS standards. These assessments are often passed along the chain of entities involved in payment card transactions through contracts with indemnification provisions. Thus, the obligation to comply with these standards and the imposition of fines and penalties involved are essentially contractual private arrangements rather than government regulatory schemes, although government entities are starting to adopt these standards, as discussed below. The deviation from PCI-DSS standards also can be used as evidence of departure from industry standards in both industry investigations and third-party lawsuits.

When a data breach occurs involving credit card information maintained by an entity subject to PCI-DSS, and the breached entity has not satisfied PCI-DSS standards, the associated fines and contractual assessments can be quite substantial. Each brand has its own rules and labels for such assessments and what qualifies as a data compromise event subject to these assessments, and these rules are modified periodically. Such assessments, imposed separately by each card association, can include:

- Fines for violation of PCI-DSS non-compliance, and possibly additional fines for prohibited data retention;

---

389 *See, e.g.*, PCI DSS Quick Reference Guide, PCI Security Standards Counsel, available at https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf.

390 Verizon, *2014 PCI Compliance Report.* at p. 6.

391 *Id.* at p. 8

- Significant additional monthly fines until confirmation of compliance;
- Assessments referenced by card associations as for "Incremental Counterfeit Fraud" or "Fraud Recovery" that the card associations identify as being potentially tied to a security data breach;[392] and
- Assessments by the card associations on behalf of themselves and/or their members for "Operational" expense reimbursement;.[393]
- Additional administrative assessments.

In addition, after a breach, a merchant's classification or tier will usually be adjusted upwards to Level 1, regardless of the number of credit card transactions it processes, resulting in the imposition of further obligations and potentially even greater assessments should another breach occur. Merchants are responsible for all costs associated with any system modifications required to achieve PCI-DSS compliance.

The Brands are currently in an effort to enforce a shift in the U.S. to payment cards using microchips rather than the magnetic strips that are more vulnerable to having data on them stolen and copied, with acquirers, processors and subprocessors supposed to have had the capability to process chip-enabled cards by April 2013 (referred to as EMV cards, based on initial development by Euromoney, MasterCard and Visa). . Effective October 1, 2015, the Brands will impose a shift in the current liability system whereby the party who does not support the chip cards, either the card issuing bank or the merchant and its bank, will bear the liability for counterfeit card fraud. Visa and MasterCard have issued rules and guidelines for processors and merchants to support EMV chip technology..[394]

Issues as to the nature of validity and enforceability of card brand assessments, and whether their nature is that of fines and penalties versus reasonably calculated reimbursement for fraudulent transactions and card monitoring and replacement costs resulting from a data breach, have recently been raised in several lawsuits. For instance, in 2011, a Utah restaurant filed a counterclaim against its acquiring bank and payment processor, after the bank and processor demanded indemnification for fines and penalties assessed by Visa and MasterCard arising from an alleged data breach at the

---

[392] *See, e.g.*, Visa's Global Compromised Account Recovery ("GCAR") program, available at http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf; *see also, e.g.*, MasterCard's Account Data Compromise program, available at http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf.

[393] For instance, under Visa's Global Compromised Account Recovery program, *supra*, "Operating Expense Recovery . . . is $2.50 per eligible account" for qualifying events. Visa's Global Compromised Account Recovery ("GCAR") program was introduced in April 2012. Under Visa's prior program (Visa's Account Data Compromise Recovery process), a $1.00 multiplier was used. *See, e.g.*, Updated Account Data Compromise Recovery (ADCR) Frequently Asked Questions, Visa Inc. (2008), at p. 9. For a description of MasterCard's "Operational Reimbursement" calculation, see Section 10.2.5.4 of MasterCard's Security Rules and Procedures, available at http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf.

[394] See http://www.mastercardadvisors.com/_assets/pdf/emv_us_aquirers.pdf; http://usa.visa.com/download/merchants/visa-merchant-chip-acceptance-readiness-guide.pdf; http://www.emvc.com

https://www.chasepaymentech.com/faq_emv_chip_card_technology.html; http://www.smartcardalliance.org/pages/publications-card-payments-roadmap-in-the-US; http://www.emvco.com.

restaurant. The restaurant argued that the bank and card processor improperly demanded indemnification from the restaurant, and collected payment from the restaurant's bank account, for the card brand assessments despite, according to the pleading: "Neither the alleged data breach nor any resulting fraud loss has ever been proved;" "[The merchant restaurant] was not given an opportunity to challenge the assessments or present evidence in its defense;" "Visa did not follow its own rules in assessing liability;" and "The fines and penalties were punitive in that they bore no relationship to the non-existent harm to Visa or MasterCard." The case was filed in Utah state court.[395]

In March 2013, another merchant (a specialty retailer) brought suit directly against Visa after Visa allegedly assessed approximately $13 million in "non-compliance fines and issuer reimbursement assessments that Visa wrongfully imposed and collected from" the merchant's acquiring banks following a data breach, according to the complaint. The complaint also alleged that the acquiring banks in turn collected that amount from the merchant through the merchant's "contractual obligation to indemnify the Acquiring Banks against such wrongful assessments." The merchant further alleged that the assessments constituted "unenforceable penalties" and that "Visa had no reasonable basis for concluding that [the merchant] was non-compliant with the PCI DSS requirements at the time of the Intrusion or at any other relevant time." The suit is currently pending Tennessee federal court.[396]

Similar issues were raised by a breached merchant against it payment processor and bank, based on the assessments collected by them from the merchant, as the retailer's agreement with its payment processor allegedly had a limit of liability clause that limited the retailer's indemnification obligation to it payment processor for reimbursement of losses claimed by issuing banks, which limitation did not apply to "fees, fines, and penalties assessment by payment card networks."[397] Thus, the complaint raises the issue of what is a loss versus a fee, fine or penalty.

b. Incorporation of PCI-DSS into State Law

Several states, such as Minnesota, Nevada and Washington, have incorporated PCI-DSS requirements into their data protection laws, as detailed below.

---

395 *See Elavon Inc. v. Cisero's Ristorante Inc.*, No. 100500480 (3rd Dist. Ct., Summit County, Utah). On March 21, 2013, the court dismissed the merchant restaurant's second amended answer and counterclaim cause of action for negligence, on the basis that this claim was barred by the economic loss doctrine under Utah law (the court found that the restaurant could not establish a duty owed by the bank or payment processor "independent of any contractual obligations between the parties"). The merchant's remaining counterclaims, which include breach of contract, conversion, and breach of fiduciary duty, survived.

396 *See Genesco Inc. v. Visa U.S.A. Inc. et al*, Case No. 3:13-cv-00202 (U.S. District Court, Middle District of Tennessee). Causes of action alleged in the suit by the merchant include breach of contract, breach of the implied covenant of good faith and fair dealing, violation of the California Unfair Business Practices Act, and unjust enrichment. Early motions were denied, with the parties proceeding to discovery, much of it filed under seal, and trial scheduled for the end of 2014.

397 *Schnuck Markets, Inc. v. First Data Merchant Data Services Corp. and Citicorp Payment Services, Inc.*, Case No. 4:13-CV-2226-JAR (U.S. District Court, Eastern District of Missouri). A motion by Schnuck for judgment on the pleadings is pending as of May 2014.

i. Minnesota

The Minnesota Plastic Card Security Act,[398] enacted on May 21, 2007, was the first of its kind. This act prohibits companies doing business in Minnesota from retaining card security code data, PIN verification code numbers or the full contents of any track of magnetic stripe data following authorization of a transaction, for longer than 48 hours following authentication of a PIN debit transaction. The act provides for liability to financial institutions that issued a payment card (*e.g.*, issuing banks) for certain costs of reasonable actions undertaken by them in the event of a breach exposing such data when it is stored in violation of the Act.

ii. Nevada

An amendment to Nevada data protection law that became effective January 1, 2010, requires companies doing business in Nevada that accept payment cards to comply with PCI-DSS.[399] The amendment also requires that other data collectors doing business in Nevada encrypt personal information contained in certain kinds of transmissions and when stored on a data storage device.

iii. Washington

Under a Washington law effective July 1, 2010, if a credit or debit card processor or business fails to take reasonable steps to guard against unauthorized access to account information that is in its possession, and such failure is found to be the proximate cause of a breach, the processor or business is liable to financial institutions such as banks that issued the credit cards for reimbursement of their reasonable actual costs related to the reissuance of credit or debit cards, even if the financial institution has not suffered another injury as a result of the breach.[400] The processor or business may also be liable to the financial institution for attorneys' fees and costs incurred in connection with any legal action. In addition, vendors of card processing software and equipment may be held liable for the damages incurred by a financial institution if the vendor's negligence was the proximate cause of such damages. The new law provides for several exemptions. Processors, businesses and vendors that are compliant with PCI-DSS at the time of the breach are not liable to financial institutions. They are considered to be compliant if their PCI data security compliance was validated by an annual assessment, and if the assessment took place no more than one year prior to the date of the breach. In addition, processors, businesses and vendors are not liable if the breach involved encrypted card information.

As there is increasing regulatory scrutiny on data breaches involving payment card information in which the breached entity is not PCI-DSS compliant, other states may soon follow in incorporating PCI-DSS requirements into their data breach laws.

---

398 Minn. Stat. § 325E.64.

399 Nev. Rev. Stat. § 603A.215.

400 Wash. Rev. Code § 19.255.

IV. THE REGULATORY AND STATUTORY LANDSCAPE OUTSIDE THE U.S.

a. Introduction to the International Scope of Privacy and Data Protection

Global compliance with data protection laws presents an increasing challenge, as the number of jurisdictions with such laws increase and the multi-jurisdictional scope of business operations and customers increases. It is trite to say that the flow of data in today's digitalized world may not recognize international borders and yet when data crosses into different legal jurisdictions, the rules that apply to it may change. Whilst there have been some attempts by privacy regulators to cooperate on the development of international standards[401], there is still no recognized set of international standards. Moreover, given that over 90 countries have enacted data protection laws[402] (a number that is increasing), the regulatory challenges facing multi-national companies are substantial. Added to this, the penalties for non-compliance with data protection laws also seem set to increase.[403]

Many companies' operations may be affected by the data security laws of multiple countries, apart from the jurisdiction in which they are domiciled. Many companies have subsidiaries, affiliates or employees in other countries. Thus, taking the example of breach notification (noting that this is not a central plank of data protection law in many non-U.S. jurisdictions, including the European Union), a U.S. company that sustains a breach that includes Personal Information of international customers may need to consider carefully the impact of the data security and breach notification laws of other countries, and whether they impose reporting or notification obligations on the U.S. breached company. Breach notification requirements of various countries are described in the World Law Group Global Guide to Data Breach Notification Requirements.[404]

In addition to the Member States of the European Union ("E.U."), over 45 other countries now have data protection or privacy laws and others are in the process of developing them. Some of those with existing laws are contemplating revising them to enhance obligations, and increase penalties for non-compliance.

Aspects of the E.U. Data Protection Directive, as well as selected countries' national laws and enforcement powers, are considered below.

b. The Dilemma of Whistleblower Hotlines

Many multi-national companies have implemented whistleblower hotlines, which permit employees and service providers to report allegations of fraud, infractions of codes of conduct or similar

---

401 For example, the Madrid Resolution on International Standards on the Protection of Personal Data and Privacy of 2009 was approved by more than 50 countries at the 31st International Conference of Data Protection and Privacy Commissioners, but has failed to become influential.

402 Greenleaf, Graham, Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. Available at SSRN: http://ssrn.com/abstract=2000034

403 For example, the European Parliament's draft of the EU Data Protection Regulation would allow national DPAs to impose fines of up to 5% of the worldwide gross revenue of an infringing organization.

404 This is available at the www.globaldatabreachguide.com.

complaints. For U.S. companies, such hotlines are often part of compliance with the Sarbanes-Oxley Act of 2002, the Foreign Corrupt Practices Act of 1977 or other U.S. laws.

Implementing such hotlines in E.U. Member States gives rise to certain data protection issues which should be given careful consideration.[405] In some Member States, amendments must be made to the hotline reporting procedure in order to comply with local laws or guidelines. Certain issues which may arise in selected Member States are considered below. In February 2006, the Article 29 Working Party issued an opinion[406] to provide guidance to industry in establishing whistleblower hotlines throughout the E.U. that were compliant with both the Sarbanes-Oxley Act and the Data Protection Directive, although individual Member States' laws and guidance must still be considered.

Most E.U. Member States require notification of hotlines to the relevant data protection authority (DPA), and in some Member States hotlines cannot be operated until approval has been obtained. Where hotlines involve the transfer of personal data from the E.U. to the U.S., Member States will require certain contractual and technical security measures to be in place. Company works councils may need to be consulted prior to the implementation of a whistleblower hotline.

The World Law Group has published a Global Guide to Whistleblowing Programs, which provides a brief overview of legislation governing whistleblowing programs in a number of countries.[407]

c. The European Union

The E.U. Data Protection Directive and the rules for determining when a particular Member State's laws apply are considered below. Many U.S. companies maintain subsidiaries, affiliates or employees in the E.U and such companies, whether or not publicly traded, must comply with relevant E.U. Member States' data protection laws and guidelines where "personal data" (as defined by the pertinent law) is collected, processed or transferred by local operations. Moreover, because E.U. data protection law requires that personal data may only be transferred to a non-European Economic Area country[408] where that country ensures an adequate level of protection for that data, this demands (albeit indirectly) that U.S. companies wishing to engage with E.U. consumers or businesses adhere to E.U. data protection standards. [409]

---

[405] See World Law Group Global Guide to Whistleblowing Programs (2012), available at http://www.theworldlawgroup.com/?cm=Doc&ce=details&primaryKey=53535; *see also* Mark Schreiber, *The Practitioner's Guide to The Sarbanes-Oxley Act*, Volume II, Chapter 9 – *Anonymous Sarbanes-Oxley Hotlines for Multi-National Companies: Compliance with EU Data Protection Laws*, 2009, and http://www.ico.gov.uk/news/blog/2011/half-term-report-on-cookies-compliance.aspx.

[406] Opinion 1/2006 on the application of E.U. data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

[407] Available at http://w.theworldlawgroup.com/files/file/WLG%20Global%20Guide%20to%20Whistleblowing%20Programs-2012-Web.pdf.

[408] The European Economic Area or EEA comprises the Member States of the European Union (excluding Croatia who's EEA membership is pending approval by all EEA states) plus Iceland, Liechtenstein and Norway.

[409] See *Handbook on European data protection law*, published by the European Union Agency for Fundamental Rights, 2013, Council of Europe, 2013. The Handbook, and any updates to it, are available at the FRA website at fra.europa.eu and at the Council of Europe website at coe.int/dataprotection, and on the European Court of Human Rights website under Case-Law menu at echr.coe.int.

The main criteria in determining which Member States' laws apply are the location of the establishment of the data controller and, where the data controller is established outside the EEA, the location of the equipment used by the controller to process the data. To illustrate this with three simple examples:

(a) Where a controller is established in one Member State, the national law of that Member State will apply.

(b) Where a controller has an establishment in two or more Member States the national law of the host Member State will apply to the data controller based therein, provided the processing is carried out in the context of the activities of that controller. Where the activities are carried out in the context of only data controller, then its host's laws will apply to every establishment.

(c) Where a controller is not established in any Member State, the law of each applicable Member State in which the data controller uses equipment to process the data will apply.

i. E.U. Data Protection Directive

E.U. Member States' data protection laws are based on E.U. Directive 95/46/EC, known as the "Data Protection Directive." Member States are required to implement the Data Protection Directive by passing national laws. There is considerable variation between Member States' interpretation and implementation of the Data Protection Directive, and thus individual Member States' laws must be considered as well as the Data Protection Directive.

Under the Data Protection Directive, responsibility for compliance rests with the "data controller," who is the natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data. Subject to certain exceptions, data controllers are required to notify their national DPA of their data processing activities.

The Data Protection Directive requires data controllers to process personal data only in accordance with certain data protection principles, including the requirements that data be processed fairly and lawfully, that there be a justification for processing, and that there be implementation of appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

Under the Data Protection Directive, the meaning of "personal data" is broader than the term "Personal Information" generally applicable in the U.S. (and broader than as used elsewhere in this White Paper). It includes any information relating to an identified or identifiable natural person.

Controllers are prohibited from transferring personal data to countries outside the E.U. that do not ensure an adequate level of protection of personal data. The U.S. is not currently considered to provide such an adequate level of protection,[410] and thus personal data may not be transferred from

---

[410] Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the U.S. Government, EC Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data.

the E.U. to persons in the U.S. without additional protections. Such additional protections include the transferee being enrolled in the Safe Harbor program,[411] under which the transferee voluntarily agrees to be bound by data protection rules broadly equivalent to those set out in the Data Protection Directive, or entering into a compliant data transfer agreement. The European Commission has the authority to determine whether a country ensures an adequate level of protection by reason of its domestic law or international commitments. It has deemed there to be an adequate level of protection in other jurisdictions (including Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, and Switzerland),[412] pursuant to Model Contracts,[413] pursuant to "binding corporate rules"[414] or pursuant to another relevant exception.

U.S. companies may encounter such a prohibition on transfer in a wide range of circumstances. For example, in a U.S. court case,[415] a Utah court ordered a U.S. company to disclose customer complaint data that was relevant to a claim that had been filed against it, notwithstanding that the data was located in Germany and the transfer to the U.S. may breach German data protection laws. The court was not sympathetic to the dilemma faced by the U.S. company. One concern is that to allow other countries' data transfer restrictions to trump U.S. court directions to produce information in U.S. legal proceedings could operate to encourage transfer of sensitive and perhaps unfavorable information outside the U.S. in jurisdictions that render transfer back into the U.S. difficult.

Traditionally, DPAs of each Member State have tended to enforce data protection legislation independently of other Member States. However, the actions launched against Google for violation of E.U. privacy law[416] have been coordinated simultaneously by six national DPAs (France, Germany, Italy, the Netherlands, Spain, and the UK). This is the first time national DPAs have launched a coordinated action.

In January 2012, Viviane Reding, the Vice-President of the European Commission and European Union Justice Commissioner, formally released the Commission's Proposed Regulation[417]. The Proposed Regulation implements a comprehensive reform of European data protection laws intended to strengthen online privacy rights and boost Europe's digital economy. It seeks to take into account the realities of modern data flows, particularly in light of the increased use of social networking sites, cloud computing, location-based services and smart cards. The Proposed Regulation's release followed a period of uncertainty after it was understood that at least six E.U. policy units had issued negative opinions on the draft Regulation leaked in December 2011, and it is still subject to discussion. If and when it is adopted and implemented, the Proposed Regulation will

---

411 Commission Decision 2000/520/EC of 26.7.2000.

412 http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

413 http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

414 http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

415 *AccessData Corp. v. Alste Techn. Gmbh*, 2010 WL 318477 (D. Utah Jan. 21, 2010).

416 *Google privacy policy: six European data protection authorities to launch coordinated and simultaneous enforcement action*, CNIL, Apr. 2, 2013, http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo.

417 Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

impact organizations doing business in the E.U., including U.S. organizations that are active in the European Union market and offer their services to E.U. citizens.

The following are key areas of the reform that will affect privacy and data protection compliance for organizations:

- **A Single Set of Rules:** The Proposed Regulation provides for a single set of rules for all organizations processing personal data in the E.U.

- **Fines:** National DPAs will be allowed to impose fines of up to 2% of the worldwide gross revenue of an organization.

- **"One-Stop Shop":** The Proposed Regulation implements a "one-stop shop" approach to data protection compliance in the E.U., meaning that an organization only needs to comply with the data protection laws in place in the jurisdiction in which it has its main establishment.

- **Data Breach Notification:** The Proposed Regulation imposes a general requirement on all businesses to notify DPAs and data subjects in the event of a data breach. Notice of data breaches must be provided to the DPA "where feasible" within 24 hours, and to affected data subjects "without undue delay." While breach notification has recently become a requirement for telecommunications and Internet service providers, the Proposed Regulation extends this requirement to all organizations.

- **Consent:** Where consent is to be used as a justification for processing personal data, the Proposed Regulation requires that it be given explicitly, rather than assumed.

- **Data Portability:** The Proposed Regulation introduces a new individual right of data portability, which is designed to facilitate an individual's access to personal data and improve competition. It requires organizations to permit customers to move their data to new organizations offering similar products or services.

- **The "Right to be Forgotten":** The Proposed Regulation also adds a new "right to be forgotten" that allows an individual to require an organization to delete personal data where there is no longer any legitimate reason for keeping it. This new right is more stringent than the existing obligation of data controllers not to keep data for longer than is necessary.

- **International Transfer of Data:** The Proposed Regulation provides for a shift in the rules to reflect the way that data is currently transferred internationally. It seeks to address the problem that current data protection laws function only within a given territory, usually defined along national borders, and do not reflect the reality of international business, and that organizations making use of the cloud may collect data in one territory and subsequently process it in other territories. The Proposed Regulation will simplify the requirements for organizations seeking to do this and aims to improve the current system of "binding corporate rules" (typically a set of intra-corporate global privacy policies that satisfy the E.U. standard of adequacy when organizations are seeking to transfer the data

outside of the EEA), by requiring all DPAs to recognize "binding corporate rules" approved by an individual DPA.

- **Data protection by design and by default:** The Proposed Regulation requires data controllers to collect and retain personal data only to the minimum extent necessary in relation to the purposes for which they are intended by design to be processed.

- **Accountability and Data Protection Officers:** The Proposed Regulation seeks to increase the accountability of data controllers and data processors, including by requiring that they carry out data protection impact assessments prior to risky data processing activities. In addition, organizations with more than 250 full-time employees will be required to have a Data Protection Officer.

The Proposed Regulation is subject to approval by the European Parliament and the Council of the European Union (which comprises representatives of the Member States) following a process of tripartite negotiations between the European Commission, European Parliament and the Council of the European Union. Whilst the Commission is ready to commence these negotiations, along with the European Parliament (which voted to approve its own "compromise" version of the Proposed Regulation on 12 March 2014), the Council of the European Union is yet to approve a version as of April 2014. This has caused delays to the original timetable for implementation of the Proposed Regulation (which was originally intended to be adopted by the end of 2014) and may mean that adoption of the Proposed Regulation is delayed or even disrupted.

ii. Cookies and other tracking technologies

Tracking of users' internet usage remains an issue in the E.U. In November 2009, an amendment to the E.U. E-Privacy Directive[418] was adopted that required E.U. Member States to ensure that the storing of or access to information such as cookies, spyware or other tracking devices on the equipment of an Internet user is permitted only if the user has been provided with clear and comprehensive information about the purposes of the processing and has given his or her consent. Prior to this amendment, user consent was not required and users had only to be given the opportunity to refuse the storing of or access to devices (which was commonly achieved by the user adjusting browser settings to prevent such storage or access). There is an exception to the requirement to obtain consent where the storage is strictly necessary for a service expressly requested by the user. E.U. Member States were required to pass national legislation implementing the amendment to the E-Privacy Directive by 26 May, 2011. Whilst a number of E.U. Member States were slow to implement the relevant amendments to the E-Privacy Directive (to the extent that the European Commission felt compelled to commence legal action against E.U. Member States for their failure to implement[419]), as of January 2013, the amendments have now been

---

418 *Id.*

419 *Digital Agenda: Commission starts legal action against 20 Member States on late implementation of telecoms rules*, Jul. 19, 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/905.

implemented in all EU Member States according to the Article 29 Working Party's guidance on obtaining consent for cookies dated 2 October, 2013[420].

The Article 29 Working Party has taken the position that the requirements for consent are for "prior consent" and that all information must be provided and consent obtained before any information is sent or collected from a user's device.[421] This gives rise to complicated and prohibitive pop-ups or similar notifications for users, particularly where there are numerous third-party advertising networks involved. On the other hand, advertising networks, advertisers and content providers are seeking to rely on Recital 66 of the E.U. E-Privacy Directive, which seems to offer a more pragmatic approach to consent by inferring that prior consent is only required "where it is technically possible and effective." In addition, Recital 66 infers that consent may be obtained through the use of "appropriate settings of a browser or other application." The Interactive Advertising Bureau (IAB) Europe and the European Advertising Standards Alliance (EASA) have sought to build on this pragmatic approach with industry-led solutions providing for a means of opting-out from tracking.[422] However, the Article 29 Working Party has been repeatedly very critical of these solutions and this has raised issues as to whether they comply with law.[423]

The UK Information Commissioner's Office issued guidance[424] allowing for a 12-month grace period, which ended in May 2012, for companies to develop ways of complying with the UK's national legislation implementing the amendment to the E-Privacy Directive. On the eve of the expiry of this grace period, the UK's Information Commissioner's Office updated its Guidance on the rules on use of cookies and similar technologies to specifically state that implied consent can in some contexts be considered a valid form of consent.[425]

iii. Mobile Privacy

On March 14, 2013, the E.U. data protection authorities of the Article 29 Working Party announced[426] that they had adopted an opinion[427] addressing the key data protection risks of mobile apps. According to the Working Party, the risks range from a lack of transparency and lack of awareness among app users to poor security measures, invalid consent mechanisms, a trend towards data maximization and elasticity of data processing purposes. The Working Party noted in its

---

[420] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[421] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf.

[422] *EDAA to be launched*, European Advertising Standards Alliance, Dec. 8, 2011, http://www.easa-alliance.org/News/News/page.aspx/46?xf_itemId=146&xf_catId=1.

[423] *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, Article 29 Data Protection Working Party, Dec. 8, 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.

[424] *Enforcing the revised Privacy and Electronic Communications Regulations (PECR)*, May 25, 2011.

[425] *Guidance on the rules on use of cookies and similar technologies*, Information Commissioner's Office, May 2012, available at http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.

[426] *Press Release*, Article 29 Data Protection Working Party, Mar. 14, 2013, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130314_pr_apps_mobile_en.pdf.

[427] *Opinion 02/2013 on apps on smart devices*, Article 29 Data Protection Working Party, Feb. 27, 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

Opinion that many of these risks have already been examined by other international regulators, such as the FTC and the California Attorney General.

The Working Party particularly focused on the obligations of app developers, like Google and Facebook, but also considered all other parties involved in the development and distribution of mobile apps in the E.U. Such parties include manufacturers of operating systems and devices, app stores, and other parties involved in the processing of personal data, such as advertisers and analytics providers. The Working Party claims that, on average 1,600 new apps are added to app stores daily and 37 apps are downloaded per smartphone user. These apps collect large quantities of data, including photographs, or use location data. The Chairman of the Working Party, Jacob Khonstamm, said that "[t]his often happens without the free and informed consent of users, resulting in a breach of European data protection laws."

The Working Party highlighted that apps may have significant risks to the private lives and reputations of users of smartphones, and added that individuals must be in control of their personal data. In some instances where the purpose of the data processing is excessive and/or disproportionate, even if the user has consented, the app developer will not have a valid ground for processing data and would likely be in violation of E.U. data protection laws. The Working Party said that app developers should request user consent before the app collects, processes, or stores information on the mobile device.

Particular focus was given to processing data relating to children. The Working Party shares the concerns expressed by the FTC in its staff report on mobile apps for kids. The Working Party also made conclusions and recommendations to the various parties involved in the mobile app ecosystem to consider and implement. The Working Party called on the industry to "use [its] creative talent to deliver more innovative solutions to effectively inform users on mobile privacy."[428]

d. Selected Countries' Data Protection Laws

E.U. Member States have passed their own national data protection laws in order to implement the Data Protection Directive. Many non-E.U. countries have also instituted data protection laws in recent years, addressing what is a worldwide problem and presenting additional compliance issues for companies with multinational operations.

i. United Kingdom

In the UK, the Data Protection Directive was implemented by the Data Protection Act 1998 ("UK Act"). The Information Commissioner's Office ("ICO") is responsible for ensuring compliance with, and bringing enforcement action for breaches of, the UK Act.[429] Since April 2010, the ICO has had the power to impose fines of up to £500,000 where there has been a serious contravention of the principles set out in the UK Act and certain other requirements are met.

---

428 *Id.*

429 More information about the UK Act and the ICO is available at www.ico.gov.uk.

In June 2012, the ICO imposed its highest fine yet, of £325,000 against Brighton and Sussex University Hospitals NHS Trust for stolen hard drives that were sold on eBay in 2011. The ICO also issued a penalty of £60,000 to St George's Healthcare NHS Trust in London in July 2012 after a vulnerable individual's sensitive medical details were sent to the wrong address.[430] There has been much criticism that these fines are not high enough.

In January 2013, the ICO levied a £250,000 fine against Sony, following the hack of the Sony network in 2011. The ICO found that the attack on the network, and the subsequent compromise of the personal data of millions of Sony customers, could have been easily prevented with up-to-date software.[431] Further, in March 2013, the ICO fined DM Design, a Glasgow company, £90,000 for repeatedly targeting members of the public with nuisance marketing phone calls, and refusing to remove customer details even when explicitly requested to do so.[432]

In March 2014 the British Pregnancy Advice Service was fined £200,000 where a hacker threatened to publish thousands of names of people who sought advice on abortion, pregnancy and contraception. Also in March 2014, Kent Police were fined £100,000 after highly sensitive and confidential information, including copies of police interview tapes, were left in a basement at the former site of a police station. Further, in April 2014, The ICO served home improvement company Amber Windows with a £50,000 fine after an investigation discovered they had made unsolicited marketing calls to people who had registered with the Telephone Preference Service (TPS).[433]

Although historically the ICO has tended to impose money penalties on the public sector, recent fines indicate that the ICO is starting to find a balance between enforcement actions in the private and public sectors. This traditional emphasis on enforcement actions against the public sector is due, in no small part, to the more stringent notifications requirements that were placed on public authorities for privacy breaches. A greater number of public sector enforcement actions is an inevitable result of a greater number of reported public sector breaches.

Fines are likely to increase once the E.U. data protection regime is overhauled by implementation of the Proposed Regulation, discussed above, which will take effect two years after it is adopted by the European Parliament. National DPAs will be allowed to impose fines of up to 2% of the worldwide gross revenue of an organization.

In the UK, regulated financial services firms, such as banks, insurance companies and brokers, must also comply with the rules prescribed by the Financial Services Authority ("FSA"). The FSA's enforcement powers include private censure, removal of authorization, withdrawal of approved person status and potentially large fines. The FSA has taken a very strict approach when dealing with weaknesses in information security, in circumstances where there has been a breach of

---

[430] *ICO takes action after medical examination results are sent to the wrong address*, Information Commissioner's Office, Jul. 12, 2012, http://www.ico.gov.uk/news/latest_news/2012/ico-takes-action-after-medical-examination-results-are-sent-to-the-wrong-address-12072012.aspx.

[431] *Sony fined £250,000 after millions of UK gamers' details compromised*, Information Commissioner's Office, Jan. 24, 2013, http://ico.org.uk/news/latest_news/2013/ico-news-release-2013.

[432] *Glasgow company fined £90,000 as ICO tackles nuisance calls*, Information Commissioner's Office, Mar. 20, 2013, http://ico.org.uk/news/latest_news/2013/glasgow-company-fined-90000-as-ico-tackles-nuisance-calls-20032013.

[433] To keep up to date with The ICO's monetary penalty notices visit http://ico.org.uk/enforcement/fines

Principle 3 of the FSA Handbook requiring an organization to take reasonable care to organize and control its affairs responsibly and effectively.

ii. Germany

In Germany, the Data Protection Directive was implemented by the Federal Data Protection Act 2001[434] ("German Act"). Germany has a number of regional DPAs rather than a single national DPA. Under the German Act, a data controller must notify the relevant German DPAs and affected data subjects if it determines that certain serious or sensitive categories of personal data have been recorded, unlawfully transferred or otherwise unlawfully disclosed to third parties, threatening serious harm to the data subjects' rights or legitimate interests. If notifying all affected data subjects individually would require a disproportionate effort, notification can be replaced by public advertisements in daily newspapers or other effective means.

German DPAs have the power to impose fines of up to €50,000 for simple violations and €300,000 for serious violations of the German Act and to order organizations to remedy compliance failures.

In April 2007, a working group of German DPAs adopted a report entitled "Whistleblowing – Hotlines: Internal Warning Systems and Employee Data Protection"[435] that introduces guidelines to allow companies to introduce whistleblower hotlines which are compliant with German data protection law. A company's works council needs to be consulted prior to implementation of a whistleblower hotline and the works council has a right of co-determination, such that the terms of the hotline program are to be negotiated with them.

In Germany, a data breach notification regime is wider in scope than the breach notification regime pursuant to the E.U. Privacy Directive and applies to all companies subject to the German Federal Data Protection Act as well as to companies subject to the German Telecommunications Act and the German Telemedia Act. This regime came into force in September 2009.

iii. France

In France, the Data Protection Directive was implemented through an amendment to the existing law 78-17 of January 6, 1978 relating to the Protection of Data Subjects as Regards the Processing of Personal Data.[436] The financial sanctions which the French DPA, the Commission nationale de l'informatique et des libertés ("CNIL"), can impose include fines of €150,000 for the first breach and up to €300,000 in the case of a repeat breach within five years. Criminal sanctions may also be imposed of up to a maximum of five years' imprisonment and fines from €15,000 (and up to €75,000 for legal entities) to €300,000 (and up to €1,500,000 for legal entities).

---

[434] Federal Data Protection Act (Bundesdatenschutzgesetz), published in the Bundesgesetzblatt I Nr. 23/2001, p. 904 , May 22, 2001.

[435] Available at http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationsmaterial/wirtschaft/whistleblowing.html.

[436] Available at www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf.

In November 2005, CNIL published guidelines[437] to assist companies in the introduction of whistleblower programs that are compliant with both the Sarbanes-Oxley Act and French law. Since then, the French DPA has had a two-tier system of authorization in place, under which whistleblower programs may be authorized by either: (a) self-certifying to the French DPA through an automated online process that a whistleblower program complies with certain specified parameters (the "AU-004 authorization"); or (b) seeking CNIL's formal approval.

In late 2010, revised guidance[438] issued by CNIL for the AU-004 authorization became mandatory, narrowing the permitted scope of whistleblower programs that qualify for AU-004 authorization. Companies wishing to qualify for the AU-004 authorization must now restrict their whistleblower program scope to concerns about accounting, financial, banking, anti-competitive or corruption matters. Matters in the "vital interests" of the company or its employees' physical or mental integrity, which were permitted under the earlier guidance, are now outside the scope of whistleblower programs that qualify for AU-004 authorization. These other serious "vital interest" matters arguably covered matters relating to discrimination, environmental violations, violations of workplace safety rules and disclosures of trade secrets.[439]

In April 2011, CNIL announced that it intends to increase inspections of companies transferring data into and out of France to ensure compliance with French data protection laws.[440] The inspections will include a focus on verifying that U.S. companies enrolled in the Safe Harbor program are, in fact, compliant with its rules.

In March 2011, CNIL issued a fine of €100,000 against Google with respect to its Street View data processing, which reportedly recorded information from Wi-Fi networks that Google cars drove past as part of the mapping process. The resulting revision of Google's privacy policy continued to attract the scrutiny of the CNIL as well as of other European DPAs as to whether their data protection laws have been breached.[441] CNIL and DPAs of at least five other E.U. Member States, as well as a number of U.S. states, are continuing their scrutiny of Google's privacy policies.[442] In May 2012, CNIL published guidance[443] on breach notification law affecting electronic communications service providers. The guidance was issued with reference to the E.U. Privacy Directive, which imposes specific breach notification requirements on electronic communication service providers. However, given the ongoing discussions relating to the Data Protection Directive covering personal data, it is likely that such an obligation will be extended to all sectors.

---

437 Available at http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf.

438 Available at http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/83/.

439 See Edwards Wildman Client Advisory, *Global Whistleblower Hotlines: New French Restrictions Require Immediate Program Amendments*, July 2011, http://www.edwardswildman.com/newsstand/detail.aspx?news=2354.

440 Available at http://www.cnil.fr/la-cnil/actu-cnil/article/article/programme-des-controles-2011-une-ambition-reaffirmee-des-competences-elargies/?tx_ttnews%5bbackPid%5d=2&cHash=91ae300acd.

441 Letter from the President of the CNIL to Larry Page, CEO, Google Inc., dated Feb. 27, 2012.

442 Charles Arthur, *Google facing legal threat from six European countries over privacy*; The Guardian, Apr. 2 2013; *see also* Ian Steadman, *Google fined by German regulator over Street View privacy breach*, Wired, Apr. 22 2013, http://www.wired.co.uk/news/archive/2013-04/22/google-germany-fine.

443 Available at http://www.cnil.fr/la-cnil/actualite/article/article/la-notification-des-violations-de-donnees-a-caractere-personnel.

In January 2014, CNIL's Sanctions Committee issued a monetary penalty of 150 000 € to Google Inc. upon considering that it did not comply with several provisions of the French Data Protection Act[444]. In its decision, the Sanctions Committee considers that the data processed by the company about the users of its services in France must be qualified as personal data. It also judged that French law applies to the processing of personal data relating to Internet users established in France, contrary to the company's claim. Overall, six EU Authorities individually initiated enforcement proceedings against Google Inc. and the latest French conclusions are similar to those laid down by the Dutch and Spanish Data Protection Authorities in November and December 2013 on the basis of their respective national laws.

The CNIL has now implemented an online breach reporting mechanism on its website, www.cnil.fr. While there is no strict legal requirement regarding the method of giving notice, the new online breach reporting mechanisms now means that notice should be given using the notice form that may be downloaded from the website. The notice form may then be submitted online or sent by post.

iv. Spain

In Spain, the Data Protection Directive was implemented through Organic Law 15/99 of December 13, 1999 on the Protection of Personal Data. The Spanish DPA has issued an opinion to the effect that it considers anonymous reports to be unsuitable and not permissible for a whistleblower hotline in Spain. Notification to the Spanish DPA is required, so it has the opportunity to carry out a review of whistleblower programs and confirm compliance with local law. There may be options for compliance in Spain, outside the hotline system, for making reports, but this area is still unsettled.

Under one of the data protection principles set out in the Data Protection Directive discussed above, controllers must process personal data fairly and lawfully (the "fair processing principle"). In most E.U. Member States, controllers may seek to comply with the fair processing principle on the basis that processing is for the purposes of legitimate interests pursued by the data controller (the "legitimate interests condition"). The legitimate interests condition gives controllers a broad basis on which to comply with the fair processing principle. Under Spanish law, the legitimate interests condition is not available to data controllers and so other, less flexible, conditions must be relied upon instead.

In early 2011, the Spanish Data Protection Agency fined a Spanish bank €150,000 following a court ruling that the bank improperly included the names of a couple in two of Spain's most widely used debtors databases (Asnef and Badexcug). The couple had been victims of a scam and had found themselves obliged to make payments on a bank loan. The loan was subsequently declared void by the courts. The couple informed the bank of their intention to withhold any further payments and also sent written notice to the bank stating that if the withholding of payments led to their inclusion in the debtors databases, that would be considered a breach of personal data protection rules. The bank, ignoring both that the judgment had voided the loan and the couple's notice, proceeded to

---

444 The CNIL's Sanctions Committee issues a 150 000 € monetary penalty to GOOGLE Inc., 08 January 2014, at: http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/

include them in the aforementioned registries. As a result the Spanish Data Protection Agency imposed the fine. The Spanish DPA also levied subsequent fines of €50,000 on three other banks and financial institutions for the same offence of improperly adding the data subject to their respective debtor files.

The Spanish DPA continued to be active in other areas throughout 2012, most notably levying a €100,000 fine on Telefónica Móviles for processing data without the data subject's consent, and for charging invoices (to which the data subject had not contracted) to the data subject's account.

In January 2014 The Spanish Data Protection Authority (AEPD) issued fines against two jewelry companies, Navas Joyeros S.L. and Luxury Experience S.L., a total of 5,000 Euros for not providing clear and comprehensive information about the tracking programs they used and therefore violated the Spanish 'cookie consent' requirement[445]. These are the first monetary penalties imposed under Spain's Law of Information Society Services and Electronic Communications (LSSI-CE) which implements the e-Privacy Directive (Directive 2002/58). The Directive obliges website owners to give clear and comprehensive information about the tracking programs they use, and to gain consent from users. The AEPD began investigations in July 2013, four months after releasing their guidelines on the use of cookies. The Spanish legislative is currently drafting a General Telecommunications Act, which will allow the AEPD to pursue enforcement against site owners who fail to collect prior consent from users and will widen its range of tools in applying the cookie regime.

v. Sweden

In Sweden, the Data Protection Directive was implemented through the Personal Data Act 1998[446] ("Swedish Act"). Under the Swedish Act, it is generally prohibited for companies to process data relating to criminal allegations or violations of law, including in a hotline. Companies wishing to operate a hotline in Sweden must therefore apply to the Swedish DPA for an exemption from such prohibition. The Swedish DPA has a policy of granting such exemptions subject to certain restrictions, including that only key personnel and employees in a management position may be reported and personal data relating to other groups of employees may not be processed through the hotline. This may require certain language in the notice to employees in Sweden that the hotline should be used only where the report relates to a member of management or a key employee of the company. In some cases, it may not always be possible to impose such a limitation or the boundaries may become inevitably blurred.

vi. Austria

Under Austria's Federal Act concerning the Protection of Personal Data, data controllers that process certain personal data must notify the Austrian Data Protection Authority, which keeps a register of all data applications that is accessible by the data subjects.[447] Additionally, if a data

---

445 Spain: AEPD issues first European cookie fine, Updated: 06/02/2014 , at: http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2203

446 Available at http://www.regeringen.se/content/1/c6/01/55/42/b451922d.pdf.

447 Federal Act concerning the Protection of Personal Data (2000), available at http://www.dsk.gv.at/site/6274/default.aspx.

collector learns that personal data from his data application are "systematically and seriously misused" and the data subject may suffer damages, the collector is required to immediately inform the data subject in an "appropriate manner." Such obligation does not exist if the information – taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned – would require an inappropriate effort.

vii. Canada

Canada has federal, provincial and territorial privacy statutes that apply to the collection, use, disclosure and management of personal information in the private, public and health sectors, each with some variation in provisions.[448]

The Privacy Act governs the personal information handling practices of federal departments and agencies.[449] In the private sector, the four main privacy statutes are: the federal Personal Information Protection and Electronic Documents Act ("PIPEDA');[450] Alberta's Personal Information Protection Act ("PIPA");[451] British Columbia's Personal Information Act;[452] and Quebec's An Act Respecting the Protection of Personal Information in the Private Sector.[453]

In May 2010, Alberta became the first Canadian province to pass a general data breach notification law,[454] amending its Personal Information Protection Act ("PIPA"), to require notice of a data breach to Alberta's Information and Privacy Commissioner ("Alberta Commissioner") under certain circumstances. The amendment also granted the Alberta Commissioner authority to require organizations to notify individuals who face a "real risk of significant harm" as a result of the breach. The Alberta Commissioner is also required to issue a Notification Decision, which is published on the Alberta Commissioner's website.

Ontario, New Brunswick, Newfoundland and Labrador have privacy legislation that applies to health information and that has been declared substantially similar to PIPEDA with respect to health information custodians.[455]

viii. China

China does not presently have a single comprehensive data protection law. Rights to privacy may be traced back to the Constitution of the People's Republic of China ("Constitution").[456] Article 40 of the Constitution provides that no organizations or individuals are permitted to infringe upon,

---

448 See http://www.priv.gc.ca/resource/pb-avp/pb-pa_e.asp

449 Privacy Act (R.S.C., 1985, c. P-21).

450 S.C. 2000, ch. 5 ("PIPEDA").

451 S.A. 2003, ch. P-6.5 ("PIPA Alberta").

452 S.B.C. 2003, ch. 63 ("PIPA BC").

453 R.S.Q. ch. P-39.1 ("Quebec Privacy Act").

454 Mexico and Alberta Pass New Data Protection Laws, InsureReinsure.com, June 10, 2010. http://www.insurereinsure.com/?entry=2507.

455 See http://www.priv.gc.ca/resource/pb-avp/pb-pa_e.asp.

456 Available at: http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm.

among other things, the confidentiality of a citizen's communications for any reason, except in the case of national security, investigation of a criminal offence or monitoring by the public security or prosecutorial authorities in accordance with legally-prescribed procedures.

In December 2011, the Ministry of Industry and Information Technology ("MIIT"), the Chinese internet and telecommunications industry regulator, issued the Several Provisions on Regulating the Internet Information Service Market Order ("IIS Provisions").[457] The IIS Provisions apply to entities in mainland China providing information services through the internet or engaging in related activities and have a special focus on protecting internet users' legitimate expectation of privacy from perceived abuses. The IIS Provisions define "users' personal information" to mean any information associated with a user from which, either independently or when combined with other information, such user can be identified. Under the IIS Provisions, information services providers are (i) prohibited from collecting personal information without prior consent of the user; (ii) required to expressly inform users of the method, content and purposes of collecting and using their personal information; (iii) prohibited from collecting personal information other than as is necessary in connection with the product or service provided; (iv) prohibited from disclosing or transferring users' personal information to a third party without the consent of the user, unless the laws and regulations provide otherwise; and (v) prohibited from deceiving, misleading or coercing a user into transferring any information the user has uploaded.

In February 2013, the People's Republic of China's General Administration for Quality Supervision, Inspection, and Quarantine and the Commission for the Administration of Standardization jointly issued the Guidelines on Personal Information Protection within Information System for Public and Commercial Services on Information Security Technology ("Guidelines").[458] The Guidelines are intended to regulate all organizations and entities with regard to protection of personal information; however, they do not have the force of law. The Guidelines contain rules and principles collecting, processing, transferring and deleting personal information on "computer information systems" (as opposed to other data storage media in hard copy form). The Guidelines divide personal information into "sensitive personal information" and "general personal information," similar to the distinction in the EU data privacy regime. The collection and use of sensitive personal information requires the relevant owner's express consent, and evidence of such consent must be kept. The collection and use of general personal information only requires implied consent (that is, where the owner raises no objection to its collection). In either case, express consent is required for transfer of any personal information outside of mainland China.

On 16 July, 2013, following the Decision on the Strengthening of the Protection of Network Information passed by the Standing Committee of the National People's Congress ("NPC"), the MIIT promulgated the Provisions on Protection of Personal Information of Telecommunications and Internet Users ("Personal Information Provisions").[459] The Personal Information Provisions address collection and use of personal information of individual users such as passwords, names, dates of birth, addresses, account numbers and so forth by providers of telecommunications and internet information services within mainland China. The Personal Information Provisions also

---

457 Available at: http://www.miit.gov.cn/n11293472/n11293832/n12843926/n13917012/14414975.html.

458 Available at: http://www.cinic.org.cn/site951/zcdt/2013-03-29/636814.shtml.

459 Available at: http://www.miit.gov.cn/n11293472/n11294912/n11296542/15514014.html

include standards, security measures and penalties concerning collection and use of information by service providers and third parties engaged to handle collection and use of such information (i.e. outsourcing).

In addition, amendments to the Consumer Protection Law ("Amended Consumer Protection Law")[460] came into force on 15 March, 2014. The Amended Consumer Protection Law covers all businesses that provide goods or services to consumers, and extends to all means of collection of personal data (such as membership enrollments at supermarkets, credit card applications made at shopping malls and patient details provided at clinics). For the first time, it establishes the right of consumers to have their personal information protected, and consumers may obtain compensation from business operators which infringe upon this right.

ix. Hong Kong

The principal privacy law in Hong Kong is the Personal Data (Privacy) Ordinance (Cap 486) ("Ordinance"),[461] enacted in 1995 and amended in 2013 to protect personal data, *i.e.* data relating directly or indirectly to a living individual (data subject), from which it is practical to ascertain (directly or indirectly) the identity of the individual; and in a form in which access to or processing of the data is practicable. The Ordinance applies to any person (data user, including private sector, public sector and government department) who controls the collection, retention, processing or use of personal data. The Ordinance sets out six data protection principles[462] governing the proper collection, accuracy, retention, use, security, access and correction of personal data, the contravention of which per se is not an offense.

The independent Office of the Privacy Commissioner for Personal Data ("PCPD")[463] was established in 1996 with the mandate to promote data protection practices and to oversee data users' compliance with the Ordinance. Since its establishment, PCPD has issued various guidance to data users on different areas to promote good data protection practices. In February 2014, PCPD issued "Privacy Management Programme: A Best Practice Guide" calling for businesses to adopt comprehensive privacy management programs for achieving compliance in all aspects of business.

In Hong Kong, personal data cannot be transferred to another data user (even if it is within a group of companies) without the data subject's prior consent. The Ordinance also prohibits transfers of personal data outside Hong Kong except in specified circumstances; however, that provision has not yet gone into effect.[464]

Hong Kong heavily regulates the use of personal data and provision of data for use in direct marketing. Data users are required to inform data subjects of the kinds of personal data they will be using for direct marketing purposes and the classes of goods or services that will be marketed. Data

---

460 Available at: http://www.saic.gov.cn/zcfg/fl/xxb/201310/t20131030_139167.html.

461 Available at: http://www.legislation.gov.hk/blis_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf

462 See Schedule 1 to the Personal Data (Privacy) Ordinance (Cap 486).

463 More information about the PCPD is available at http://www.pcpd.org.hk/.

464 Section 33 of the Personal Data (Privacy) Ordinance (Cap 486).

users may not use personal data in direct marketing or provide data to another person for use in direct marketing unless they have obtained the data subject's consent. Silence is not sufficient.

Hong Kong maintains "do not call" registries for commercial electronic messages communicated within Hong Kong to Hong Kong recipients by email, fax, SMS, MMS or by pre-recorded voice message. These registries are separately provided for under the Unsolicited Electronic Messages Ordinance (Cap.593).[465]

While data users are not statutorily required to inform the PCPD about a data breach incident, the Guidance on Data Breach Handling and the Giving of Breach Notifications issued by the PCPD advises data users to provide such notice as a recommended practice for proper handling of such incidents. In 2013, there were 61 known data breach incidents (compared with 50 incidents in 2012), affecting 90,000 individuals.[466] The PCPD was made aware of these incidents through voluntary notifications from the data users as well as reports from the media and the general public. These incidents ranged from unauthorised disclosure of personal data through hacking to inadvertent circulation of lists of personal data to unrelated third parties.

The PCPD may investigate suspected breaches of the Ordinance, either in response to a complaint or at its own initiative. If the PCPD concludes a contravention is likely to be repeated, it may issue an enforcement notice and impose a penalty. Individuals may also claim compensation through civil proceedings for damage caused to them as a result of a contravention of the Ordinance.

In 2013, the PCPD received a total of 1,792 complaints, which represented a record high. Thirty-eight percent of those complaints concerned the use of personal data without the consent of data subjects (673 cases), 36% were about the purpose and manner of data collection (643 cases), 9% were related to data security (169 cases) and 9% were about data access/correction requests (161 cases). The PCPD issued 32 warnings and 25 enforcement notices. It referred 20 cases to the Police for consideration of prosecution, an increase of 33% compared to 2012. As many as 14 cases related to suspected contraventions of the provisions governing direct marketing, including the making of repeated telemarketing calls despite the complainants' request to opt out from such marketing approach and failing to take specified steps before using individuals' personal data for direct marketing. Most of the referred cases are still under Police investigation, and no conviction was recorded in 2013.[467] India

In April 2011, India adopted new privacy regulations, known as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Indian Rules").[468] The Indian Rules impose a number of obligations on data controllers, including requirements to have a privacy policy, to obtain the consent of data subjects before collecting or processing sensitive personal data, and to comply with reasonable security practices and procedures, as well as restrictions on disclosing personal data to third parties.

---

[465] Available at: http://www.legislation.gov.hk/blis_pdf.nsf/CurAllEngDoc/BE5AA57E2A0358C7482575EF00201941/$FILE/CAP_593_e_b5.pdf

[466] See http://www.pcpd.org.hk/english/infocentre/press_20140123a.htm.

[467] See http://www.pcpd.org.hk/english/infocentre/press_20140123a.htm.

[468] Available at www.mit.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

Guidance issued by the Ministry of Communications and Information Technology clarifies that the Indian Rules only apply to Indian entities and that several provisions, including those relating to the collection and disclosure of personal information, do not apply to Indian outsourcing services providers, other than in relation to the data of their own India-based personnel or customers, or to individuals who contract directly with them.[469]

In April 2012, Indian authorities requested that the European Commission designate India as a "white listed" country for transferring personal data outside of the EEA. This would allow the transfer of personal data from the EEA to India on the basis that India would be deemed to "have an adequate level of protection for personal data." The issue was raised during the negotiation of a bilateral trade agreement.[470] For many organizations outsourcing services to India, that the European Commission has not designated India as a secure country means that complex procedures, consents or, in some cases, prior authorizations are required before personal data can be transferred to India, which is a significant barrier to the continuing success of outsourcing services to India-based companies.

x. Mexico

In April 2010, the Mexican Senate passed a data protection law that addresses how private and public entities handle the collection, use and disclosure of personal information of Mexican residents.[471] The new law expands the authority of the Mexico's DPA, now called the Federal Institute of Access to Information and Data Protection ("IFAI"). In December 2011, a second-draft of regulations implementing the new data protection law, came into force, establishing principles relating to the clarification of notice and consent requirements, changes to restrictions on cloud computing, updates to requirements regarding data transfers, and clarifications regarding data subjects' rights.[472]

V. The Exposures Presented by Data Breaches

1. The Breadth of the Problem

The costly and growing exposure presented by data breaches is demonstrated by the following recently reported statistics. As breaches of Personal Information are the most reported and studied, these statistics focus on the costs associated with data incidents involving Personal Information.

---

469 *See Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000*, Ministry of Communications & Information Technology Press Note, Aug. 24, 2011, http://pib.nic.in/newsite/erelease.aspx?relid=74990.

470 Amiti Sen & Harsimran Julka, *India seeks 'Data Secure Nation' status, more Hi-end business from European Union*, The Economic Times, Apr. 16, 2012, http://articles.economictimes.indiatimes.com/2012-04-16/news/31349813_1_data-security-council-data-protection-laws-standard-contractual-clauses.

471 Mexico and Alberta Pass New Data Protection Laws, InsureReinsure.com, Jun. 10, 2010, http://www.insurereinsure.com/?entry=2507.

472 Available at: http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011.

Less quantified are the increasing breaches involving theft of other type of company information, such as trade secrets and other confidential business information, and denial of service attacks.[473]

a. The Big Picture: Number of Breaches and Associated Costs

- The average cost of cyber crime generally for 234 large organizations in six countries (U.S., U.K, Australia, Berman, France and Japan) was $7.2 million per year, with a range of $375,387 to $58 million; business disruption and lost productivity represented the highest external cost at 38% of external costs(defined as a cost created by external factors such as fines, litigation and marketability of stolen information), with costs associated with information accounting for 35% of external costs.[474]

- In 2013, in the U.S. there were 619 reported breaches, a significant increase of 30% over the total number of tracked braches in 2012. There were over 57 million records reported as exposed.[475]

- Globally, 63,000+ security incidents with 1,367 confirmed data breaches were reported by a group of 50 organizations tracking such incidents worldwide.[476]

- In one study, 59% of the over 120 of the world's largest Technology, Media and Telecommunications ("TMT") organizations surveyed reported information security breaches; 73% reported denial of service attacks.[477]

- A 2014 study of 314 companies globally found that the average total cost of a data breach for the companies in 2013 was $3.5 million; these costs included breach notification costs, other post breach costs such as investigations, remediation, product discounts and other costs, and also include lost business costs). German and U.S. companies had the mostly data breaches, with $201 and $195 per record, respectively, and the highest total costs (U.S. at $5.85 million and Germany at $4.74 million); the least costly breaches reported occurred in Brazil and India.[478]

- Analysis of claims payout data submitted by cyber insurers of 140 incidents occurring between 2010 and 2012 (with some still claims still not over at the time of the report) resulted in somewhat different results than studies of costs without regard

---

[473] *See*, *e.g.*, Prolexic, Quarterly Global DDos Report for information on DDoS attacks, whose Q4 2013 report noted an increase in size and frequency of DDoS attacks in 2013 compared to 2012. Reports are available at www.prolexic.com.

[474] Ponemon Institute LLC, *2013 Cost of Cyber Crime Study: Global Report*, October 2013.*t*

[475] *See* Identity Theft Resource Center,http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html. This number reflects data breaches that the ITRC considers published by a reliable source. Additional breaches may have occurred, and not all reported breaches identify the number of records exposed.

[476] Verizon, *2014 Data Breach Investigations Report,* Apr. 2014.

[477] *Deloitte 2013 TMT Global Security Survey: Blurring the Lines: Information Security in a World Without Boundaries*, Jan. 8, 2013.

[478] Ponemon Institute LLC, *2014 Cost of Data Breach Study: Global Analysis*, May 2014 (the majority of data breach incidents studied for the report happened in the 2013 calendar year) .

to what was paid by insurers. The mean claim payout was reported to be almost $1 million ($954,253), and the median at $242,500; however, many of the claims had not yet been fully resolved and paid, and thus the overall costs including amounts within self-insured retentions was estimated to end up averaging $3.5 million with a median of $250,000. The average cost per record was $6,790 (reduced to $307 if outlier incidents with only a few records by extremely high payouts were removed), and the mediate cost was $107.14; the average number of records exposed was 2.3 million, with the median of 1000; the average cost for legal defense was $574,894, for legal settlement was $258,009, and for crisis services (including forensics, notification, call center and related legal counsel) was $737,473 with the median $209,473.[479]

- The total economic burden created by data breaches in the healthcare industry has been estimated as $5.6 billion annually, with the average cost in a March 2014 study noted to be $2 million over a two year period, which is a decrease of $400,000 from the prior year's study indicating healthcare organizations have improved ability to control data breach costs.[480]

- In a recent study among 3,200 business executives and IT leaders from 16 countries, including the UK, 29% reported experiencing data loss and 23% said they faced a security breach, with losses averaging approximately $860,000 per year as a result of data breaches.[481]

- Having a strong security posture, incident response plan and CISO (Chief Information Security Officer) appointment has been found to reduce the cost per record of a data breach by $14.14, $12.77 and $6.59 respectively, while (too) quick notification increased costs by $10.45 per record. Breaches involving lost or stolen devices had increased costs of $16.10 while third party involvement in a breach was found to increase costs by $14.80 per record.[482]

- According to a 2013 study, the correlation between receiving a data breach notification and being a victim of fraud is one in four, compared to only one in nine in 2010.[483]

- One study noted that on average, each respondent encountered 2 successful cyber-attacks on their systems per week, with an average of 122 successful attacks per week across 60 respondents. This represented an increase in 18% over the frequency

---

479 NetDiligence, *CyberLiability & Data Breach Insurance Claims: A Study of Actual Claim Payouts*, Oct. 2013.

480 Ponemon Institute LLC, Report, March 2014, *Fourth Annual Benchmark Study on Patient Privacy & Data Security*.

481 AlertsecExpress, *23% of Organizations faced a Security Breach in 2013*, Nov, 2013 (citing data from EMC survey). http://blog.alertsec.com/2013/11/23-organizations-faced-a-security-breach-in-2013/.

482 Ponemon, *2014 Cost of Data Breach Study: Global Analysis, supra.*

483 EMC White Paper, 2013. *Cybercrime and the Healthcare Industry. http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf.*

of attacks in 2012. The most costly of such attacks were caused by denial of services, malicious insiders and web-based attacks.[484]

- Stolen healthcare information has a substantially higher value on the black market than "ordinary" information; one study notes that the average payout for a medical identity theft is $20,000, compared to $2,000 for regular identity theft.[485]

- "Fullz" or "full identity profiles" are more desirable for hackers than individual items such as credit cards. For example, one study notes that the average selling price for a stolen U.S. credit card is around $1, however when such card is sold in a "fullz" or "full identity profile," the cost increases to around $500, with health insurance information adding an additional $20 per each credential.[486]

- A 2013 EU study noted that 76% of respondents believe the risk of being a victim of cybercrime has increased in the past year.[487]

- "Mega Breaches" (single incidents exposing personal details of at least 10 million identities) increased from 1 to 8 from 2012 to 2013.[488]

- One study found that 77% of all websites in 2013 contained "vulnerabilities" that could potentially be exploited by attackers, compared to only 53% in 2012.[489]

- A 2014 found that U.S. companies participating in a survey faced an average lost business cost (defined as abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill) of over $3.3 million.[490]

b. The Industries, Assets, and Types of Data Most Frequently Compromised

Large scale data security incidents continue to be front page news, with hundreds of lesser but still costly breaches each year affecting companies in a broad range of industries.[491] Indeed, any entity that has Personal Information in its possession, whether that of employees, customers, clients or third parties, is a potential target for data breaches, either malicious or accidental. Companies with

---

484 Ponemon 2013 Cost of Cyber Crime Report, *supra.*

485 EMC White Paper, *supra*.

486 EMC White Paper, *supra*.

487 Commercial Risk Europe, Nov. 2013, *Fears over cybercrime rising among EU consumers*. http://www.commercialriskeurope.com/cre/2832/56/Fears-over-cybercrime-rising-among-EU-consumers/?elq_mid=25180&elq_cid=2339560.

488 Symantec, *Internet Security Threat Report 2014*, Apr. 2014.

489 Symantec, *Internet Security Threat Report 2014*, *supra.*

490 Ponemon, 2014 Cost of Data Breach Study, *supra.*

491 This does not include the vast number of incidents where Personal Information is stolen directly from individuals, or in which the breach involves heft of information that does not qualify as Personal Information subject to mandatory breach reporting.

intellectual property or other confidential business information can also be a target of espionage, and trade secrets and confidential business information is frequently a target of malicious cyber attacks. Moreover, virtually every company is also susceptible to the more garden-variety data security incident that results from lost laptops and smart phones, improperly disposed of paper records, and lack of protection measures with vendors to whom businesses provide access to Personal Information or company networks.

As demonstrated by the recent reports of large scale data breaches involving retailers, breaches involving theft of Personal Information remain a major exposure, as cyber criminals target points of data concentration to acquire large amounts of consumer information, such as personal identification numbers (PINs) with associated debit and credit card numbers, usually for resale. Social Security numbers are also a prime target, due to their usefulness in identity theft and the fact that, unlike credit cards, they are not easily cancelled and removed from usage.

While the industry that has the top spot for publicly reported breaches can vary somewhat from year to year, certain industries are always on the top ten list such as retail, healthcare, hospitality, financial services and educations institutions, and others may be under the radar but also exposed, such as professional service firms. Below are some of the industries with those exposures, as well as some recent statistics on types of data and number or records exposed in recent breaches.

Targeted industries include

- **Retailers**:

  Because of their heavy use of credit and debit card transactions, and the financial value of credit and debit cards for use for fraudulent charges, retailers have long been targets of cyber criminals. Hackers have attacked online networks as well as in store pin pads and registers. The continued exposure of both bricks and mortar and online retailers to massive data breaches affecting millions of consumers has been vividly demonstrated in recent months.

  In late 2013, Target endured a massive data breach that made headlines around the world, compromising over 40 million customers' payment card accounts and other information of an additional 70 million customers, including names, mailing addresses, phone numbers and email addresses. The U.S. Senate Committee on Commerce and Transportation identified issues that are of concern to many others, including providing a third party vendor with access to company networks; adequacy of response to automated warnings from the company's anti-intrusion software; issues of whether there was proper isolation of the most sensitive network assets. [492] The large losses resulting from the breach have generated not only dozens of lawsuits, but also proposed legislation on both the state and federal levels in the U.S. seeking to

[492] United States Senate Committee on Commerce, Science and Transportation, *A "Kill Chain "Analysis of the 2013 Target Data Breach*, March 26, 2014.

impose upon retailers greater liability (holding retailers responsible for reimbursement of costs sustained by customers as a result of the breach) and security obligations.[493]

In early 2014, eBay, the quintessential ecommerce site, reportedly sustained a security breach potentially impacting over 145 million people around the world, although the exact nature of the information accessed and the circumstances is still to be determined with potential investigations announced in the UK as well as the U.S. Reports are of accessed email addresses and passwords, and so far not financial accounts.[494]

Many attacks may be automated searches for vulnerable networks containing payment card information, rather than deliberate targeting of a particular store or retailer.

Retailers are subject not only to data breaches, but also to non-breach related consumer litigation directed at business practices in the collection and usage of Personal Information, thus rendering retailers a target of exposures on both breach and other privacy related fronts.

- **Hospitality/Food and Beverage**:

  The heavy use of credit and debit card transactions in the hospitality industry, which includes hotels, restaurants, and food retailers, makes businesses in this industry a target for cyber criminals as well as more garden-variety theft or inadvertent disclosure of Personal Information.[495] For restaurants and others in this industry, breaches can simply be the result of careless use or disposal of credit and debit card information, or it can be that they are the target of cyber criminals seeking to obtain credit and debit card numbers as they are transmitted by customers for payment.[496] Further, this industry like all others is susceptible to lost laptops and other breaches of security involving employee and client Personal Information.

---

493 See Allison Grande, *Retailer Take Brunt of Breach Liability Under New Bills*, Law360, May 30, 2014, http://www.lw360.com/articles/540367/print?selection=consumerprotection (discussing recent legislative proposals in California and Minnesota.

494 Harry Wallop, *eBay hacking: on line gangs are after you*, Telegraph, 23 May 2014, http://www.telegraph.co.uk/technology/internet-security/10849689/eBay-hacking-online-gangs-are-after-you.html; Lauren Hertzler, *Scams expected to hit customers hard after eBay data breach*, Philadelphia Business Journal, May 25, 2014, http://www.bizjournals.com/philadelphia/news2014/05/25/scams-expected-to-

495 Joe Sharkey, *Credit Card Hackers Visit Hotels All Too Often*, The New York Times, Jul. 5, 2010 (citing study released by SpiderLabs); *see also Hospitality Industry Data Theft: Hotel Owners Must Prevent Breaches of Credit Card Processing Systems*, Aug. 7, 2010, *http://hospitalityrisksolutions.com/2010/08/07/hospitality-industry-data-theft-hotel-owners-must-prevent-breaches-of-credit-card-processing-systems-by-cyber-criminals-who-install-malicious-programs-to-steal-data/*.

496 *See* Will Oremus, *A Burger, An Order of Fries, and Your Credit Card Number*, Slate, Mar. 22, 2012 (discussing that restaurants are prime targets for hackers as small businesses such as most restaurants often don't set up unique passwords after they install point-of-sale charge systems).

- **Healthcare Providers and Healthcare Insurers:**

  The healthcare industry has one of the highest rates of reported breaches, with the new rules governing healthcare breach reporting that went into effect in 2013 increasing the likelihood that unauthorized access to information about a patient will be reported. (See discussion of breach notification obligations under HIPAA and the HITECH Act above, Section III. 2.e and f).

  The U.S. Department of Health and Human Services reports that as of February 2014, the number of breaches of patient Personal Information affecting 500 or more people since it began keeping records in 2009 reached 834, with more than 21.7 million patients affected.[497]

  The good news is that a recent study reports that healthcare institutions have improved in controlling data breach response costs, with a decrease of 17% noted between 2013 and 2012.[498] Unfortunately, that same report noted a 100% increase in criminal attacks on healthcare systems in the last four years.

  Data breaches involving healthcare institutions and health insurers can range from simple loss of a laptop, to systemic electronic data breach of patient Private Information, to a reported incident of a worm infecting medical equipment run with the assistance of computer systems. A concern with compromise of medical center systems that is not an issue with most other industries is that it has the potential to negatively affect patient care, either directly affecting operation of equipment or by interrupting the systems that provide information used in the rendering of care, with resultant bodily injury. Healthcare service providers and their vendors include not only major medical centers but also small groups that, as with other small businesses, cannot easily bear the costs of a major data breach

  Data breaches involving healthcare institutions and health insurers can range from simple loss of a laptop, to systemic electronic data breach of patient Private Information, to a reported incident of a worm infecting medical equipment run with the assistance of computer systems. A concern with compromise of medical center systems that is not an issue with most other industries is that it has the potential to negatively affect patient care, either directly affecting operation of equipment or by interrupting the systems that provide information used in the rendering of care, with resultant bodily injury. Healthcare service providers and their vendors include not only major medical centers but also small groups that, as with other small businesses, cannot easily bear the costs of a major data breach. The financial

---

[497] *HIPAA & Breach Enforcement Statistics for February 2014,* produced by Health Information Privacy/Security Alert, published by Melamedia, LLC. *See also Health Information Privacy,* U.S. Department of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[498] Ponemon Institute LLC, *Fourth Annual Benchmark Study on Patient Privacy and Data Security:* March 2014.

burden that a breach can place on a small vendor was demonstrated by the reported bankruptcy of a medical records vendor faced with a break-in to its offices that resulted in a breach of electronic medical records that included Personal Information and medical diagnoses of 14,000 people. As a result of the costs of responding to the breach, the vendor filed for bankruptcy.[499]

Healthcare insurance identification is apparently worth many times more than payment card information on the black market and this makes healthcare institutions a target. According to one research firm, criminals tend to use information stolen from medical records for an average of 320 days versus 81 days for data stolen from other sources, and it takes twice as long to detect a medical data breach compared with other kinds of thefts of Personal Information.[500]

Increasingly, healthcare providers faced with a data breach are also being subjected to large regulatory fines, particularly when the post-breach regulatory scrutiny reveals lax security procedures were in effect or there was delayed or problematic breach response.

- **Financial Institutions:**

Financial institution no longer hold one of the top spots of industry targets, perhaps because they generally have among the most sophisticated security and response. However, they remain a target of cyber criminals due to the volume and nature of the information they collect and maintain, as well as less malicious exposures (as an American bank robber is apocryphally know to have said, he robs banks "because that is where the money is"). Thus, while they no longer hold top spot for web based and other types of attacks, they are still a top target for payment card skimmers: in 2013, 87% of skimming occurred on ATMs.[501]

Banks have been the target not only of hackers seeking to obtain Personal Information of customers for financial gain, but also those seeking to disrupt the bank's operations for political reasons.[502] This has not been limited to U.S. banks, as demonstrated by the well-publicized attacks on banks in South

---

499 Katy Stech, *Burglary Triggers Medical Records Firm's Collapse*, The Wall Street Journal, Mar. 12, 2012.

500 Neil Versel, *Report: Medical data theft growing as more adopt EMRs*, Fierce EMR, Apr. 1, 2010, http://www.fierceemr.com/story/report-medical-data-theft-growing-more-adopt-emrs/2010-04-01.

501 Verizon, *2014 Data Breach Investigations Report, supra.*

502 Ellen Nakashima, *U.S. response to bank cyberattacks reflects diplomatic caution, vexes bank industry*, Washington Post, Apr. 27, 2013.

Korea, with the culprits suspected to be from North Korea reportedly using malware intended to render computer unusable.[503]

Hacking of financial institutions raises not only concerns not only of large – scale theft of Personal Information, but also of politically motivated hackers deliberately trying to wreak havoc on global financial markets.

- **Payment Processors:**

Payment processors of credit card transactions are a major target of malicious attacks, as a successful attack on their systems can yield large amounts of Personal Information, particularly credit card information of consumers as well as of merchants, potentially for use in fraudulent financial transactions. Among the best known of these data breaches are those of Global Payments (March 2012); Heartland Payment Systems (January 2009); and RBS World Pay (December 2008).

In early 2013, a ring of hackers conducted a large and complex international theft, by utilizing malware to breach two card processors used by banks in the United Arab Emirates and Oman, one in the U.S. and one in India. The criminals reportedly overrode security protocols, found prepaid debit cards and deleted the limits on those accounts, and loaded the account information on magnetic strips, which were then used by a "cashing crew" to withdraw over $45 million in cash from ATMs.[504] Several cashing crew members were identified and indicted shortly after the withdrawals.[505]

The reported costs resulting from the Heartland breach demonstrate the potential size of exposures presented by data breaches of payment processors, who by the nature of their business have Personal Information of thousands (or millions) on their systems. In May 2009, Heartland disclosed it had spent or set aside more than $12.6 million to cover legal costs and fines related to the data breach. Apart from its settlements with the class of the class of affected consumers, and settlements with other third parties, settlements reached by Heartland with the card brands represent an additional significant cost. It reportedly reached a settlement with American Express for $3.6 million;[506] settled with Visa for up to $60 million;[507] and with MasterCard for

---

503 Chris Strohm & Eric Engleman, *Cyber Attacks on U.S. Banks Expose Computer Vulnerability*, Bloomberg, http://www.bloomberg.com/news/2012-09-28/cyber-attacks-on-u-s-banks-expose-computer-vulnerability.html, Sept. 28, 2012; Choe Sang-Hun, *Computer Networks in South Korea Are Paralyzed in Cyberattacks*, The New York Times, Mar. 21, 2013.

504 *See, e.g.*, Penny Crosman, *Data Breaches Back in Spotlight After $45 M ATM Heist*, American Banker, May 14, 2013.

505 United States of America against Alberto Yusi Lajud-Pena, et al. Indictment CR13-0259, United States District Court, Eastern District of New York, Apr. 25, 2013.

506 Robert McMillan, *Heartland Pays Amex $3.6 Million Over 2008 Data Breach*, PC World, Dec. 17, 2009, http://www.pcworld.com/article/185052/article.html.

507 Grant Gross, *Heartland to Pay up to $60 Million to Visa Over Breach*, Computer World, Jan. 8, 2010, http://www.computerworld.com/s/article/9143480/Heartland_to_pay_up_to_60M_to_Visa_over_breach.

$41.4 million.[508] As discussed below, it is still in litigation with several issuing banks for reimbursement of losses they allegedly sustained. A number of financial institutions were reportedly affected by the Heartland data breach, including banks in 40 states. Many banks apparently had credit or debit cards they had issued compromised by the incident. Heartland shareholder litigation was also commenced, although unsuccessful. The Heartland breach demonstrates the wide range of third-party claims that may be asserted when there is a large breach resulting in unauthorized access of credit card numbers, as well as the significant costs to which a company that has a large breach is subject.

- **Universities and Other Educational Institutions**

  Universities have been one of the major sources and targets of data breaches, as have lower level educational institutions. This may be because of the large number of computer terminals accessible by a myriad of students and employees and a more casual attitude toward computer security at some educational institutions, or because many universities have research facilities and programs whose information is a target for those with financial or political motives. In any event, almost every year educational institutions have a place relatively high on the list of industries with reported breaches.[509]

- **Law Firms**

  Law firms are a repository of clients' confidential and Personal Information, and the Personal Information of claimants in litigations they handle, as well as of their own employees' Personal Information. Thus, they are a significant potential source of inadvertent data breaches as well as a potential target of malicious ones.[510]

  Many breaches are simply due to improper information disposal practices or lost laptops and other mobile devices. Client records containing personal and confidential information have been found in paper form in dumpsters, and in electronic form in improperly discarded electronic devices. There is increasing concern, however, of law firms being targeted by hackers to obtain information about firm clients, particularly clients whose security procedures have made intrusion more difficult. The FBI has warned law firms that they are being targeted by hackers.[511] Other security experts have also warned that law firms may be increasing targeted by those seeking to obtain

---

[508] Nancy Gohring, *Heartland, MasterCard Settle Over Data Breach*, Computer World , May 9, 2010, http://www.computerworld.com/s/article/9176999/Heartland_MasterCard_settle_over_data_breach.

[509] See www.idtheftcenter.org, which lists reported breaches by industry each year.

[510] See Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, The New York Times, March 326, 2014, http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/?_php=

[511] Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, The Wall Street Journal, Jun. 26, 2012; ABA Law Practice Management Newsletter, *Preventing Law Firm Breaches*, Vol. 38, No. l.

confidential information of their clients, either for political motivation or economic advantage (*e.g.,* bidding information or trade secrets).[512]

In addition, law firms frequently allow their employees to use their own devices to access firm data bases, giving rise to the security risks attendant with BYODs (Bring Your Own Device). Many firms also do a significant amount of business with companies in the healthcare industry may qualify as "business associates" of entities covered by HIPAA, and thus be subject to its breach notification requirements. Furthermore, law firms that perform large-scale document review and productions often use outside vendors and Internet-based data storage systems. As this practice continues to grow, law firms increase their exposure to potential cyber attack as well as inadvertent data breaches involving their vendors as well as themselves.

- **Real Estate Agents**

Real estate and rental agents and others involved in the sale or rental of properties, particularly residential properties, often collect and maintain applications that contain financial as well as other Personal Information of applicants. Those, those involved in such real estate transactions are a course of data breaches that is often not fully considered. Some reported breaches in this industry are due to disgruntled employees, and other due to improper disposal of records as well as thefts.

Government Entities

Government agencies on both local and national levels aggregate vast amounts of sensitive information about individuals, and they can be as susceptible to reach of such data as any private entity, as demonstrated by reports of breaches of government agencies in the U.S. and UK.

- **Vendors**

Breaches by companies' third-party service providers such as outsourcers, contractors, consultants and business partners remain a concern, with reports of large breaches such as Target noting that vendors can be a point of access to company networks.[513]

Outsourcing of services is done to some extent in almost every business, and often involves transfer of or allowing access to Personal Information from a company to it vendor, such as IT, payroll, accounting, pension and other financial services, and operations vendors that obtain access to company

---

[512] *See, e.g.*, Legal Week Benchmarker study in association with Stroz Friedberg, *Locked Down? A Closer Look at the Rise of Cybercrime and the Impact on Law Firms*, May 2013.

[513] United States Senate Committee on Commerce, Science and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach*, March 26, 2014.

networks even if their function does not directly involve Personal Information. Entities that provide vendor services to other companies are a potential source of data breach risk for their clients, and their data protection procedures and standards can be as important as the companies' own. The data they have or have access to of their client's employees or customers is subject to loss or malicious theft, from insiders and outsiders. Even when data protection security standards are in place, vendors with access to large amounts of Personal Information or other confidential or sensitive information can make attractive targets for hackers.

The risk presented by vendors is generally recognized, but not always addressed. However, Massachusetts encouraged that it be addressed when it included in the Massachusetts Regulation a requirement that companies require by contract that their vendors implement and maintain appropriate security measures for Personal Information (see Section III. 2.e. above on Data Security Requirements: Massachusetts Remains at the Forefront in the U.S.), and other states also have contract requirements.

- **Employers of All Varieties**

  Many reported data breaches involve not the data of a company's customers, but that of its own employees. Employers retain Personal Information data of their employees for a variety of reasons, including payroll and benefits. Breached information in some cases involved the data of former employees, as well as current ones, illustrating the long-term hazard that may have prompted many regulators overseeing data security to scrutinize the period of time that companies retain data and whether the retention time is necessary for business operations. Compromised employee data also illustrates that virtually any type of entity that employees a staff, whether for profit or not, is potentially at risk for a data breach.

Some statistics on types of data and number of records exposed in recent breaches are:

- Credit card information continues to be a major target. In December 2013, Target became the "target" of one of the largest cyber-attacks in U.S. history. According to Target's statement, stolen information included "names, mailing addresses, phone numbers or email addresses for up to 70 million individuals." The data was reportedly retrieved by stealing encrypted PIN data, customer names, and credit and debit card numbers and expiration dates from the magnetic strips on the backs of cards used at Target between November 27th and December 15th.[514]

- The industries most commonly affected by Point-of-Sale intrusions remain restaurants, hotels, grocery stores and other brick-and-mortar retailers. For web

[514] USA Today, *Target: Data Stolen from Up to 70 Million Customers*. January 10, 2014. http://www.usatoday.com/story/money/business/2014/01/10/target-customers-data-breach/4404467/.

based attaches, the top industries are information, utilities, manufacturing and retail.[515]

- According to one 2013 study, the Healthcare industry was the most frequently breached industry (29.3% of all cyber breaches) followed by the Financial Services Industry (15%).[516]

- As of March 11, 2014, the healthcare industry accounts for 46.2% of all data breaches, with 962,228 records exposed. This represents a 3% increase in the proportion of total breaches occurring within the healthcare industry. Since 2009, over 29 million patient records have been exposed.[517] Criminal attacks on the healthcare systems have reported risen 100% between 2010 and 2014.[518]

- Among the main industries affected by security incidents in 2013 (and thus most likely to trigger data breach notification requirements) were retail, accommodation and financial services.[519]

- Of the various types of assets compromised in 2013 by payment card skimmers, one study found that automated teller machines (ATMs) users were most frequently breached (87%), with gas terminals coming in second at 9%.[520]

- In 2013, approximately 90% of all attackers were able to compromise their targets within a day or less, whereas only approximately 25% of victims were able to detect such breaches within a day. This disparity has been increasing year-to-year over the last decade.[521]

- One 2013 EU study found that 12% of internet users have had their social media or email account hacked.[522]

- A 2014 study found that the most common attack (81%) on social networks was a "fake offering" inviting users to join a fake event or group, where joining often requires the user to share credentials with the attacker or to send a text to a premium rate number.[523]

---

515 Verizon, *2014 Data Breach Investigations Report*, *supra.*

516 NetDiligence Data Breach Report, *supra*.

517 See Identity Theft Research Center 2014 Data Breach Stats, March 2014. http://www.idtheftcenter.org/images/breach/ITRC_Breach_Stats_Report_2014.pdf

518 Ponemon Institute LLC, Report, March 2014, *Fourth Annual Benchmark Study on Patient Privacy & Data Security*.

519 Verizon, *2014 Data Breach Investigations Report*, *supra.*

520 Verizon, *2014 Data Breach Investigations Report*, *supra.*

521 Verizon, *2014 Data Breach Investigations Report*, *supra.*

522 Commercial Risk Europe, *supra*.

523 Symantec, *Internet Security Threat Report 2014*, *supra*.

- In 2013, 13.1 million consumers suffered identity fraud, the second highest level on record.[524]

- In 2013, the United States was victim to the most cyber-espionage attacks, with 54% of all such attacks globally targeted at U.S.-based networks of systems linked to state-affiliated actors.[525]

- One study found that, in contrast to 2012, the greatest mobile threats are now attacks that track users by spying on the devices, including collecting text messages and phone logs and tracking GPS coordinates. Such attacks amount to 30% of all mobile threat attacks. In contrast, attacks that steal information from mobile devices, particularly device information, configuration data and banking details, accounts for 28% of all mobile threats, down from 32% in 2012.[526]

- Of the major mobile devices, a 2014 study found that Apple iOS iPhone/iPad had by far the most documented vulnerabilities in 2013 with 82% of all mobile vulnerabilities. The Android came in second at 13%.[527]

- One study on per capita costs note that the Healthcare industry reports the higher per capita data breach costs of any surveyed industry at $359, with Education coming in second at $294 and Pharmaceutical coming in third at $227.[528]

c. Causes

- Approximately 60% of all data theft in 2013 was driven by financial motives (down 15% from 2012), although espionage and activism (attacks by hacktivists) are substantial.[529] The motives vary by industry; for example, financial motive is primary in incidents involving the retail industry, and espionage is more often the motive for incidents involving manufacturing companies.[530]

- A 2014 study found that in the U.S., 44% of all data breaches were caused by a malicious or criminal attacks, 31% were caused by human errors and 25% were caused by system glitches.[531]

- In one survey of 120 global organizations, 74% noted that security breaches involving third parties were among their top security threats.[532]

---

524 Javelin, *2014 Identify Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends*, 2014. https://www.javelinstrategy.com/brochure/314

525 Verizon, *2014 Data Breach Investigations Report, supra.*

526 Symantec, *Internet Security Threat Report 2014, supra.*

527 Symantec, *Internet Security Threat Report 2014, supra.*

528 Ponemon, 2014 Cost of Data Breach Study, *supra.*

529 Verizon, 2014 *Data Breach Investigations Report, supra.*

530 Verizon, 2014 *Data Breach Investigations Report, supra.*

531 Ponemon, 2014 Cost of Data Breach Study, *supra.*

- A study of 140 claims submitted to insurers found that lost or stolen laptops and other devices were in first place at 207% of claims, with hackers at 18.6%, rogue employee at 12.1%, malware and viruses at 10% and paper records at 8.6%.[533]

- At least for breaches regarding credit cards, less than 1% of perpetrators used tactic rated as of high difficulty, and 78% of the techniques reviewed were in the low or very low categories of difficulty for initial compromise. Organizations breached tended to be less compliant with Payment Card Industry Data Security Standards than the average organizations.[534]

- A May 2013 Security Risk survey based on interviews with IT professionals reported that 91% of companies had at least one external IT security incident, and 85% had at least one reported internal incident. The survey revealed that nearly 90% of all respondents significantly underestimated the amount of new malware samples that appear daily (approximately 200,000).[535]

- The percentage of data breaches involving malware was lower in 2013 (although the total number of incidents have increased), but this is attributed to a relative proportional increase in other categories, such as social network threats and hacking, as opposed to an actual decline.[536]

- Malware targeting Android mobile operating systems grew 400% in 2012, going from 50,000 to over 200,000 new malicious programs identified as targeting the platform.[537]

- One 2013 IT survey noted that among their respondents, malware (66%), spam (61%), phishing (36%), network intrusion (24%) and theft of mobile devices (21%) were the five main threats generally faced by such companies.[538]

- The new "bring your own device" trend has resulted in an increase in breaches, with one survey noting that 95% of all of its respondents reported at least one mobile device-related security incident in 2013.[539]

- One 2013 study noted that the act of "phishing" is on the rise, with 32% of all respondents indicating that phishing has most changed their risk exposure.[540] The

---

532 Deloitte, 2013 TMT Global Security Survey, *supra*.

533 NetDiligence Data Breach Report, *supra*.

534 Verizon 2014 PCI Compliance Report.

535 Kaspersky, *Global Corporate IT Security Risks: 2013*. May, 2013. http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf.

536 Verizon, 2014 *Data Breach Investigations Report, supra*.

537 Trustwave, *2013 Trustwave Global Security Report.*

538 Kaspersky, *supra*.

539 Kaspersky, *supra*.

same study also notes that 45% of respondents say that mobile computing has most changed their risk exposure.

- One 2013 study found that lost/stolen laptop/devices were the most frequent cause of actual financial losses (20.7%) followed by hacking (18.6%).

- One 2013 study of over 2,200 applications found that 80% of all such applications were vulnerable to problems related to server misconfiguration, improper file settings, outdated versions of applications, or other post-implementation misfires that leave such applications particularly vulnerable to attackers.[541]

- According to one study, nearly 46% of iOS and Android applications analyzed use encryption improperly.[542]

- One study noted that in 2013, approximately 18% of all users will visit a link in a phishing email, compared to 9% of users that will click on an attachment.[543]

- In 2013, 1 in 196 emails contained an email virus, compared to 1 in 291 in 2012.[544]

- A 2014 study found that hackers are accountable for 34% of all exposed identities, with 29% of exposed identities attributable to accidents and 27% attributable to thefts or losses of computers or hard drives.[545]

- The use of "bots" to compromise computers is on the rise in the U.S., with 20% of all malicious "bot" activity occurring in the U.S. in 2013, as opposed to only 15.3% in 2012. China comes in second with 9.1% of all malicious "bot" activity in 2013.[546]

d. Breach Discovery and Response

Reports of 2013 breaches provide the following information about the discovery of, and response to, data breaches:

- Outsiders are still the main source of detection of a data breach, including customers and law enforcement. About 50% of incidents take months or longer to discovery,

---

[540] Ernst and Young, Insights on Governance, Risk and Compliance, October 2013. *EY's Global Information Security Survey 2013. (*"Ernst and Young Report") *http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf*

[541] Hewlett-Packard, *Cyber Risk Report 2013 Executive Summary*, 2013. http://images.info.arcsight.com/Web/ArcSight/%7B18595257-4120-428e-9021-8ce6267def8c%7D_4AA5-0920ENW.pdf

[542] Hewlett-Packard, *supra*.

[543] Verizon, *2014 Data Breach Investigations Report, supra.*

[544] Symantec, *Internet Security Threat Report 2014, supra*.

[545] Symantec, *Internet Security Threat Report 2014, supra*.

[546] Symantec, *Internet Security Threat Report 2014, supra*.

although once discovered about half of organizations studied in one report took days or less to respond and contain an incident.[547]

- One study indicated that data was able to be recovered within minutes in only 27% of all incidents, suggesting that in most instances, such organizations were not adequately equipped to handle breaches.[548]

- Mitigation of certain attacks, such as denial of service, malicious insiders and web-based attacks, will often require enabling technologies such as SIEM, intrusion prevention system, application security testing and enterprise governance, risk management and compliance (GRC) solutions.[549]

- Costs of a breach response are reduced if the breached entity has a strong security posture, incident response plan, and Chief Information Security Officer.[550]

- According to a recent 2013 survey of nearly 600 directors around the country, knowledge of information technology was among the top four qualities that respondents considered when deciding on their new directors. 40% of all respondents noted their boards could improve their knowledge and understanding of risk oversight.[551]

- One 2013 survey indicates that only 10% of organizations have an information security function that reports directly to the CEO. The survey also indicates that only 35% of organizations have information security professional that report to the board (or equivalent governing structure) on a quarterly basis, and only 10% on a monthly basis.[552]

- 43% of respondents in one particular survey noted their information security budgets are on the rise, with 46% of respondents indicating their budgets are switching from operations and maintenance of current security systems to actively improving and innovating such systems. Furthermore, 68% said their information security systems only partially meet their needs and are now actively working to improve such systems. Twenty-five percent of all respondents had no threat intelligence program. Perhaps most importantly, 59% of all respondents in the survey indicated a perceived increase in external threats.

---

547 Verizon, *2014 Data Breach Investigations Report, supra.*

548 AlertsecExpress, *23% of Organizations Faced a Security Breach in 2013*, *supra*.

549 Ponemon 2013 Cost of Cyber Crime Report, *supra.*

550 Poneman, 2014 Cost of Data Breach Study: Global Analysis, *supra.*

551 SpencerStuart, *What Directors Think: 2014 Survey*, 2014, available at: https://www.boardmember.com/uploadedFiles/Home/Research/Articles/What_Directors_Think_2014_Results-final_2-27-14.pdf

552 Ernst and Young Report, *supra.*

- A study of 313 companies found that only 32% had procured a cyber-insurance policy to manage the risk of attacks or threats. A majority of such companies were satisfied with their coverage.[553]

- A 2013 IT survey reflects anti-malware solutions are the most common way of securing a corporate IT infrastructure, yet only 54% of respondents use tools to manage their regular software updates, down 9% from 2012.[554]

- Reporting of data breaches has been waning, with one study noting that 57% of companies do not report data breaches unless they are required by law. Only 35% of such respondents shared information with industry peers.[555]

- A 2014 study found that participating U.S. companies faced an average breach notification cost of $509,237 per year.[556]

- One study notes that with respect to POS intrusions (remote attacks against environments where retail transactions are conducted), 51% of all systems are compromised within seconds and in 88% of cases the desired information is removed by the attacker within minutes. In contrast, in 85% of all cases discovery of the breach and extraction does not occur until "weeks" after the compromise.[557]

The reality is that any entity that obtains, maintains or transmits Personal Information of employees, customers, clients, or any other third party is potentially exposed to a data security incident and related costs. These costs include direct expenses such as engaging forensic experts, obtaining legal advice as to whether notifications are required and if so to whom and their content, payment of any fines imposed, and the defense and resolution of third-party claims, as well as the indirect costs of in-house time spent addressing the incident and supporting the resulting investigations, the damage to reputation, and the loss of customers, business and related revenue. While not all incidents of penetration of networks or breach of data security are confirmed to be data breaches as defined by applicable law, those that are generally involve substantial costs of providing notifications and outsourced call center support, offers of free credit monitoring subscriptions and identity theft insurance and discounts for future products and services.

2. The Importance of Timely and Proper Notification

A poorly executed breach response can harm a company's reputation and increase its out-of-pocket costs, including exposure to fines and lawsuits arising from non-compliance with data security laws and regulations.

---

553 Ponemon, 2014 Cost of Data Breach Study, *supra.*

554 Kaspersky, *supra*.

555 Advisen Cyber Risk Network, *Survey: data breach reported, maybe, if law requires*, March, 2014.

556 Ponemon, 2014 Cost of Data Breach Study, *supra.*

557 Verizon, *2014 Data Breach Investigations Report, supra.*

One study noted that quick notification is actually a factor that increases the cost of a data breach, but $10.45 per record.[558] This indicates that a thoughtful, unrushed response is important in responding to a breach and avoiding cost inefficiencies and the potential need to supplement notifications with resulting cost duplications.

Loss of customers remains a major cost of a data breach, as discussed in many of the studies of the cost of data breaches this past year cited here. In a prior study of consumer response to data breaches, 83% of consumers surveyed reported receiving a data breach notification during the 24 months prior to the survey, while 55% had been notified of two or more data breaches.[559] The study found that 63% of the respondents said the notification letters offered no direction on the steps consumers should take to protect their personal information and, as a result, 31% terminated their relationships with the organization and 57% said they lost trust and confidence in the organization. Over half of the respondents rated the timeliness, clarity, and quality of the breach notification as only poor-to-fair.[560]

Also to be taken into account is that lawsuits arising from data breaches often include causes of action alleging the breached company failed to timely notify customers and others whose Personal Information was compromised by the breach, proximately causing damages that allegedly would have been avoided or minimized with a more timely response. Moreover, recent regulatory investigations of data breaches have often focused on the length of time the company sustaining a breach took to notify those affected.

These statistics reinforce the importance of companies establishing a good response plan before a breach occurs so they can address a breach promptly and properly. This is critical both for maintaining regulatory compliance and for minimizing the negative impact on customer relationships and business reputation.

Thus, having a breach response plan in place is likely to enable a company to respond to a breach both appropriately and within a reasonable time frame, and support a company's legal defense against third-party lawsuits as well as regulatory investigations arising from the breach.

3. The Potential Costs and Damages of a Breach

The costs of a data breach include both the direct costs of immediate investigation, response, notification and remediation costs, and the indirect and at times longer-term costs of reputational damage and business interruption that can result from a publicized data breach. Costs of a breach can also often include liability to third parties whose Personal Information is acquired without authorization causing them financial detriment, or who sustain other losses as a result of a data breach that can be attributed to the negligence of the breached entity. Even if such third-party claims do not ultimately succeed, they can involve very substantial litigation costs to defend. For publicly traded corporations, there is also often an effect on the stock price when a breach of their

---

[558] Ponemon, *2014 Cost of Data Breach Study: Global Analysis, supra.* Similar results of a quick notification increasing costs was found in prior years' studies as well. See, e.g., *2010 Annual Study: U.S. Cost of a Data Breach.*

[559] Dr. Larry Ponemon, C*onsumer's Report Card on Data Breach Notification*, Apr. 15, 2008.

[560] *Id*.

data security is reported and, as discussed above, recent SEC Guidance identifies cyber risks and incidents as potentially material information to be disclosed by publicly traded companies.

For insurers of companies that sustain a data breach, there are often claims under a variety of policies ranging from traditional general liability to D&O policies and some types of professional liability and errors and omissions policies, to crime policies, to specialty data breach and cyber risk policies, as insureds seek recovery of at least some of the substantial financial costs that they incur when they are involved in a data breach.

As noted above, in one study of 2012 breaches, the average total cost of a data breach per company was more than $11.6 million.[561] Another study of payouts by insurers for covered breaches that occurred between 2010 and 2012 reported the average total cost per incident estimated at $3.5 million/.[562] Although averages may be driven up by a few outlier breaches of either extraordinarily large number of records or unusually large costs per record, the unavoidable reality is that a breach results in substantial costs, due to mandatory reporting requirements for breaches involving Personal Information, the third-party claims that many breaches trigger, and the reputational damage and business disruption to the entity sustaining the breach.

a. First-Party Costs

The range of immediate economic costs to entities sustaining a breach involving Personal Information often include:

- Payment of forensic experts to find the cause of the breach and what needs to be done to stop it or prevent recurrence, and to evaluate if the cause was due to any non-compliance with applicable law or standards;
- Obtaining legal advice on whether notice requirements are triggered and, if so, which ones and the types and content of notice required;
- The cost of providing notice, including printing and mailing of letters;
- The cost of providing a call center to answer inquiries by individuals receiving the notice;
- The cost of credit monitoring services and identity theft insurance, if offered; and
- Payment of public relations consultants for publicity control.

Added to these are the "indirect" costs of loss business and reputational damage, which some of the studies cited above quantify as over half the cost of a data breach. (See Section V above on the Ezposures Presented by Data Breaches, which cites to numerous recent studies that have attempted to quantify the cost of a data breach).

---

561 Ponemon, 2013 *Cost of Cyber Crimes Study*, *supra*.

562 NetDiligence Report, Oct. 2013, *supra.*

b. Fines and Penalties

Additional significant costs to entities subject to data breaches are contractual and regulatory assessments, often referred to as fines and penalties, although the legal nature of such assessments and whether they qualify as fines, penalties or compensatory damages has been the subject of dispute and litigation.[563]

For entities subject to payment card breaches, there are often contractual fines and other assessments imposed under the Payment Card Industry rules, regulations and contractual agreements if there is a failure to comply with their standards for protection of payment cardholder information. Such assessments are in various categories, with some for non-compliance with PCI-DSS (the Payment Card Industry Data Security Standards) often expressly labeled as a fine, with other categories labeled in PCI industry contracts as for fraud reimbursement and for operational/administrative costs. (See Section on the Regulatory and Statutory Landscape in the U.S., subsection on PCI Standards for Protection of Credit Cards, above).

Additionally, breached entities are often subject to regulatory fines and penalties that may be imposed by regulatory agencies and states' attorneys general, as well as statutory imposition of assessments per violation that raise the issue of whether they are in the nature of fines, punitive damages or compensation. These often raise insurance coverage issues, as many policies preclude or limit coverage for fines, penalties and damages that are punitive, exemplary, or multipliers of compensatory damages. (See section on Insurance Company Exposures, below).

c. Third-Party Claims

Third-party claims by those who have allegedly been damaged by a data breach trigger longer-term costs to the breached entity, and those generally include substantial defense costs even when the claims are defeated. Section VII of this White Paper, Privacy Litigation: Current Issues, discusses trends in privacy-related litigation. However, we also identify here some of the exposures to third-party claims faced by entities that have been the subject of a data breach of Personal Information.

i. Consumer Claims

Consumer claims in the breach context in the past have had only limited success, as they face a number of obstacles, although recently there have been some successes by plaintiffs in avoiding early dismissals.

At the inception of a lawsuit, courts scrutinize whether the consumers have Article III Constitutional standing to pursue their claims, which requires an injury in fact (see discussion on Standing in Litigation section below). Courts will also analyze whether the consumers have sustained a legally cognizable injury under the applicable state's law. While many data breaches

---

[563] As discussed above in Section III.3, on PCI Standards for Protection of Credit Cards, recent litigation about the nature of the PCI assessments include: *Elavon Inc. v. Cisero's Ristorante,* No. 100500480 (3d Dist. Ct, Summit County, Utah); *Genesco Inc. v. Visa USA Inc., et al.*, Case No. 3:13-cv-00201 (U.S. District Court, Middle District, Tennessee.); *Schnuck Markets, Inc. v. First Data Merchant Data Services Corp. and Citicorp Payments Services, Inc.*, Case No. 4:13-CV-2226-JAR (U.S. District Court, Easter District of Missouri).

involve unauthorized access to Personal Information, affected individuals have not always been able to demonstrate that they sustained the requisite injury or recoverable damages.[564]

However, some recent decisions indicate that while consumers will likely still have difficulty ultimately prevailing in most claims absent demonstrated actual identity theft and resulting financial losses, defendants may not be able to obtain early pre-discovery dismissals of consumer claims as readily as they were in the past. Many of the early battles in consumer actions against breached entities focused on whether the consumers had the requisite injury in fact to establish standing and survive a motion to dismiss, as well as a legally cognizable injury under the applicable state law. Often, consumers do not actually sustain identity theft, and thus there have been a growing number of somewhat varying decisions as to what constitutes sufficient injury, and increasing claims of violation of consumer protection statutes under which there are assessments per violation without regard to actual economic loss to the consumer. These issues and a number of these cases are discussed in the section on Privacy Litigation: Current Issues below.

Yet another obstacle to consumer claims is the prospect that the consumer's application for class certification may be denied. The losses claimed by an individual consumer will generally be minimal. On the other hand, certification of a class of thousands, or millions, of affected consumers can multiply such losses and thereby create the incentive for plaintiffs' lawyers to pursue litigation. Moreover, consumer plaintiffs may have difficulty obtaining certification of their lawsuits as class actions due to the highly individualized proof of loss and of causation of loss by the breach in issue required for each plaintiff, and the difficulties in demonstrating that questions of fact and law common to class members predominate over questions affecting only individual members.[565]

ii. Bank Claims

Added to the list of potential third-party claims are efforts by banks and credit unions that sustained losses as a result of their customers' payment cards being canceled and replaced, and of fraudulent charges they absorbed, to recover such financial losses from the entity breached. While often consumers cannot demonstrate actual financial loss if they did not sustain or pay unauthorized charges, banks have been increasing pressure on state and federal lawmakers as well as on courts to allow them the right to reimbursement from breached entities for the costs banks, particularly

---

564 Consumer liability for fraudulent credit card charges is limited by federal statutes, such as *The Electronic Fund Transfers Act* (EFTA), see *EFTA*, Pub. L. No. 95-630 (Title XX § 2001), 92 Stat. 3728 (Nov. 10, 1978), codified at 15 U.S.C**.** §1693 *et seq*. *See also Truth in Lending Act* (TILA), 15 U.S. C. §1643. Moreover, at least some of the card brands have a "zero liability policy" under which the card issuer will not hold the cardholder responsible for unauthorized purchases under many circumstances. MasterCard is reportedly extending its zero liability policy in the United States to include all PIN based and ATM transactions, Reuters, *MasterCard extends zero liability policy to ATM transactions*, May 28, 2014, http://www.businessinsurance.com/article/20140528/NEWS07/140529863?tags=

565 As confirmed by the U.S. Supreme Court in *Wal-Mart Stores, Inc. v. Dukes*, 131 S.Ct. 2541 (Jun. 20, 2011), there must be a certain degree of commonality among members of a plaintiff class, which requires more than an alleged violation of the same law (reversing class certification, noting that millions of employment decisions were in issue, and holding that "[c]ommonality requires the plaintiff to demonstrate that class members 'have suffered the same injury'" and that the common contention "must be of such a nature that it is capable of class wide resolution, which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one strike" and noting that the trial court is required to undertake a "rigorous analysis").

See, as an example of the difficulties of overcoming the hurdles to class certification, *Stollenwerk v. TriWest Healthcare Alliance*, No. 03-0185 (D. Ariz., Jun. 10, 2008).

payment card issuing banks sustain from absorbing fraudulent charges and reissuing debit and credit cards.

Many issuing banks forgo litigation, relying for recovery on the contractual indemnification provisions in their payment card processing agreements with entities in the chain of accepting, processing, and paying payment card charges. (See Section III.3 on PCI-DSS above). However, some financial institutions who may not be fully reimbursed by that contractual system, have sought recovery from breached merchants, payment processors, and others in the chain of payment card processing who may have contributed to the breach and resultant financial losses to banks and credit unions.

While initially the legal basis for efforts by banks and other financial institutions to recover their costs from a breached company were very limited, efforts are underway to provide routes for legal recourse. As noted above, Washington State passed legislation that provides for liability of a credit or debit card processor or business to a financial institution if the processor or business fails to take reasonable steps to guard against unauthorized access to account information that is in its possession, and such failure is found to be the proximate cause of a breach. Similarly and as also discussed above, the Minnesota Plastic Card Security Act provides that financial institutions may recover from a company that accepts payment cards if the company retains card security code data, PIN verification code numbers or the full contents of any track of magnetic stripe data for longer than 48 hours after authorization of a transaction and there has been a security breach exposing payment card data.

Several cases illustrate the courts' approach to whether such claims by banks constitute cognizable injuries under common law, and which causes of action courts are likely to recognize and which they tend to dismiss. In one of the first of these,[566] the First Circuit Court of Appeals held that, under Massachusetts law, banks issuing credit and debit cards to customers who subsequently had that card information stolen from a merchant's computer systems and used for fraudulent transactions, stated a claim against the store operator and the bank serving as its "processing bank" for the store's payment transactions. The banks claimed that both the merchant and its processing banks were negligent in failing to follow PCI-DSS security protocol and in delaying notice after the breaches had been discovered, and that as a result they had sustained financial losses from reimbursing the customers for fraudulent charges, monitoring their accounts, and cancelling and reissuing payment cards. Their complaint included claims for negligence, breach of contract, and unfair or deceptive practices, and also sought to assert a claim for conversion. The First Circuit upheld the denial of the dismissal of the negligent misrepresentation claim that was based on the argument that by accepting and processing credit card transactions, the merchant and its processing bank impliedly represented that they would comply with MasterCard and Visa data security requirements, although it noted that "the present claim survives, but on life support." Similarly, the claim for unfair or deceptive trade practices survived dismissal, but primarily based on the lack of discovery of the defendant's conduct in issue and with reference to the merchant's argument for dismissal having to "await discovery and perhaps a summary judgment motion." However, the dismissal of the tort-based negligence claim was upheld on the grounds that Massachusetts, like so many states, holds that "purely economic losses are unrecoverable in tort and strict liability actions

---

566 *In Re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489 (1st Cir. 2009) (as amended on rehearing in part May 5, 2009).

in the absence of personal injury or property damage." Efforts by one bank to claim "property damage" based on property interest in the payment card information failed on the grounds that it was not a result of physical destruction of property. The dismissal of the breach of contract claim was also upheld, as while the merchant and its processing bank had agreements with Visa and MasterCard to comply with certain security procedures, the claimant banks were not parties to those contracts and did not demonstrate that they were third-party beneficiaries of those contracts. The First Circuit also upheld the denial of the addition of a claim for conversion, although in wording that arguably left the door open for it to be more successfully pleaded in another matter. Subsequent to the First Circuit's decision, the remaining parties settled their claims and the District of Massachusetts dismissed the case.

In another case,[567] the Supreme Judicial Court of Massachusetts demonstrated that even if a claim survives a motion to dismiss, it may not survive a motion for summary judgment. The court upheld two lower court decisions dismissing claims by credit unions and their insurer for damages arising from an alleged data security breach in which third parties obtained and fraudulently used debit and credit card information of cards issued by the credit unions, for which fraudulent charges the credit unions reimbursed their customers and the credit unions' insurer then reimbursed the credit unions. Like the First Circuit, the Court upheld dismissal of the third-party beneficiary contract claims because the plaintiffs could not show that they were intended beneficiaries, and upheld dismissal of the negligence claims under the economic loss doctrine. With regard to claims for fraud and negligent misrepresentation, which were based on allegations that in accepting credit and debit cards for payment the defendants represented that they were in compliance with Visa and MasterCard regulations prohibiting them from storing data, the court upheld summary judgment dismissing those claims after finding that the plaintiffs had never seen the defendants' agreements with Visa and MasterCard and thus they could not establish that the defendants' representations induced them to become or remain card issuers. The court also found that the plaintiffs could not establish that they would have altered their participation in the card system after becoming aware of the defendants' breach. Additionally, the court found that any reliance on the alleged misrepresentations would have been unreasonable.

Banks continue to pursue litigation against companies that have suffered data breach of debit and credit card information. After Heartland Payment Systems, a processor of debit and credit card transactions, reported that debit and credit card data had been stolen from its system, a number of issuing banks that paid fraudulent transactions and replaced credit cards of customers filed lawsuits against Heartland and its acquiring banks in federal court in Texas.[568] The plaintiffs asserted claims for negligence, negligence *per se*, negligent and intentional misrepresentation, violation of consumer protection statutes, and breach of contract. The U.S. District Court for the Southern District of Texas decided Heartland's motion to dismiss the claims of the Financial Institution plaintiffs, which were nine issuer banks (banks that provided the credit/payment cards to consumers) that alleged that the data breach resulted from a failure by Heartland to follow industry security standards (PCI-DSS), resulting in the issuing banks incurring significant expenses replacing payment cards and reimbursing fraudulent transactions. The court initially granted the motion to dismiss in part and denied it in part, holding that (1) the claims for negligence and

---

567 *Cumis Ins. Soc'y, Inc. et al. v. BJ's Wholesale Club, et al.*, 918 N.E.2d 36 (Mass. 2009).

568 *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, Case No. 09-MD-2046-LHR (S.D. Tex.).

violation of New Jersey, New York and Washington states' consumer protection laws were dismissed with prejudice; (2) the claims for breach of contract, breach of implied contract, express misrepresentation, negligent misrepresentation based on nondisclosure, and violation of California, Colorado, Illinois and Texas consumer protection statutes were dismissed without prejudice and with leave to amend; and (3) the motion to dismiss the claims brought under the Florida Deceptive and Unfair Trade Practices Act was denied.[569] A later decision held that the Amended Complaint failed, and the District Court dismissed the action in its entirety.[570] Attempts by credit card issuer banks affected by the Heartland breach to obtain additional recoveries continued, and the card issuing banks appealed the dismissal of their claims. This resulted in a decision by the Fifth Circuit reversing the dismissal and remanding the case for further proceedings, on the grounds that the law of the applicable jurisdiction (New Jersey) did not bar a negligence claim by the banks against the breached card processor, Heartland, although part of the basis for the decision was that the record was not clear whether Heartland's contracts with its banks would require it to comply with the Visa and MasterCard rules and regulations providing contractual dispute resolution and compensation mechanisms for losses, and whether it had contracts directly with Visa and MasterCard that would govern.[571]

Recently, the large losses arising from the Target retail breach has also generated litigation directly by banks and credit unions against the breached entity for costs such as card replacement and fraud losses and monitoring, including one Minnesota credit union reportedly relying upon the Minnesota statute [572] that provides for liability by a breached entity to financial institutions that issued a payment card (*e.g.*, issuing banks) for certain costs of reasonable actions undertaken by them in the event a breached company doing business in Minnesota retained certain card data in violation of the Act, apparently for losses allegedly not subject to the PCI recovery program.[573]

Banks have alleged a number of theories to try to obtain recovery from breached merchants, including attempts to allege that they are equitably subrogated to claims that consumers may have, but mostly without success.[574] While banks have struggled to avoid dismissal of common law claims, the legislation passed in states such as Washington, Nevada and Minnesota, discussed

---

569 *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig./Fin. Inst. Track Litig.*, 834 F. Supp. 2d 566 (S.D. Tex. 2011).

570 *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig./Fin. Inst. Track Litig.*, No. H-10-171, 2012 WL 896256 (S.D. Tex. Mar. 14, 2012), *rev'd in part, Lone Star National Bank v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013).

571 *Lone Star National Bank v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir. 2013).

572 Minn. Stat. § 325E.64.

573 The dozens of lawsuits filed against Target by consumers, shareholders, banks and credit unions have been consolidated before a U.S. District Court sitting in St. Paul, Minnesota, *In Re Target Corporation Customer Data Security Breach Litigation*, Case No. 0:14-md-02522-PAM. See also Tracy Kitten, *Bank Files Unique Suit Against Target: Umqua Bank Alleges Violations of Minnesota Statute*, Bank Info Security, March 17, 2014, http://www.bankinfosecurity.com/bank-files-unique-suit-against-target-a-6639/p-2 ; David Morrison, *Price is Right for Credit Union to Join Target Data Breach Lawsuits*, Credit Union Times, March 26, 2014, http://www.cutimes.com/2014/03/23/price-is-right-for-credit-union-to-join-target-dat; Advisen, *100 lawyers in a room Target case draws the suits to St. Paul*, May 15, 2014, http://fpn.advisen.com/articles/article218095276-888238653.html?user=.

574 *See, e.g.*, *BankNorth, N.A. v. BJ's Wholesale Club, Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006) (dismissing the issuing banks' suit against a breached merchant to recover for unauthorized charges to customer accounts based on claims of negligent failure to protect cardholder information and equitable subrogation); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F. 3d 162 (3d Cir. 2008) (dismissing negligence claim by a bank that issued credit cards against the merchant and its payment processor for costs associated with replacement of customer credit cards and reimbursement for fraudulent purchases).

above, is providing banks with statutory grounds for seeking damages even where common law grounds may fail. However, it is still to be seen whether any of these financial institutions will ultimately prevail in a direct action against a breached entity.

iii. Other Third-Party Claims

As breaches continue, an increasing range of potential third-party claims can be expected, by individuals and entities purportedly affected by breaches, as well as by regulators. For example, a nationwide class of mobile device users brought claims against members of the mobile device industry. There, the plaintiffs alleged that defendants violated their privacy rights under federal and state law by unlawfully allowing third parties to access their devices to collect and make use of personal information for commercial purposes without user consent or knowledge.[575] One study identified over 86 different causes of action cited in 231 cases arising from unauthorized disclosure of Personal Information, including a wide variety of tort and contract claims, and alleged violations of state and federal statutes.[576]

VI. Insurance Company Exposures

1. Exposure of Companies in the Insurance Industry as Entities Subject to Data Breaches

While insurers generally focus on the exposures of their insureds, they are themselves in an industry in which companies have potential exposure to data breaches. Insurance industry companies have the same vulnerabilities to data breach as other institutions. Some may even have an elevated risk due to their heavy dependence on computer systems and the nature of the information stored on their systems. As stated by the New York Department of Financial Services on May 28, 2013, when it sent letters to the largest insurance companies that it regulates requesting information on the policies and procedures they have in place to protect against cyber attacks: "The extraordinary sensitive health, personal and financial information that [people] entrust to their insurance companies is a virtual is a virtual treasure trove for hackers."[577]

First, at risk is their own employee information. As large-scale employers, often of employees residing in many different states (including Massachusetts with its rigorous data security requirements), insurers, reinsurers, brokers and companies servicing the insurance industry are subject to breach of their own employees' Personal Information, including payroll, personnel, pension, workers' compensation and disability claim information.

---

575 *In re iPhone Application Litig.*, No. 11-MD-02250, 2012 WL 2126351 (N.D. Cal. Jun. 12, 2012) (holding that although plaintiffs established Article III standing, alleged disclosure of users' personal data did not violate plaintiffs' right to privacy, and that plaintiffs failed to state a claim under federal, state, and common law claims).

576 Sasha Romanosky, David A. Hoffman, Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, Temple University Beasley School of Law Legal Studies Research Paper NO. 2012-29, available at http://ssrn.com/abstract=1986461.

577 See May 28, 2013 NYDFS press release, *Governor Cuomo Launches Inquiry Into Cyber Threats at Largest Insurance Companies*, available at http://www.governor.ny.gov/press/05282013-cuomo-launches-inquiry-cyber-threats-insurance-companies.

Second, at risk is the Personal Information insurers have of policy applicants, insureds, claimants and beneficiaries.[578] Liability insurers often have claimant information, ranging from medical records and financial documents to claimants identified by name and Social Security number which, if lost or improperly accessed, would be a data breach of Personal Information. Personal lines and life and health insurers may maintain Personal Information of policyholders and of beneficiaries, which are also subject to data breaches. Such Personal Information may remain stored by insurers, reinsurers, brokers, and third-party administrators as well as vendors of such entities, either in paper or electronic form, for decades.

Insurers are also subject to extensive state and federal regulation that includes requirements for safeguarding Personal Information, including pursuant to the Gramm-Leach-Bliley Act and implementing regulations promulgated by state insurance departments, as well as common law standards for protecting confidential information.[579] In addition, the departments of insurance of several states have issued bulletins and regulations requiring insurers and certain other of their licensees to send data breach notifications to the departments of insurance, in some cases under shorter timelines and under different definitions of "breach" than most other U.S. breach notification requirements. For example, the Connecticut Insurance Department issued Bulletin IC-25 in 2010 to require its licensees to notify the Department of any information security incident as soon as the incident is identified, but no later than five calendar days afterward, and requiring certain uncommon content and regulatory consultation.[580] The Washington State Office of the Insurance Commissioner promulgated a regulation effective June 1, 2013 requiring licensees to notify the insurance commissioner within two business days after determining that notification must be sent to consumers or customers pursuant to HIPAA or the Washington State breach notification requirement (Wash. Admin. Code 19.255.010).[581]

---

[578] For example, in February 2013, a putative class action was filed against an insurance company following an October 2012 data breach. The proposed class was alleged to include approximately 1.1 million people, and defined as follows in the complaint:

> All persons who sought an insurance quote from Nationwide Mutual Insurance Company or Allied Insurance Company, and whose names, and some combination of their Social Security numbers, driver's license numbers, dates of birth, marital statuses, genders, occupations, and their employers' names and addresses, were compromised by the October 3, 2012 data breach of the computer network used by Nationwide Mutual Insurance Company and Allied Insurance Company agents ….

See Galaria et. al. v. Nationwide Mutual Insurance Company, No. 2:13-cv-118 (S.D. Ohio, filed Feb. 8, 2013). On February 10, 2014 the defendant insurance company's 12(b)(6) motion to dismiss the action, in part, on the basis that the plaintiffs failed to allege any cognizable harm from the intrusion or that any third party used any of their personal information was granted. *See Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118, 2014 WL 689703 (S.D. Ohio, Feb. 10, 2014) (finding even if deprivation of value of personally identifiable information ("PII") was an injury-in-fact, the plaintiffs failed to allege facts supporting their assertion that they were deprived of the value of their PII and therefore lacked standing). The plaintiffs have filed a motion for reconsideration and a motion to file an amended complaint.

[579] *E.g*, in *Daly v. Metro. Life Ins. Co.*, 4 Misc. 3d 887, 782 N.Y.S.2d 530 (2004), a New York state court denied a motion to dismiss claims brought by a life insurance applicant against a life insurer arising from the purported theft of her personal information by a janitor who cleaned the insurer's premises and which resulted in fraudulent use of her personal information to create credit accounts. The court noted that after completing her application, the applicant had received a Privacy Notice from the insurer detailing the company's privacy policy and stating that confidential information would be safeguarded. The court found that the gravamen of the plaintiff's claim was that in order to obtain a life insurance policy the plaintiff had to provide sensitive personal information and the insurer represented that information would be protected and remain confidential. Thus, the court found that the insurer had a common law duty to protect the confidential personal information provided by the applicant and, in light of questions of fact concerning precautions taken by the insurer to safeguard that information, it denied summary judgment of claims at that juncture.

[580] The Connecticut Bulletin is available at http://www.ct.gov/cid/lib/cid/Bulletin_IC_25_Data_Breach_Notification.pdf.

[581] Wash. Admin. Code 284-04-625

Insurers are also subject to federal and state regulations of Personal Information and Protected Health Information that are not specifically directed at the insurance industry, but apply to all companies that obtain and maintain Personal Information (such as state data breach notification laws) or, with respect to Protected Health Information, to all entities subject to HIPAA[582] Thus, for example, the broad-ranging Massachusetts Regulation discussed above affects any entity that has Personal Information of a Massachusetts resident, and thus is likely to affect a significant number of insurers. It technically applies to liability insurers with Personal Information of Massachusetts claimants and to life insurers that have Personal Information of non-policyholder beneficiaries, as well as to those with employees or insureds who are Massachusetts residents.

Accordingly, in addition to the exposures insurers face as the issuers of policies that may cover the costs of data breach incurred by their insureds and claims asserted against insureds arising from data breaches, insurers and other entities in the insurance industry have their own risk of data breaches.

a. Potential Insurance Coverages for Data Breaches and Privacy Related Claims

The increasing range of costs incurred by entities that sustain a breach and the third-party claims against them have given rise to efforts by such entities to seek coverage for those costs and claims. Specialty insurance products have been developed to specifically address data breach and other cyber related risks, although not all address the full scope of costs and claims. Moreover, entities that sustain a breach that have not purchased policies directed at providing data breach coverage often look with varying success and failure to the more traditional types of policies they have in place for coverage of at least some of the costs, defense expenses and indemnity payments they incur.

A number of different types of insurance policies have the potential to be implicated in the event of a data breach and other types of cyber attacks that disrupt business operations and result in costs to and claims against the entity that sustained the breach or attack – or at least have the potential to be subject to a request for defense and/or indemnity – depending on factors such as the type of breach or attack, the relationship of the parties, the nature of the information in issue (Personal Information, Intellectual Property), the type of costs or damages in issue, the type of policy and, if for third-party liability, the allegations asserted and the type of damages in issue. As in all requests for coverage, the determination of coverage turns on policy terms, including both grants of coverage and exclusions, as well as on the specifics of the claim.

As the risk of data breaches and statutory privacy violations becomes increasingly recognized, policy definitions and exclusions are being added and tightened to reduce the exposure of policies not intended to apply to those risks, and sublimits for some types of costs are often included even in those policies expressly directed at insuring the risks of data breach, network security failures, and the claims arising from collection and usage of information about individuals. Many insurers

---

582 For instance, in July 2011, Wellpoint Inc. (an Indiana-based insurer) reportedly agreed to pay the State of Indiana $100,000 for failure to promptly notify consumers and the Indiana Attorney General after the Personal Information of thousands of Wellpoint customers was potentially accessible through an unsecured website. This settlement followed a 2010 lawsuit brought by the Indiana Attorney General against Wellpoint under Indiana's data breach notification statute. *See* Press Release, Attorney General reaches settlement with WellPoint in consumer data breach, Jul. 5, 2011, http://www.in.gov/portal/news_events/71252.htm.

impose application procedures directed at identifying the risks and the security procedures of the applicant entities, and some impose risk management conditions before agreeing to issue a policy that provides coverage for these types of claims.

As the field of privacy develops, so do the types of claims made, the effect of data breaches and privacy violations on individuals and companies, and the information available as to the nature and source of the cyber attacks and alleged privacy violations. These, in turn, raise new issues and exposures for insurers and their insureds. Thus, questions are increasing arising as to, *e.g.*, whether cyber attacks from foreign sources are government-sponsored and potentially subject to terrorism exclusions, whether attacks result in physical damage or loss of use of tangible property, whether information collection practices constitute knowing and deliberate conduct, and whether resultant business losses can be accurately measured and insured, among other issues.

Some of the issues that may be presented by a claim for coverage are identified below, although of course the issues can vary depending on the claim and the policy wording.

i. Cyber Risk/Data Breach/Privacy/Network Security Policies

A growing number of insurers are offering policies – or endorsements - specially tailored to provide coverage for a variety of cyber risks, ranging from breaches of Personal Information, to cyber extortion, to business interruption and reputational damage arising from cyber attacks, to claims of wrongful collection, usage or disclosure of information about individuals. Coverage has also been developed for liability associated with social media, such as posting of a defamatory comment on a blog. Some of these policies and endorsements are industry-specific, such as cyber risk insurance designed for technology companies, restaurants, healthcare entities, or financial institutions. In the current market, coverages are often expanded and new coverages developed, including express coverage for the Payment Card Industry (PCI) contractual assessments that are often associated with breaches of Personal Information involving credit card numbers. As data protection regulations and statutes, with concomitant response requirements, continue to be enacted and expanded in the U.S., E.U., and elsewhere, the market for such specialty products is expanding and new products are likely to be developed.[583]

Policies designed to provide data breach coverage do not necessarily restrict themselves to electronic breaches of statutorily defined Personal Information. These policies may also broadly encompass coverage for costs and claims arising from other types of data breaches and cyber attacks, including loss or theft of Personal Information contained in paper records and other types of confidential information that, while not itself Personal Information, can be used to obtain Personal Information or interfere with the business operations of a breached company or its clients. In addition to providing insurance coverage in the event of a breach, many insurers offer breach prevention services to their clients.

Some of these specialty policies have both first and third-party coverages. First-party coverages in such policies are generally designed to pay or reimburse an insured that has sustained a breach for

---

583 *See The Betterley Report – Cyber/Privacy Insurance Market Survey 2012: Surprisingly Competitive, as Carriers Seek Market Share,* June 2012; *Data protection measures could increase demand for cyber risk products*, Post Magazine, Dec. 16, 2011; *Cyber risks and data privacy market set for strong 2012 growth*, Insurance Insider, Dec. 12, 2011.

its own costs incurred in addressing a breach, such as notification costs, although some such policies limit coverage of notification costs to situations in which the insured is legally obligated to provide notice of data breach under state or federal statutes or to a maximum number of individuals. Policies directed at providing coverage for data breaches may also provide some coverage for costs directed at mitigating loss or reducing the likelihood of third-party claims, such as legal advice as to the company's notice obligations, credit monitoring offered to those whose Personal Information is compromised, and forensic investigation as to the cause of the breach. Some policies offer first-party coverage for business interruption losses related to data breaches, even in the absence of physical damage to tangible property. Liability coverages for defense costs and losses arising from a claim by a third party for damages arising from a data breach are also generally the subject of express coverages under such policies. Some cyber risk policies now also integrate coverage for online media liability.

However, even policies directed at providing coverage for data breaches of Personal Information and other privacy exposures vary in the scope of coverages provided and often have sublimits for certain types of costs or damages, and exclusions for others. Issues can arise as to whether there is coverage of costs incurred by an insured that are not legally required but are undertaken to preserve an insured company's reputation or reduce the likelihood of a third-party claim; of contractual indemnity obligations; of contractual fines and penalties as well as fines and penalties imposed by regulatory authorities; of breaches due to insured/employee dishonesty; of business interruption loss; of losses due to reputational harm; and of other types of claims or costs. The terms of these policies are largely untested by the courts, and their terms, conditions and exclusions are still in flux.

Moreover, the focus of such specialty policies is no longer just on data breaches and traditional out-of-pocket costs. There is increasing recognition of the exposures presented to companies by regulatory and legal proceedings asserting wrongful collection, usage and disclosure of information about individuals. Such information is often one of the most valued assets of companies, and a key component of targeted marketing, but recent increasing regulatory scrutiny from states and countries around the globe on company practices and disclosures of their collection and usage of such information have made both insurers and insureds consider the insurability of the exposures generated by such practices.

ii. Property Policies – First-Party

First-party property policies, which usually cover physical damage to real and personal property and may (depending on their terms) also provide coverage for resulting business interruption, may be scrutinized by insureds looking for potential insurance coverage, particularly those who sustain not only a data breach, but also business interruption losses, or costs for replacement of a computer system or data storage unit as a result of a breach.

However, such claims generally fail in the absence of some indication of physical damage to the computer system involved, or an express provision for coverage of replacement costs for loss of electronic data (which at times is offered, although usually on a sublimited basis). Such policies generally cover "direct physical loss or damage" to insured property caused by a covered cause of

loss. "Physical" is generally construed to mean "tangible."[584] Case law generally maintains that electronic data is not tangible property.[585]

Further, policy exclusions often specifically exclude or limit coverage of electronic data and other "valuable papers and records." Business interruption coverage is generally required to result from damage to or destruction of property caused by a loss otherwise covered under the policy, and thus if there is no physical loss or damage to tangible property in a data breach, the resultant business interruption losses are also generally not covered under a traditional property policy.

Non-coverage of a claim under a policy, though, cannot always be assumed. If a computer becomes unusable due to the installation of malware, a policyholder may be able to seek recovery under a coverage for loss of use of tangible property that is not physically injured.[586] There can also be claims involving destruction or corruption of electronic data on the system of the insured due to viruses which may be covered under the limited electronic data additional coverage provided by some property policy forms.[587] Further, there can be endorsements and other manuscript provisions added to more traditional business property forms that expressly provide some additional limited coverage for impairment of data systems and papers and other losses implicated in a data breach claim. Should there be potential coverage of any portion of a loss under a property policy, loss mitigation provisions may also be targeted by policyholders as a basis for requests for coverage of loss mitigation costs.

iii. Fidelity / Commercial Crime Insurance

In the 1990 film *Ghost*, one of the characters, who works at a financial institution, sets up a dummy account to facilitate a money-laundering scheme. In the event of a hypothetical real-world scenario where an insider steals customer account data in order to siphon money out of customers' accounts – and in the absence of a Patrick Swayze to change the password and thwart the crime – the financial institution might be able to bring a claim under its Fidelity and Crime insurance policy. Such policies generally protect organizations from the loss of money, securities, or inventory

---

584 *See, e.g., Florists' Mut. Ins. Co. v. Ludy Greenhouse Mfg. Corp.*, 521 F.Supp. 2d 661, 680 (S.D. Ohio 2007); *Philadelphia Parking Auth. v. Fed. Ins. Co.*, 385 F. Supp. 2d 280, 288 (S.D.N.Y. 2005).

585 *See, e.g., Ward Gen. Servs., Inc. v. Employers Fire Ins. Co*., 114 Cal. App. 4th 548, 556-57 (Cal. App. 4 Dist. 2003); *Se. Mental Healthcare Ctr., Inc. v. Pac. Ins. Co., LTD*, 439 F. Supp. 2d 831, 838-839 (W.D. Tenn. 2006); *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 93-98 (4th Cir. 2003); *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113 (W.D. Okla. 2001). Courts reaching a different conclusion have done so where the data is permanently lost to its owner, not merely improperly accessed. *See Computer Corner, Inc. v. Fireman's Fund Ins. Co*., 46 P.3d 1264 (N.M. 2002) (holding that loss of the pre-existing electronic data was tangible property damage covered by CGL policy where computer store repairing customer's computer permanently lost all the data); *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc*., No. 99-185, 2000 WL 726789, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (holding that computer data permanently lost during a power outage constituted "direct physical loss or damage from any cause" covered by first-party insurance policy); *NMS Servs. Inc. v. Hartford*, 62 Fed. Appx. 511 (4th Cir. 2003) (characterizing the erasure of vital computer files and databases as direct physical loss or damage to property for purposes of business income coverage).

586 *See, e.g., Eyeblaster, Inc. v. Fed.l Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).

587 *See, e.g., Lambrecht & Assocs. Ins. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. 2003) (holding that a property policy covered loss of business income due to damage to software and electronic data by a virus, where the section of the policy defining coverage for loss of income included "electronic media and records," defined to include electronically stored data); *see also Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., Ltd.*, 439 F. Supp. 2d 831,837-39 (W.D. Tenn. 2006) (finding corruption of a commercial insured's pharmacy computer after a storm and power outage constituted "direct physical loss of or damage to property" under business interruption policy).

resulting from employee crime. "Common Fidelity/Crime insurance claims allege employee dishonesty, embezzlement, forgery, robbery, safe burglary, computer fraud, wire transfer fraud, counterfeiting, and other criminal acts."[588]

Many data breaches involve theft and other criminal conduct by employees, *e.g.*, theft of laptops or other computer equipment containing Personal Information or other confidential data. Thus, depending on its terms and exclusions, the company's fidelity insurance may be triggered. Moreover, some fidelity or crime insurance policies may expressly provide for computer crime coverage in the form of a computer fraud endorsement, while others may contain exclusions that limit or preclude such coverage. Whether such an endorsement would provide coverage to the insured company for its losses and claim expenses arising from a data breach will depend on the policy terms, including if there is a loss of electronic data exclusion, and the jurisdiction considering the issue of coverage.[589]

iv. CGL – Third-Party Claims

An insured entity subjected to a lawsuit in connection with a data breach it suffers may tender the defense of that suit under its commercial general liability ("CGL") policy. While privacy and data security are developing areas of the law, there are a few judicial decisions indicating the likely issues on which a coverage dispute will focus when a claim for coverage is made under a CGL policy. However, in response to attempts to obtain coverage (or at least a defense) for breach related claims under CGL policy language developed before the prevalence of data breaches, recently new endorsements have been issued by ISO,[590] to amend policies and add provisions expressly directed at precluding or limiting the application of CGL policies to data breach and other types of cyber claims. Some insurers have developed manuscript policy forms of their own with provisions that preclude or in some cases affirmatively provide coverage for data breaches or other

---

588 Hossein Bidgoli, Handbook of Information Security, 820 (John Wiley and Sons, 2006).

589 For example, in *Retail Ventures, Inc. v. Nat'l. Union Fire Ins. Co. of Pittsburgh, PA*, No. 2:06-CV-00443 (S.D. Ohio Mar. 30, 2009), *aff'd,* Nos. 10-4576, 10-4608, 2012 WL 3608432, at *9 (6th Cir. Aug. 23, 2012, decided under Ohio law), coverage was found to be available for a data breach under a "Computer & Funds Transfer Fraud" endorsement of a commercial crime policy. There, a hacker fraudulently accessed a national retail company's computer system and stole data for approximately 1.4 million customers, including credit card and checking account information. As a result of the breach, among other costs, the U.S. Secret Service initiated an investigation; the company paid the cost of reissuance of credit cards for customers whose account information was fraudulently used; the Ohio Attorney General brought suit; and four class action lawsuits were brought by customers. The insurer argued, in part, that (1) the theft of the customers' data did not result in a "direct loss" to the store under the endorsement language, which only covered "loss . . . resulting directly from" theft of insured property, and (2) the following exclusion was applicable: "Coverage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind." The district court, however, disagreed with both points. It determined that the "direct loss" language of the endorsement required only application of the traditional *proximate cause* standard, and found that there was a "sufficient link between the computer hacker's infiltration of [the company's] computer system and [the company's] financial loss to require coverage . . . ." Second, the district court found the exclusion inapplicable, in part, because the information obtained in the hacking theft did not constitute "proprietary information" or even "other confidential information of any kind" within the meaning of the exclusion. On appeal, the Court of Appeals for the Sixth Circuit recently affirmed. *See Retail Ventures, Inc.*, 2012 WL 3608432, at *9 (6th Cir. Aug. 23, 2012) (finding that the district court correctly applied the proximate cause standard, and that "stored data consisting of customer credit card and checking account information would not come within the plain and ordinary meaning of 'proprietary information'"). However, the policy in issue apparently did not include an electronic data exclusion or other terms that, if present, might well have led to a different result.

590 ISO is the Insurance Services Organization, Inc., which provides policy language, statistical information, and other services to member property and casualty insurers. Its policy forms are filed for approval with U.S. state insurance departments, for use by admitted insurers.

types of cyber risks. Thus, case law that is based on versions of CGL policies that do not have such amendments is probably not a good indicator of how a court would decide a claim for coverage under a CGL policy that does incorporate such amendments.

While CGL coverage issues have recently become a battleground,[591] the field is not likely to be a static one. Insurers are amending policy forms, and policyholders will likely continue to attempt to find loopholes in CGL policies to trigger at least a duty to defend data breach claims in situations not contemplated by insurers or intended to be covered by such policies. Any success by policyholders will likely result in insurers again responding by drafting and including in policies additional exclusions and limitations on coverage directed at preventing any unintended coverage from being found.

(1) Coverage A – Bodily Injury and Property Damage

Coverage A of a CGL policy typically provides that "we will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage' to which this insurance applies." "Property damage" is typically defined as "physical injury to tangible property, including all resulting loss of use of that property," and "loss of use of tangible property that is not physically injured."[592]

Generally in data breach cases, the focus of analysis as to whether there is coverage, or at least sufficient allegations to trigger a duty to defend, under Coverage A is on its "property damage" prong. Because of the required component of "tangible property," it is usually considered unlikely that lawsuits related to a typical breach of electronic data security would be covered under Coverage A.[593] As in the first-party property policy context, case law generally maintains that electronic data is not tangible property.[594] Additionally, ISO's 2004 form and other CGL forms include in the

---

591 See cases identified in footnotes in this section, and in the section below about Privacy Litigation.

592 This is standard policy language in recent ISO form policies (see CG 00 01 12 04). While there is variance in language among different insurers' CGL policies, the ISO language is in widespread use and there are judicial decisions dealing directly with ISO wordings.

593 If tangible property is actually stolen, however, such as a CD containing personal information, it is possible that a court may find the "property damage" requirement satisfied (depending upon the precise definition of "property damage" in the policy at issue), at least for purposes of a duty to defend, although exclusions may nonetheless operate to preclude coverage. *See, e.g.*, *Nationwide Ins. Co. v. Cent. Laborers' Pension Fund*, No. 11-cv-618, 2012 WL 734193 (S.D. Il. Mar. 6, 2012) (employee of an accounting firm left a laptop with a CD in her automobile containing personal information of approximately 30,000 participants and beneficiaries of several pension funds that the accounting firm was performing audit work for; following theft of the CD, and claims by the pension funds against the employee to recover costs incurred as a result of the theft such as credit monitoring, the employee submitted a claim for coverage under her homeowner's policy, which provided coverage "[i]f a . . . suit is brought against an 'insured' for damages because of . . . 'property damage' caused by an 'occurrence' to which this coverage applies," and defined "property damage" as "physical injury to, destruction of, or loss of use of tangible property"; the district court found, under Illinois law, and for purposes of a duty to defend, that the property damage requirement *was satisfied* because the employee suffered a "loss of use of tangible property," but nonetheless found coverage excluded because the policy did not cover "property damage to property rented to, occupied or used by or in the care of the insured"), *aff'd,* 704 F.3d 522 (8th Cir. 2013) (finding that the exclusion for "in care of" the insured applied, as well as alternatively an exclusion for "property damage arising out of or in connection with a business engaged in by an insured").

594 *But see, e.g.*, *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 801-02 (8th Cir. 2010) (underlying allegations of loss of use of a computer – *e.g.*, that the computer "froze," was "taken over and could not operate," and was otherwise "no longer usable" due to software installed by the insured – found sufficient to satisfy the "loss of use of tangible property that is not physically injured" prong of the definition of "property damage").

definition of "property damage" the provision that "for the purpose of this insurance, electronic data is not tangible property."[595]

In addition, the 2004 ISO form (and many other CGL forms) include an Electronic Data Exclusion, according to which "this insurance does not apply to… damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." Under policies containing such an exclusion, for there to be any coverage there would need to be damages caused by physical injury to, or the loss of use of, "tangible property," which must be something other than electronic data. However, there may be data breaches involving damage other than to electronic data for which insureds may be able to satisfy the "tangible property" requirement as well as the "occurrence" requirement, and demonstrate either physical injury to that property or loss of use of the property containing the data, such as malware attacks that cause damage to computer hardware.

In 2013, ISO announced it was issuing an endorsement amending the Electronic Data Exclusion which was optional, [596] and in 2014 it issued "mandatory" endorsements for its filed CGL forms effective May 2014. It relabeled the Electronic Data endorsement (traditionally exclusion p to CGL Coverage A), to entitle it "Access or Disclosure of Confidential or Personal Information and Data-related Liability." In one version, it carved out from the exclusion for "loss of, loss of use of, damage to, corruption of, inability to access , or inability to manipulate electronic data" those damages that are because of "bodily injury"; another version is without that option. It also added a prong to the overall exclusion for access to or disclosure of a person's or organization's confidential or personal information. [597]

Further, while analyses of whether Coverage A applies have focused on the property damage aspect of that Coverage Part, Coverage A also applies to "bodily injury." The recent spate of consumer third-party claims has often included an emotional distress component. Thus, if a policy or governing law defines "bodily injury" as including emotional distress even when there is no physical injury, there potentially could be a claim for coverage for that aspect of the alleged damages. However, while the "tangible property" barrier would not apply to such a claim, the insured would still have to demonstrate that the "bodily injury" was caused by an "occurrence," and that the Electronic Data Exclusion in whatever form it is present in the policy did not apply, and circumvent any other provisions that may preclude coverage for the claim. The potential for

---

595 The ISO definition of "property damage" also defines "electronic data" for purposes of applying the policy: "As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."

596 ISO announced that in 2013 that its CGL policy form would include a revision of the electronic data exclusion that would make the exclusion expressly inapplicable to bodily injury claims. *See, e.g., Changes to the CGL Coverage Form*, International Risk Management Institute, Inc., Feb. 2013 ("The exclusion is being revised to make it inapplicable to bodily injury claims, meaning that only consequential property damage resulting from an electronic data loss is excluded. So, for example, loss of production on a computerized manufacturing assembly line caused by damage to the software that runs it would be excluded from CGL coverage. Injury to a patient in a hospital caused by the accidental corruption of electronic medical records would not be excluded.").

597 See ISO forms CG 21 06 05 14 (Exclusion - Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exception) and G 21 07 05 14 (Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – Limited Bodily Injury Exception Not Included). The exclusions expressly provide that they apply "even if damages are claimed for notification costs, credit monitoring expenses, forensic expense, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described … above."

coverage may be more likely for data breaches and other cyber incidents directly causing demonstrable bodily injury, such as those involving computer-controlled medical equipment that impact medical care of individuals, rather than for the typical electronic data breach involving Personal Information.

(2) Coverage B – Personal and Advertising Injury

Attempts at seeking coverage, or at least obtaining a defense, under CGL policies have been asserted under Coverage B, Personal and Advertising Injury. Results have varied depending on jurisdiction and claim.

Personal and Advertising Injury coverage under Coverage B is limited to injuries arising out of certain enumerated offenses.[598] Standard versions of Coverage B provides (until recent amendments to ISO forms): "we will pay those sums that the insured becomes legally obligated to pay as damages because of '*personal and advertising injury*' to which this insurance applies," and the policy's definition of personal and advertising injury generally lists the enumerated offenses for which coverage is provided. Although "personal injury" and "advertising injury" used to be separately defined as two different sets of enumerated offenses within Coverage B, the industry began merging the terms into one consolidated set of enumerated offenses in 1998.[599] Among those enumerated offenses is typically "injury … arising out of … oral or written publication, in any manner, of material that violates a person's right of privacy." This is the offense that is often alleged to apply when a claim for coverage for a data breach is made.

In response to efforts to obtain coverage under Coverage B based on this prong of the definition of personal and advertising injury, recently some insurers have amended the definition to delete this prong, in an effort to avoid costly coverage disputes. [600] Moreover, effective May 2014, ISO issued an endorsement including an exclusion applicable to Coverage B – Personal and Advertising Injury, which provides that the policy does not apply to "'Personal and Advertising Injury' arising out of any access to or disclosure of any persons or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of non-public information…."[601]

---

598 This is in contrast to Coverage A, which is typically triggered by an *accidental* occurrence. *Accord, e.g., Stonelight Tile, Inc. v. Ca. Ins. Guarantee Ass'n*, 58 Cal. Rptr. 3d 74, 89 (Cal. Ct. App. 2007) ("Personal injury liability is a term of art that covers certain enumerated offenses. Unlike liability coverage for property damage or bodily injury, personal injury coverage is not based on an accidental occurrence.").

599 *See* CGL Policy Handbook, § 9.01

600 The ISO revisions to its 2013 CGL form include the option of an endorsement that deletes the prong of "oral or written publication, in any manner, of material that violates a person's right of privacy" from the list of covered offenses in Coverage B. See ISO form CG 24 13 04 13, Amendment of Personal and Advertising Injury Definition, effective April 2013; *see also,* Chris Boggs, *ISO's CGL Changes for 2013 – Part III*, Claims Journal, Apr. 9, 2013, www.claimsjournal.com/new/national/2013/04/09/226615.htm. If such an endorsement were included in a policy, that would be a potentially significant change in the coverage afforded under the policy and remove the basis for many of the arguments that have been presented in coverage disputes for coverage of data breach claims under CGL policies. *See, e.g., Changes to the CGL Coverage Form*, IRMI, Feb. 2013, *supra;* Ted A. Kinney, *2013 Change in the Commercial General Liability Program*.

601 See ISO forms CG 21 06 05 14 and G 21 07 05 14, discussed above with regard to Coverage A.

However, there are still policy forms without those recently introduced amendments, and claims that could be submitted under those forms. Thus, case law based on versions of CGL policies that do not include the new amendments can still be relevant to many coverage disputes arising out of requests for coverage for a breach claim. To successfully tender a data breach claim under a CGL policy that has the prong of Coverage B that includes "injury … arising out of … oral or written publication, in any manner, of material that violates a person's right of privacy" (and does not include an exclusion for access or disclosure of personal or confidential information) then, an insured would have to demonstrate, among other things, at least a potential that the data breach in issue constituted a "publication" that violated the data owner's "right of privacy." The standard ISO insurance form including this prong does not define the terms "publication" or "right of privacy." Courts ruling on the applicability of Coverage B to privacy claims have found some types of personal data, but not others, to be within the data owner's "right of privacy," and the result can vary depending on the information and the jurisdiction's law that applies, as well as the specific policy's provisions and exclusions. Thus, some courts have found privacy rights implicated for purposes of Coverage B where the issue was an insured's improper access and use of certain types of information that are statutorily protected, such as access and use of credit reports in violation of the Fair Credit Reporting Act (FCRA expressly states that it is intended to protect consumers' right to privacy).[602] Similarly, the personal data at issue in data breach scenarios is sometimes also protected by statutes designed to keep that data private. However, to the extent that the right to privacy is based on a statute, there are often other exclusions that serve to preclude coverage.[603] Moreover, to the extent that a claim is based on a common law or constitutional right to privacy, under some states' law, only information that is of an embarrassing nature and published under egregious circumstances is considered to be in violation of a right to privacy.[604]

Even apart from the content of the information involved, the application of a "publication" requirement under Coverage B presents a significant hurdle in data breach cases, particularly those

---

602 *See Pietras v. Sentry Ins. Co., No. 06 C 3576*, 2007 WL 715759, 2007 U.S. Dist. LEXIS 67013 (N.D. Ill. Mar. 6, 2007) (holding under Illinois law that the insurer had a duty to provide a defense); *American Family Mutual Ins. Co. v. C.M.A. Mortgage, Inc*., 2008 WL 906230 (S.D. Ind. Mar. 31, 2008) (holding under Indiana law that a claim involving improper use of credit reports in violation of FCRA states a potentially covered claim and thus triggers the insurer's duty to defend) (order rescinded in part due to docketing error, 2008 WL 5069825); *Zurich Am. Ins. Co. v. Fieldstone Mortgage Co*., No. 06-cv-2055, 2007 WL 3268460 (Md. Dist. Ct. Oct. 26, 2007) (holding under Maryland law that a FCRA claim based upon improper access and use of others' credit information triggered a duty to defend).

603 As mentioned below, to the extent statutes create a "right of privacy" in the type of Personal Information in issue, CGL policies typically also include an exclusion applicable to Coverage B for Violation of Information Law that may preclude coverage for claims based on violations of such statutes.

604 *See, e.g., Allstate Ins. Co. v. Ginsberg*, 863 So.2d 156 (Fl. 2003) (finding absence of personal injury coverage because underlying claims did not allege common law violation of privacy); *Lextron, Inc. v. Travelers Cas. and Sur. Co. of Am.*, 267 F. Supp. 2d 1041, 1047 (D. Colo. 2003) (looking to the Restatement (Second) of Torts for guidance); *A & B Ingredients, Inc. v. Hartford Fire Ins. Co.*, No. 08-6264, 2010 WL 5094419 (D.N.J. Dec. 8, 2010) (finding absence of personal and advertising injury coverage on the basis of a broad statutory exclusion and a finding that the jurisdiction in which the underlying claims arose apparently did not recognize common law privacy violations in that context); *Ananda Church of Self Realization v. Everest Nat. Ins. Co.*, No. C038570, 2003 WL 205144, 2003 Ca. App. Unpub. LEXIS 1095 (Cal. Ct. App. Jan. 31, 2003) (unpublished) (finding absence of Coverage B coverage, in part, on the basis that the type of information at issue, while confidential, were not facts that "the average person would find offensive or objectionable"); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121 (N.D. Cal. 2008), *aff'd*, 380 Fed. Appx. 689 (9th Cir. 2010) (holding that the employer's possible negligence (*i.e.*, in allowing the computers containing unencrypted personal information of job applicants to be stolen) did *not* rise to the level of egregiousness required). *See also State Farm Fire and Cas. Co. v. Nat'l Research Center for Coll. and Univ. Admissions*, 445 F.3d 1100, 1103 (8th Cir. 2006) (deciding under Missouri law and defining "privacy" as "isolation, seclusion, or freedom from unauthorized oversight or observation.")

involving theft of information by a third party from the breached insured. Decisions in some jurisdictions have found there to be sufficient issue of publication under some fact situations that involve violations of privacy rights to at least trigger a duty to defend in situations that, among other things, have involved insured's alleged distribution of the Personal Information in issue; however, others have held there to be no coverage as a matter of law in instances where there is no publication by an insured. Thus, in one well publicized coverage case arising out of the Sony PlayStation breach, a court found that the "publication" must be by an insured and publication by a third party hacker does not fall within the scope of "publication" under Coverage B. [605]

In Fair Credit Reporting Act cases several courts took the view that "publication" can occur when information is revealed by the insured to others, including the owner of the information.[606] One court, relying on a dictionary, found "publication" to mean "to produce or release for distribution."[607] In contrast, courts in other jurisdictions analyzing the application of Coverage B to

---

[605] One of the most publicized cases on the issue of whether there is coverage under a CGL policy for a data breach is the coverage litigation arising out of the 2011 Sony PlayStation data breach. Hackers stole the PII of PlayStation users, and the users in turn filed approximately 60 lawsuits against Sony, including consumer class actions. Sony sought coverage under its Coverage B of its tower of CGL policies, and there was a resulting a declaratory judgment action to determine the CGL insurers' coverage obligations. On February 21, 2014, Judge Oing of the New York State Supreme Court, New York County, ruled that the CGL insurers did not have a duty to defend Sony Corporation in lawsuits relating to the data breach. The court found that coverage under the prong of "personal and advertising injury" coverage for publication in violation of a right to privacy requires that the insured "commits or perpetrates the act of publicizing the information" and in the data breach in issue it was the Sony, who published the Personal Information in issue. *Zurich Am. Ins. Co. v. Sony Corp. of Am., et al.*, Index No. 651982/2011 (Supreme Court of the State of New York, County of New York, Feb. 21, 2014). On April 9th, 2014, Sony filed an appeal of Judge Oing's decision.

Another recent decision supporting this view is *Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co.*, No. X07CV095031734S, 2012 WL 469988, at *6-7 (Conn. Super. Ct. Jan. 17, 2012), *aff'd* 147 Conn. App. 450, 83 A.3d 664 (Conn. App. Ct. 2014) (130 computer data tapes, containing personal information for more than 500,000 employees of the insured, fell from the back of a transport truck and were then removed by an unknown person and never recovered; the court found "publication" for purposes of Coverage B did not occur because there was "no evidence of *communication* to a third party," finding "the loss and the subsequent theft of the tapes . . . is not the offense, publication . . . that the policy contemplates to trigger personal injury coverage.") (emphasis added); *Butts v. Royal Vendors, Inc.*, 202 W.Va. 448, 504 S.E.2d 911 (W. Va. 1998) (per curiam) (employee filed civil action against his employer for wrongful inducement after the employee's physician made certain statements in alleged breach of the patient's privacy; employer then sought coverage under its CGL policy that provided coverage for "oral or written publication of material that violates a person's right of privacy"; court found that no coverage existed under this section of the policy because there was no allegation that the insured affirmatively disseminated any statements in violation of the employee's privacy; rather, the complaint alleged that the employer "induced" a third party – *i.e.*, the employee's treating physician – to do so; the court specifically stated that the Coverage B publication offense was "not written to cover publication by a third party"); *see also Harrow Prods., Inc. v. Liberty Mut. Ins. Co.*, 64 F.3d 1015, 1025 (6th Cir. 1995) (stating that "each enumerated tort in the personal injury clause requires an intentional act" under a policy that included coverage for "publication . . . in violation of an individual's right of privacy"); *Gregory v. Tennessee Gas Pipeline Co.*, 948 F.2d 203, 209 (5th Cir. 1991) (stating that "[e]ach of the enumerated risks specifically assumed requires active, intentional conduct by the insured" in relation to a policy that included coverage for "oral or written publication of material that violates a person's right of privacy"); *Buell Indus., Inc. v. Greater New York Mut. Ins. Co.*, 259 Conn. 527, 562, 791 A.2d 489, 510-11 (Conn. 2002) (stating that a policy's "personal injury provisions were intended to reach only intentional acts by the insured" in relation to a policy that included coverage for "a publication . . . in violation of an individual's right of privacy"); *Cnty. of Columbia v. Cont'l Ins. Co.*, 83 N.Y.2d 618, 634 N.E.2d 946 (N.Y. 1994) (stating that "the coverage under the personal injury endorsement provision in question was intended to reach only purposeful acts undertaken by the insured or its agents" under a personal injury endorsement that provided coverage for "publication" that constituted an invasion of an individual's right of privacy").

[606] *See Zurich v. Fieldstone, supra,* 2007 WL 3268460 at *5; *see also, e.g. Pietras v. Sentry Ins. Co.*, No. 06 C 35762007 WL 715759 (N.D. Ill. Mar. 6, 2007) (holding that violation of a law prohibiting unsolicited pre-approved loan advertising mailings violated the claimants right to have one's private information maintained as private and that "publication" under Illinois law included communication to as few as a single person).

[607] *Id. See also LensCrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, No. C-04-1001, 2005 WL 146896 (N.D. Cal. Jan. 20, 2005) (involving alleged disclosure of private medical information); *Moore v. Hudson Ins. Co.*, No. B189810, 2007 WL 172119, at *6 (Cal. Ct. App. Jan. 24, 2007) (unpublished) (discussing scope of dissemination required).

a violation of FACTA reached a different conclusion with regard to "publication" on the grounds that it is not publication where credit card information is improperly printed in full, but is provided only to the cardholder and thus not "in any way made generally known, announced publicly, disseminated to the public, or released for distribution."[608] However, in a case construing "publication" in the context of an employer subjecting his employee to audio surveillance without informing the employee in violation of the Wiretapping and Electronic Surveillance Act, that surveillance was found to constitute "publication."[609]

Overall, the limited case law and legal authorities on the issue indicate that "publication" within the context of Coverage B requires that the insured have affirmatively disseminated the information in issue to others, rather than have that information stolen from it, for there to be any potential for the "publication" prong of Coverage B to apply. Thus, while the term "publication" has been found satisfied in the Coverage B context in instances involving affirmative acts by the insured, so far there is a dearth of authority indicating that the term "publication" may be satisfied on the basis of passive, non-affirmative conduct by the insured in the data breach context. As a result, an entity seeking coverage under Coverage B for a typical data breach involving third party theft of information is likely have an uphill battle triggering coverage obligations under Coverage B, as a data breach does not generally involve any affirmative acts of dissemination on the part of the insured, although that is an issue being litigated.[610]

Thus, in the event of a request for coverage under Coverage B of a third-party claim based upon improper access to Personal Information due to a data breach, the focus is likely to be whether there was a violation of the data owner's "right of privacy," whether there was "publication" by the insured, whether covered "damages" are sought, and which jurisdiction's law applies.

Variations in Coverage B policy wording can also affect whether a court is likely to find coverage for a data breach under Coverage B. In a case involving claims brought under the Electronic

---

608 *Whole Enchilada, Inc. v. Travelers*, 581 F. Supp. 2d 677, 698 (W. Dist. Pa. 2008); *see also Ticknor v. Rouse's Enters., LLC*, 2014 WL 668930 (E.D. La. Feb. 20, 2014) (finding grocery store operator's alleged failure to truncate expiration dates when issuing receipts for credit card transactions in violation of FACTA did not amount to a "publication" within the meaning of the store's CGL's personal and advertising injury coverage provision because the store's actions did not involve mass distribution of material to the general public or an intrusion into an individual's right to be left alone as receipts were provided only to customers who initiated credit card transactions); *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, No. 08-cv-22302 (S.D. Fla. Mar. 23, 2011) (restaurant printed more than five digits of customers' credit card numbers on printed receipts, along with expiration dates, in alleged violation of FACTA; court found no "publication" for purposes of Coverage B had occurred because the underlying complaint lacked allegations of any "dissemination of information to the public," or even any "allegation that any FACTA-violation receipt was provided to anyone other than the cardholder"), *aff'd*, 444 Fed. Appx. 370, 376 (9th Cir. 2011) ("In sum, providing a customer a contemporaneous record of a retail transaction involves no dissemination of information to the general public and does not constitute publication within the meaning of Essex's Policy").

609 *Bowyer v. Hi-Lad Inc.*, 609 S.E.2d 895, 912 (W.Va. 2004) (insured argued that the term "publication" was ambiguous and should be construed against the insurer to cover an employee's underlying claim that the insured "used the surveillance system to capture his oral communications, and then publish that audio material through speakers to the officers and employees" of the insured's business; the court held that there was "nothing in the policy indicating that the word publication necessarily means transmitting the intercepted communications to a third party, as is required of material in the defamation context. And, even were we to assume publication does require communicating to a third-party, the surveillance monitoring system apparently functioned in such a way that anyone in the manager's office or in [the hotel owner's] home had the ability to listen in on employee conversations").

610 Currently pending are several lawsuits concerning requests by policyholders for coverage, or at least a defense, under Coverage B for claims arising from breach-related events. *See, e.g.*, *Nationwide Mut. Fire Ins. Co.* v. *First Citizens Bank and Trust Co., Inc.*, No. 4:13-cv-00598 (filed Mar. 6, 2013 in South Carolina federal court). *See also* case discussions in the section below about Privacy Litigation.

Communications Privacy Act and Computer Fraud and Abuse Act in connection with the collection of information regarding the underlying plaintiffs' online activity for eventual dissemination to third-party advertisers, one court construed a policy that had Coverage B wording different from the wording found in the ISO form. That policy defined "personal injury offense" to include "Making known to any person or organization written or spoken material that violates a person's right to privacy." This took the place of the phrase "oral or written publication, in any manner" found in the ISO form.[611] Under that non-ISO definition, the court found the defendant's passage of information to its parent company and the defendant's employees sharing of the information among themselves to constitute "making known to any person or organization." (The holding was reversed on appeal but not on this point.)[612]

Further hurdles faced by insureds seeking coverage under a CGL policy for claims arising from a data breach, even if they overcome the significant thresholds to coverage contained in the Coverage B insuring provisions, include that there are typically a number of policy exclusions applicable to Coverage B that can operate to exclude coverage. For example, even apart from the new exclusions introduced in 2013 and 2014 discussed above, the standard ISO form contains an exclusion for "personal injury and advertising injury" arising out of violation of any "statute, ordinance or regulation . . . that addresses, prohibits or limits the . . . sending, transmitting, communicating or distribution of material or information."[613] Further, even if a Coverage B statutory violation exclusion does not include in its provisions that "alleged" violations are also precluded from coverage, at least two district courts in the TCPA context have found that allegations alone in the underlying complaint of such violations may be sufficient for coverage to be excluded (as opposed

---

[611] Some courts have distinguished between the terms "publication" and "making known" for purposes of Coverage B coverage. *Compare Motorists Mut. Ins. Co. v. Dandy-Jim, Inc.*, 182 Ohio App. 3d 311, 319, 912 N.E.2d 659, 655 (Ohio App. Ct. 2009) (*distinguishing* "publication" from "making known" for Coverage B purposes), *and Zurich Am. Ins. Co. v. Fieldstone Mortg. Co.*, No. CCB-06-2055, 2007 WL 3268460, at *5 (D. Md. Oct. 26, 2007) (same), *with State Farm Gen. Ins. Co. v. JT's Frames, Inc.*, 181 Cal. App. 4th 429, 104 Cal. Rptr. 3d 573 (Cal. Ct. App. 2010) (equating the term "publication" to "making known to any person or organization" for Coverage B purposes).

[612] *Netscape Commc'ns. Corp. v. Fed. Ins. Co.*, No. 06-C-00198, 2007 WL 2972924 (N.D. Cal.), *rev'd, Netscape Commc'ns Corp. v. Fed. Ins. Co.*, 343 Fed. Appx. 271 (9th Cir. 2009). The Ninth Circuit found the policy's language regarding "any person or organization" to be dispositive. However, the Ninth Circuit disagreed with the lower court regarding the applicability of an exclusion to Coverage B. The policy excluded coverage for personal injury offenses relating to defined "online activities," including the provision of Internet access. While the lower court found that the exclusion barred coverage because the claims involved the use of software to assist with downloading files, the Ninth Circuit, reading the exclusion narrowly, reasoned that the software itself does not provide Internet access, and thus the exclusion did not apply.

[613] This exclusion was slightly modified and expanded in ISO's latest 2013 filing, and now, among other things, lists not only the TCPA, CAN-SPAN Act of 2003, but also the Fair Credit Reporting Act. A variation of this exclusion was construed in *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 655 F. Supp. 2d 1316 (S.D. Fla. 2009) (Rosenbaum, U.S.M.J.), *adopted in part, ruling reserved in part*, 655 F. Supp. 2d 1316 (S.D. Fla. 2009). There certain underlying claims alleging FACTA credit card violations against a restaurant were excluded from personal and advertising injury coverage under the policy's "Distribution Of Material In Violation of Statutes" exclusion (that exclusion excluded coverage for personal and advertising injury "arising directly or indirectly out of any action or omission that violates or is alleged to violate . . .[a]ny statute, ordinance or regulation . . . that prohibits or limits the sending, transmitting, communicating or distribution of material or information"). It was held that because FACTA is a "statute that limits the information that . . . an electronically printed receipt . . . may include . . . FACTA qualifies as a statute that 'prohibits and limits the ... communicating or distribution of material or information,' within the ordinary meaning of the terms of this exclusion." It should be noted that the Court of Appeals for the Eleventh Circuit issued a related decision (as to another restaurant), and held that a restaurant's issuance of a credit card receipt to a customer does *not* constitute "publication" within the meaning of the clause "publication . . . of material that violates a person's right of privacy." *See Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, No. 11-11781, 2011 WL 4509919 (11th Cir. Sept. 30, 2011). The court reasoned that such a transaction involves "no dissemination of information to the general public." *Id.* at *5. As a result, the Ninth Circuit did not need to reach whether any exclusion was applicable because coverage was not triggered due to the absence of any "publication" by the insured.

to requiring an adjudication or admission of such violation for the exclusion to trigger).[614] Other Coverage B exclusions that can potentially come into play upon a data breach include ones for "personal and advertising injury" arising out of the criminal act of the insured (which could come into play when employee theft is in issue); arising out of intellectual property rights; committed by insureds in media and Internet type businesses; arising out of an electronic chat room or bulletin board the insured hosts, owns or controls; arising out of breach of contract; and other exclusions that may be more general in nature but apply to the specific claim in issue, or that may be specifically manuscripted for the insured in issue.

(3) The "Damages" Hurdle

Yet another hurdle for attempts to obtain coverage of a third-party data breach claim under a CGL Policy is the requirement under both Coverage A and Coverage B that the claim be for "sums that the insured is legally obligated to pay as damages." As discussed above, often consumers have not sustained out-of-pocket losses, and issues include whether there are any covered damages to which the insurance applies even if there is found to be a covered occurrence or offense, if only statutory fines or penalties are involved. As "damages" is not generally a defined term in CGL policies, the issue of what constitutes covered damages can be a contested issue that can differ based on the law of the applicable jurisdiction.

The issue of "damages" is often raised in other types of privacy related cases than those arising from traditional data breaches, particularly those involving statutory violations and monetary assessments, such as the "ZIP code litigations" (putative class action lawsuits where customers allege that retailers improperly and unnecessarily recorded customers' ZIP codes during credit card transactions in violation of applicable state statutes)[615], or in cases alleging violations of statutes such as the TCPA (Telephone Consumer Protection Act)[616] for which coverage is sought under

---

614 *See Collective Brands, Inc. v. Nat'l. Union Fire Ins. Co. of Pittsburgh, P.A.*, No. 11-4097-JTM, 2013 WL 66071 (D. Kan. Jan. 4, 2013) (finding that nothing in the exclusion required a formal adjudication and that it was sufficient if the liability arose from excluded statutory violations for the exclusion to apply); *see also Interline Brands, Inc. v. Chartis Specialty Ins. Co.*, No. 3:11-cv-731-J-25JRK (M.D. Fla. Nov. 21, 2012) ("The Court cannot find legal precedence to rewrite the insurance contract to necessitate there being an 'adjudged violation' for the exclusion to apply"). *Interline Brands, Inc.* is currently on appeal in the Court of Appeals for the Eleventh Circuit, and oral argument was held during the first week of March, 2014.

615 See Section II.1.a. above, on the Expanding Definitions of Personal Information, and Section VII.4.a below, discussing the ZIP code litigation in California and Massachusetts under those states respective laws

For example, Michaels Stores, Inc. was faced with such ZIP Code claims in California. Various customers filed six putative class actions against the retailer, and ultimately the only remaining claim was a violation of the California Song-Beverly Act. Michaels sought coverage under its CGL policy, and coverage litigation ensued. *See Arch Ins. Co. v. Michaels Stores, Inc.*, 37-2011-00097053-CU-IC-CTL (Cal. Super. Ct., San Diego County). The parties each cross-moved for summary judgment regarding the CGL insurer's duty to defend and indemnify. The court ultimately granted summary judgment in favor of the insurer, holding that the underlying lawsuits did not seek "damages" within the meaning of the CGL policy. As the policy did not define "damages," the court applied the "common" definition; "damages" are "compensation recovered by a party for a loss or detriment it has suffered through the acts of another." The court disagreed that the Song-Beverly Act's statutory penalties were compensatory in nature, and found such damages were penalties designed to "deter misconduct and harm". Since such penalties did not fall under the definition of "damages" used by the court, it held that there was no coverage under the CGL policy. *See Arch Ins. Co. v. Michaels Stores, Inc.*, 37-2011-00097053-CU-IC-CTL (Cal. Super. Ct., San Diego County, Dec. 20, 2013).

616 See discussion of TCPA above in Section III.2. j, discussing the U.S. Regulatory and Statutory Landscape, and Section VII.4.f, on Privacy Practices Lawsuits.

Some courts have held that TCPA damage of $500 per violation constitute penal or punitive damages, see, e.g., *U.S. Fax Law Center, Inc. v. iHire, Inc.*, 362 F. Supp. 2d 1248, 1253 (D. Colo. 2005), *aff'd*, 476 F. 3d 1112 (10th Cir. 2007); *Kruse v. McKenna*, 178 P. 3d 1198, 1201 (Colo. 2008) (*en banc*); *Kaplan v. Democrat & Chronicle*, 266 A.D. 2d 848, 698 N.Y.S. 2d799, 800

policies that do not have a TCPA exclusion. Requests for coverage of statutory assessments are often met with resistance by insurers who consider them to be tantamount to civil penalties, and the battle ground generally turns on whether the under the particular statute in issue the sums required to be paid under the statute for violations are punitive or penalties and thus uninsurable under the applicable jurisdiction' law, or remedial and compensatory and thus insurable "damages."

v. Professional Liability/E&O

Most professionals and entities engaged in providing services to others have errors and omissions (E&O) liability policies in place that they look to for a defense and indemnity when a claim is asserted against them by their clients. When a data breach at least arguably occurs within the scope of covered services, particularly when it involves data of its client, such an insured may look to its professional liability/E&O insurer to at least provide a defense to any third-party claims arising from the data breach. Thus, for example, a law firm, engineering firm or technology services firm that improperly disposes of or loses client files or is otherwise subject to a data breach – or a firm that is involved in issues relating to planning, designing or implementing a client's software program that is involved in a breach – and is thus subject to client claims, may try to seek coverage under its professional liability/E&O policies.

Professional liability and other E&O policies, however, may contain electronic data or software design exclusions, although some may have exceptions for such services that are incidental to the "professional services" covered and thus trigger a duty to defend some data breach claims asserted against an insured that arguably fall within the exception. On the other hand, in recent years, many professional liability policies include (or have as an option to be purchased) add-on coverage by way of endorsements or additional coverage parts that are directed at providing data breach or other cyber risk coverage, including the first party costs sustained by the insured in responding to a breach.

Some E&O policies are expressly designed to provide coverage for cyber risk claims. For example, many E&O policies issued to technology companies recognize that such insureds are engaged in activities likely to make them more prone than companies in other industries to involvement in electronic data breaches, either as direct targets or as vendors to others. Thus, policies available to such technology companies may also expressly include coverages encompassing data breach claims. Cyber risks are also increasing professional liability and other errors and omissions exposures in ways, particularly for insurance brokers and for entities involved in providing network

---

(App. Div. 1999) (mem). Other courts have disagreed, some reasoning that the cost of an unsolicited fax (loss of paper and ink, annoyance and inconvenience) is still a cost and thus a compensable harm, represented by the liquidated sum of $500 per violation, and is an incentive for private enforcement rather than punitive. *Standard Mut. Ins. Co. v. Lav*, 989 N.E. 2d 591 (Ill. 2013).

TCPA claims raise other coverage issues as well, many of which are different than those arising from data breach claims. One issue is whether the conduct in issue, such as sending faxes, is intentional with knowledge it would result I the sue of recipient's paper, toner and time, and thus is intentional and not an "occurrence" under Coverage A. *See, e.g., Nationwide Mut. Ins. Co. v. David Randall Assocs., Inc.*, 551 Fed. Appx. 638, 640 (3rd Cir. 2014); *Melrose Hotel Co. v. St. Paul Fire & Marine Ins. Co.*, 432 F. Supp. 2d 488, 507-09 (2006), *aff'd sub nom. Subclass 2 of the Master Class of Plaintiffs Defined & Certified in the January 30, 2006 and July 28, 2006 Orders of the Circuit Court of Cook County, Illinois in the Litigation Captioned Travel 100 Group Inc. v. Melrose Hotel Co.*, 503 F.3d 339, 340 (3rd Cir. 2007); see also *G. M. Sign. Inc*, 2014 IL App (2d) 121276 (Mar. 24, 2104). Courts have also considered whether TCPA claims fall under Coverage B provisions for publications in violation of a right to privacy. *See, e.g., Owners Ins.Co. v. European Auto Works, Inc.*, 695 F. 3d 814 (8th Cir. 2012) and case law cited therein.

security or other network services: there will likely be an increasing number of claims to be addressed that professionals failed to adequately advise their clients about cyber risks. As cyber risks become increasingly known as a significant risk to businesses that can result in substantial costs and claims, entities sustaining a costly cyber attack or other privacy-related claim will be looking for others to share those costs with it. If insurance for the types of costs and losses was available in the market, but not discussed with an entity as a potential part of its insurance program, that may make the entity's broker a target. When a vendor is involved, that entity and its indemnity agreements and insurance will also be scrutinized as a source of recovery. Thus, regardless of the applicability of policy limitations and exclusions of coverage, companies in the insurance industry will have the increased cost of dealing with a growing frequency of claims to address.

Often the coverage issues include whether the claim is within the scope of covered services, whether the insured's error that caused the alleged damage or financial injury in question falls under policy's definition of "wrongful act," whether there are alleged to be "damages" covered by the policy, whether contractual liability exclusions apply to indemnity claims, and whether there is an exclusion directed at data breach or other electronic claims.[617]

vi. D&O

As large publicized data breaches and other cyber incidents involving publicly traded companies often result in drops in companies' stock prices or other large financial losses, companies and their directors and officers who are faced with such a data breach or other type of cyber attack or incident may well also face the type of securities/D&O claims that frequently accompany a significant and unexpected fall in stock prices and allegations of failure to disclose a material risk. For example, following the Heartland data breach, shareholders pursued securities fraud litigation against Heartland on the basis that it had misrepresented the state of its computer security. While the suit was ultimately dismissed, it shows the potential for shareholder litigation against companies that are victims of data breaches.[618] The Target breach reported in December 2013 has also been the basis

---

[617] For example, the "wrongful act" coverage requirement has been found (under some states' law) to include "intentional, non-negligent acts but to exclude intentionally wrongful conduct." *See Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 804 (8th Cir. 2010) (under Minnesota law). In *Eyeblaster, Inc.*, a computer user sued Eyeblaster, Inc., alleging that Eyeblaster injured his computer, software, and data after he visited an Eyeblaster website. The E&O policy at issue obligated Eyeblaster's insurer "to pay loss for financial injury caused by a *wrongful act* that results in the failure of Eyeblaster's product to perform its intended function or to serve its intended purposes." The insurer conceded that the underlying claim sufficiently alleged "financial injury." Nonetheless, the insurer argued (and the district court agreed) that coverage was non-existent because Eyeblaster had acted intentionally, and thus no "wrongful act" within the meaning of the policy had occurred ("wrongful act" was defined under the policy as "an error, an unintentional omission, or a negligent act"). On appeal, the Court of Appeals for the Eight Circuit reversed, finding that although Eyeblaster had acted intentionally in placing its software in the underlying complainant's computer, there was "no evidence that the allegations . . . spoke of intentional acts that were either negligent or wrongful." Thus, the court found that the underlying complaint had sufficiently alleged a "wrongful act" on the part of Eyeblaster within the meaning of the policy, and consequently found a duty to defend had been triggered.

[618] *In re Heartland Payment Sys., Inc. Sec. Litig.*, Civ. No. 09-1043 (D.N.J. Dec. 7, 2009). The court found that the securities fraud claims failed to meet the heightened pleading standards provided by the Private Securities Litigation Reform Act of 1995 (PSLRA). The court explained that the PSLRA requires fraud to be pleaded with particularity, and also requires plaintiffs to state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind. Citing the Supreme Court's decision in *Tellabs, Inc. v. Makor Issues & Rights Ltd.*, 551 U.S. 308 (2007), the court explained that a complaint will adequately allege state of mind only if a reasonable person would deem the inference of scienter to be at least as strong as any inference of non-fraudulent intent. The court found that the plaintiffs had failed to meet this heightened pleading requirement. In particular, the court found that the defendant's statements regarding its computer security, when examined in context, were not misleading. The court also found that the plaintiffs had failed to allege that the defendant knew or should have known that its

for D&O lawsuits[619], as has the breaches involving Wyndham Hotels, which has been engaged in a hotly contested dispute with the FTC arising out of data breaches sustained by Wyndham. [620] These all demonstrate that such companies, and their D&O insurers, may face D&O and securities claims among the potential litigations that can arise, particularly if the cyber attack in issue results in substantial costs to the company..[621]

Further, with the increasing issuance by state and federal agencies of data security regulations requiring the institution of data security protocols by companies, some of which expressly require board review of data protection plans and procedures, there may be an increase in D&O claims for all types of companies within their purview. For example, in addition to the accountability placed on boards by the Sarbanes-Oxley Act of 2002, the federal Red Flags Rule discussed above specifically requires that the board of directors, a board committee, or a designated employee at the level of senior management be involved in the oversight, development and administration of the required identity theft prevention program. In addition, as discussed above, in October 2011, the SEC Division of Corporation Finance released a Disclosure Guidance stating that public companies may need to disclose their exposure to cyber security risks and incidents as potential material information subject to securities law disclosure requirements and accounting standards.[622] This also potentially provides grounds for claims alleging inadequate disclosure against directors and officers as well as public entities.

If a data breach leads to a suit by the owners of the compromised data – or by shareholders if the breach leads to a large loss to the insured company – against the allegedly responsible directors or officers, those directors and officers may look to their D&O policies to see if there is coverage

---

statements were false. Having found that the complaint failed to adequately allege two of the elements of its fraud claims, the court dismissed the complaint with prejudice.

619 See, *e.g.*, *Robert Kulla, Derivatively on behalf of Target Corporation v. Gregg W. Steinhafel et al.*, Case 0:14-cv-00203-SRN-JSM (United States District Court, District of Minnesota), filed January 21, 2014 (a shareholder derivative action against certain Target officers and directors alleging they were responsible for the data breach sustained by Target because of, among other things, alleged failure to take reasonable steps to maintain customer personal and financial information is a secure manner, and failure to provide adequate and prompt notice to consumers); *Maureen Collier, Derivatively and on behalf of Target Corporation v. Target Corporation* (United States District Court, District of Minnesota (a shareholder derivative action, alleging false and misleading statement about the data breach).

620 See *Dennis Palkon, Derivatively on Behalf of Wyndham World Wide Corporation v. Stephen P. Holmes, et al.*, Case 2:14-cv-01234-SRC-CLW (United States District Court, District of New Jersey, Filed May 2, 2014 (a derivative shareholder lawsuit alleging the individual defendant directors and officers aggravated damage to the company form data breaches by, among other things, failing to timely disclose the breaches in the company's financial filings, and failing to implement appropriate controls to detect and prevent repetitive data breaches).

621 However, in the current era of frequent news stories of data breaches, a report of even a large breach does not necessarily result in a drop in stock prices, at least not until there are reports of substantial costs to the company that arguably affect earnings, and often an initial drop is followed by a quick recovery. See Eric Chemi, *Investors don't care if a firm's data are breached,* San Francisco Chronicle, May 26, 2014, available at http://cyberfpn.advisen.com/articles/article218752948-152834721.html?user= (discussing statements from industry analysts noting that Target's stock reportedly did not initially fall substantially, until the company cut its earnings forecast, which may have been for reasons that included causes unrelated to their 2013 data breach, and noting only small drops following other reported large breaches by, among others, JPMorgan Chase and Adobe Systems).

622 For more information regarding the recently released Disclosure Guidance, *see Edwards Wildman Palmer LLP Client Advisory*, "*Public Companies May Need to Disclose their Exposure to Material Cyber Security Risks According to New Guidance Issued by SEC Division of Corporation Finance*," Oct. 2011, http://www.edwardswildman.com/newsstand/ detail.aspx?news=2634. See also section above on U.S. Regulatory and Statutory Landscape.

(mindful, of course, of any exclusions that may apply).[623] Similarly, in the event of a securities action, the targeted company will likely look to any entity coverage provided by such policies.

An indication of some of the coverage issues that can arise is demonstrated by coverage litigation arising from the request for coverage by a drug testing company that faced substantial defense cost arising from a federal HIPAA investigation, and sought overage for its defense cost under its D&O policy. Reportedly, a primary issue was whether the defense costs for a Department of Justice investigation were subject to a regulatory sublimit, or entitled to the full policy limits for third party claims.[624]

vii. Kidnap and Ransom/Cyber Extortion

Corporations and individuals operating in high-risk areas around the world often carry kidnap and ransom coverage. The policies typically provide indemnity in connection with ransom payments and personal accident losses caused by kidnapping incidents. Such policies may also cover extortion, including extortion related to a threatened introduction or activation of a computer virus to the insured's computer system unless a ransom is paid. Depending on the policy's scope of coverage, including how the policy defines "virus," such coverage may extend to a hacker's threatened use of software to capture private data.

With the increase in threats of cyber extortion in recent years, policies specifically directed at cyber extortion are now available and often offered in conjunction with specialty policy products directed at providing coverage for network security and related risks.

VII. Privacy Litigation in the U.S.: Current Issues

In the last few years there has been a dramatic increase in litigation alleging violations of data protection, breach response and other statutory and common law rights and obligations concerning the collection, usage, disclosure and protection of information about individuals. Most of the court decisions to date focus on whether plaintiffs can survive early motions to dismiss, and satisfy threshold issues such as standing and demonstrating a legally cognizable injury under applicable law, with mixed results (and significant legal expenses incurred by parties on both sides of the issues).

---

623 As to exclusions, it is possible, for instance, that the D&O policy at issue may exclude claims arising from violations of privacy rights, thus potentially limiting the scope of available coverage in the event of a data breach. *See, e.g., Resource Bank v. Progressive Cas. Ins. Co.*, 503 F. Supp. 2d 789, 795-97 (E.D. Va. 2007) (insured sought coverage under its D&O policy for two class action lawsuits alleging that the insured violated the Telephone Consumer Protection Act by sending unsolicited facsimile advertisements; court held coverage was excluded, in part, on the basis of the policy's Bodily Injury and Property Damage Exclusion that excluded coverage for claims of "invasion of privacy").

624 *Millennium Laboratories Inc. v. Allied World Assurance Company (U.S.) Inc.,* case no. 3:12-cv-02280 (United States District Court for the Southern District of California); see also *Millennium Laboratories, Inc. v. Allied World Assurance Company*, case no. 1:2014mc00009 (United States District Court for the Eastern District of California). . See Linda Chiem, *Millenium Says Insurer Must Cover HIPAA Probe Defense*, http://www.law360.com/articles/541526/print?section+pivacy.

1. Article III Standing

Consumer lawsuits x are typically pleaded as class actions and are therefore initiated in, or removed to, federal court pursuant to the Class Action Fairness Act.[625] Once in federal court, the lawsuit must comply with the requirement of Article III of the Constitution that there be an actual "case or controversy" between the parties. Among the requirements for a "case or controversy" is that the plaintiff has suffered an injury in fact that is actual or imminent, not conjectural or hypothetical.[626] In the absence of such an injury, the case is subject to dismissal based on a lack of standing.

Consumer claims based on the exposure of Personal Information have met mixed success at clearing the federal standing hurdle, and the number of decisions addressing the issue is growing yearly. Some lower courts have dismissed consumer claims for a lack of standing, finding the alleged injury to be indefinite and speculative, although frequently allowing repleading by plaintiffs to provide them with an opportunity to try to cure defects in pleading if they have a basis for doing so.[627] A few courts have found standing in some consumer lawsuits at least at the early stage of motions to dismiss complaints, but often actions which survive then don't survive later post-discovery motions for summary judgment..[628]

---

625 28 U.S.C. § 1332(d). The Class Action Fairness Act ("CAFA") grants federal courts jurisdiction over class action lawsuits even in the absence of complete diversity between the parties, if certain other conditions are met. On June 28, 2012, the Tenth Circuit ruled that defendants are entitled to estimate their own damages. *Frederick v. Hartford Underwriters Ins. Co.*, No. 12-1161, 2012 WL 2443100 (10th Cir. June 28, 2012). Moreover, the U.S. Supreme Court recently held that a named plaintiff in a putative class action who stipulates, prior to certification of the class, that the class will not seek damages that exceed the $5 million amount in controversy requirements of CAFA does not prevent removal under CAFA. *Standard Fire Ins. Co. v. Knowles*, 133 S. Ct. 1345 (2013).

626 *See, e.g., Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 180-81 (2000) (*citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (plaintiff must establish an injury-in-fact that is "concrete and particularized")).

627 *See, e.g. In Re Google Android Consumer Privacy Litigation*, 2013 WL 1283236 (N.D. Cal. Mach 26, 2013) holding allegations were insufficient, but allowing plaintiffs to amend their complaint, which survived a motion to dismiss at least as to some claims, 2014 WL 988889 (N.D. Cal. March 10, 2014) (granting in part and denying in part Google's motion to dismiss the Second Amended Class Action Complaint, finding sufficient facts alleged to show standing based on diminished battery life and fraudulent misrepresentations under California Unfair Competition Law); see also *Low v. LinkedIn Corp.*, No. 11-CV-01468, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011) (holding that plaintiff in class action claiming that LinkedIn disclosed Personal Information to third parties and marketing companies alleged harm that was too abstract and hypothetical to support Article III standing); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006); *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp.2d 1 (D.D.C. 2007), *aff'd*, 973 A.2d 702, 708 (D.C. Cir. 2009); *Giordano v. Wachovia Sec. LLC*, No. 06-476, 2006 WL 2177036, 2006 U.S. Dist. LEXIS 52266 (D.N.J. Jul. 31, 2006); *Bell v. Acxiom*, No. 06-485, 2006 WL 2850042, 2006 U.S. Dist. LEXIS 72477 (E.D. Ark., Oct. 3, 2006).

628 *See, e.g., Claridge v. RockYou*, 785 F. Supp. 2d 855 (N.D. Cal. 2011) (declining to dismiss, for lack of standing, plaintiffs' claim that they traded email and social media login credentials for access to applications, and that they lost the value of those credentials when the data was stolen by a hacker). The court found case law regarding this "novel theory of damages" to be too scarce to dismiss on standing grounds, but left open a future standing challenge following discovery. *Id.* at 861. Further, initially *In re iPhone Application Litig.*, the court found that plaintiffs sufficiently alleged injury in fact wherein plaintiffs experienced and encountered diminished storage and battery life, unexpected and unreasonable risk to the security of sensitive personal information, and detrimental reliance on Apple's representations regarding privacy protection afforded to users of iDevice apps., No. 11-MD-02250, 2012 WL 2126351, 844 F.Supp.2d 1040 (N.D. Cal. Jun. 12, 2012) (the court found it compelling that plaintiffs identified specific types of personal information collected, such as home and workplace locations, gender, and age when determining sufficient harm.). However, in a subsequent decision on summary judgment, the court found that the plaintiffs had failed to establish material issues of material fact concerning their standing under Article III, including with regard to the claims of violation of the California Unfair Competition Law and the California Consumers Legal Remedies Act, and granted Apple summary judgment. 2013 WL 6212591 (N.D. Cal. Nov. 25, 2013).

Some federal appellate courts have found the standing requirement to be satisfied by allegations of an increased risk of future harm in the context of breaches of Personal Information.[629] Other federal appellate courts, however, have found that the "risk of future harm" presented by data breaches involving exposure of Personal Information is too speculative, and have held that persons whose information "may" have been accessed does not have standing, particularly in the absence of evidence suggesting that the data has been, or will ever be, misused.[630]

The 2013 United States Supreme Court decision in *Clapper v. Amnesty International USA*[631] has already become a basis for motions to dismiss plaintiffs' complaints in the privacy and data breach context, and is likely to continue to be party of the battle cry against plaintiffs attempting to establish claims arising from data breach and other consumer privacy claims. The *Clapper* Court rejected a challenge to the constitutionality of a federal electronic surveillance statute, and held that fears of government interception of electronic communications were simply too speculative to confer legal standing on a plaintiffs' group to bring suit. According to the court, standing exists only where an injury is "concrete, particularized, and actual or imminent." The court noted that "our standing inquiry has been especially rigorous" when the challenge is an action of another branch of the federal government, and did note that in other instances it has found standing based on a "substantial risk" that harm will occur which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.[632] Nevertheless, if the standing principles discussed in *Clapper* are applied to privacy and data breach cases, the absence of concrete harm in those circumstances may very well become a significant obstacle for plaintiffs bringing suit for such claims – at least until

---

629 *See Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (finding that plaintiffs had pleaded a "credible threat" of "real and immediate harm" stemming from the theft of a laptop containing their Personal Information); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) (holding that plaintiffs' allegation of increased risk of identity theft was sufficient to confer constitutional standing, despite the plaintiffs' failure to plead financial loss or actual incidents of identity theft). *See also* discussion in section on "Privacy Issues Arising Out of Behavioral Advertising and Online Tracking," above.

630 *See, e.g., Katz v. Pershing, LLC*, 672 F.3d 64, 79 (1st Cir. 2012) (plaintiff's purchase of "identity theft insurance and credit monitoring services to guard against a possibility, remote at best, that her nonpublic personal information might someday be pilfered" was a "purely theoretical possibility" that did "not rise to the level of a reasonably impending threat."); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (concluding that "allegations of hypothetical, future injury are insufficient to establish standing" and affirming dismissal of a complaint in which the putative class members alleged that, as a result of a data breach involving personal information, they had an increased risk of identity theft, incurred costs to monitor their credit activity, and suffered emotional distress), *cert. denied*, 132 S. Ct. 2395 (U.S. 2012). *See also Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008); *In re LinkedIn User Privacy Litig.*, No. 5:12-CV-03088 EJD, 2013 WL 844291 (N.D. Cal. Mar. 6, 2013) (allegations of economic harm were insufficient to satisfy standing requirement); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009); *Hammond v. Bank of New York Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307, at *7 (S.D.N.Y. Jun. 25, 2010) ("The Court concludes that Plaintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural. There is no 'case or controversy.'").

631 568 U.S. ___, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013). *See, US Supreme Court Limits Standing to Sue in a Case that will Likely Impact Privacy and Data Breach Plaintiffs*, Edwards Wildman Client Advisory, www.edwardswildman.com/newsstand/detail.aspx?news=3595.

632 Another recent case, *Am. Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), may provide a foreshadowing of how courts balance privacy concerns with those of national security. There, the ACLU alleged that the NSA's bulk metadata collection program violated the Fourth Amendment. The court concluded that the NSA's collection of metadata related to ACLU's phone calls constituted actual injury to establish standing, but held that the collection of all phone metadata was authorized by FISA, and that the metadata collection program did not violate the Fourth Amendment.

enterprising plaintiffs can find novel ways to demonstrate more immediate impacts flowing from data breaches.[633]

2. Cognizable Injuries

Even if a consumer claim is deemed to satisfy the standing requirement, it may still be dismissed, or subject to an unfavorable ruling on summary judgment, if it fails to allege a cognizable injury under state law. In other words, the court may acknowledge that the plaintiff pleaded a sufficient injury to satisfy Article III's standing requirements, but conclude that applicable state law simply does not provide a remedy for such an injury.[634]

A recent example of the battlefield over whether consumer class actions arising from a data breach can sufficiently assert a valid cause of action for legally cognizable damages is the litigation arising from the well-publicized Sony PlaySation breach. Sony faced consumer class action suits after a

---

633 *See, e.g.*, *Strautins v. Trustwave Holdings, Inc.*, No. 12 C 09115, 2014 WL 960816 (N.D. Ill. Mar. 12, 2014) (citing *Clapper*, plaintiffs lacked standing where allegations were "insufficient to show that she and others face a 'certainly impending' risk of identity theft"). It remains to be seen how the lower courts will apply this decision to privacy and data breach cases, and there is some contradictory law in other contexts. For example, in June 2012, the U.S. Supreme Court, after hearing oral argument, elected not to consider the Ninth Circuit's decision in *First American Financial v. Edwards*, in which the Ninth Circuit had held that statutory damages could be sufficient to confer Article III standing (injury in fact) for plaintiffs. 610 F.3d 514 (9th Cir. 2010), cert. dismissed as "improvidently granted," 132 S. Ct. 2536, 183 L. Ed. 2d 611 (2012). Similarly, the court *in In re LinkedIn User Privacy Litigation*, No. 5:12-cv-03088-EJD, slip op. 100 (N.D. Cal. Mar. 31, 2014), recently refused to dismiss a putative class action against LinkedIn in which the named plaintiff, a premium subscriber to the website, alleged the company made misrepresentations about its privacy policy. She also alleges that, had she known about LinkedIn's "lax security practices", she would have either attempted to purchase premium service at a lower service or not purchased it at all. *Id.* at 3. The court had previously held that plaintiff lacked standing based on her allegations that "1) she did not receive the benefit of her bargain with LinkedIn, and 2) she now faces an increased risk of future harm as a result of the 2012 hacking incident." *Id*. at 6. The court, however, held that the allegations in the second amended complaint were sufficient to confer standing under California's Unfair Competition Law ("UCL") because plaintiff alleged that she read and relied on the LinkedIn's privacy statement. *Id*. In doing so, the court held that "the representation in LinkedIn's Privacy Policy falls within the scope of the labeling/advertising cases" subject to the UCL. *Id*. at 9. In contrast, in *Galria v. Nationwide Mut. Ins. Co.*, No. 2:13-CV-118, 2014 WL 689703 (S.D. Ohio Feb. 10, 2014), plaintiffs in putative class-action suit sued after hackers stole personally identifiable information from the defendants, but did not allege that the personal identifiable information was misused or that their identity was stolen as a result of the hacking. The court held that neither the increased risk that plaintiffs would be victims of identity theft at some indeterminate point in the future, nor the expenses to mitigate risk of identity theft, nor the loss of privacy, constituted injury sufficient to confer standing. Similarly, in *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, CV 12-2358-SLR, 2013 WL 5582866 (D. Del. Oct. 9, 2013), the court recently dismissed claims against Google alleging it violated the Electronic Consumer Privacy Act ("ECPA") and other federal and state statutes by tricking internet browsers to accept "cookies" that could be used to track users' activities in order to, *inter alia*, display targeted advertising. The court held that the putative class did not allege injury-in-fact sufficient to establish Article III standing because, although the plaintiffs' personal information has value, the plaintiffs failed to allege how Google's collection of that information affected its value. Going beyond this, the court said plaintiffs' case would also fail on the merits because Uniform-Resource Locators ("URLs") are descriptors, rather than communication, within the meaning of the ECPA. In other cases, however, courts have held that allegations that impact on battery consumption caused by data collection and aggregation practices are sufficient to allege standing at the pleading stage. *See, e.g.*, *In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013); *Goodman v. HTC Am., Inc.*, No. C11-1793, 2012 WL 2412070 (W.D. Wash. June 26, 2012) (allegation that defendant's location tracking practices shortened battery charges and battery life were sufficient to state claim under California's Unfair Competition Law. Cal Bus. & Prof.Code § 17200). The court in *In re Google Android Consumer Privacy Litig.* later held that claims related to impacts on battery life were insufficient to allege economic damages under the Consumer Fraud and Abuse Act, but allowed other claims to proceed based on such allegations. *See In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264, slip op. 78, at 7 (N.D. Ca. Mar. 10, 2014) (unpublished).

634 *See, e.g.*, *In re IPhone Application Litigation, supra; Pisciotta v. Old Nat. Bancorp*., 499 F.3d 629 (7th Cir. 2007); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 918 (N.D. Cal. 2009); *McLoughlin v. People's United Bank, Inc.*, No. 3:08-cv-00944, 2009 WL 2843269, at *8 (D.Conn. Aug. 31, 2009).

criminal intrusion into its video game network.[635] The court dismissed the original complaint against Sony entities, although with leave to amend. In doing so, the court observed that "future harm may be regarded as a cognizable loss sufficient to satisfy Article III's injury-in-fact requirement," but plaintiffs still must allege sufficient cognizable injury, as "the mere 'damage of future harm, unaccompanied by present damage, will not support a negligence action'" and the allegations as pled were also not sufficient for violation of California consumer protection laws because an increased risk alone is not sufficient.[636] Plaintiffs thereafter filed an amended complaint. While the court granted Sony dismissal of most of the claims including those for negligence and negligent misrepresentations, it did find that the allegations were sufficient for standing with regard to claims under California consumer protection statutes based on allegations that Sony had omitted material information regarding the security of its online services at the time that consumers purchased their consoles, thus sufficiently alleging a loss of money or property as a result of unfair business practices. The court also noted that plaintiffs had made sufficient allegations of affirmative misrepresentations in the company's user agreements and privacy policy regarding "reasonable security" and "industry standards encryption, as well a fraud based omissions and thus denied dismissal of claims under California consumer protection statutes.[637]

Defendants have obtained favorable holdings in other recent data breach litigations as well, although trends are difficult to predict and often depend on jurisdiction, as well as facts.[638]

An earlier federal data breach case illustrates the obstacles that both plaintiffs and defendants face, and the potential impact of jurisdiction and the particular facts and circumstances of the breach, although the result may have been different if considered by a federal court after the decision in *Clapper v. Amnesty International U.S.*, *supra*, on the issue of when injury is too speculative. .n litigation arising from the Hannaford Brothers stores breach, a federal district court in Maine, in a decision later reversed in part, initially dismissed a consumer class action due to lack of cognizable injury, concluding that consumers who did not have a fraudulent charge actually posted to their account cannot recover.[639] When the district court certified questions to the state's highest appellate court as to what constitutes a cognizable injury under Maine common law, the Maine Supreme

---

635 *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. MDL-11MD2258 AJB-MDD, 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012).

636 *Id.*

637 *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. MDL 11MD2258, 2014 WL 223677 (S.D. Cal. Jan. 21, 2014). See Stephen Prignano and Matthew Murphy, *What is next in consumer data breach litigation*?, Inside Counsel, May 8, 2014, http://www.insidecounsel.com/2014/08/01/whats-next-in-consumer-data-breach-litigation-mini.

638 *See, e.g., Willingham v. Global Payments, Inc., No. 12-cv-01157*, 2013 WL 440702 (N.D. Ga., Feb. 5, 2013) (Magistrate Judge recommended dismissal with prejudice of consumer claims against breached entity; case subsequently discontinued); *Galaria v. Nationwide Mut. Ins. Co.*, 2014 WL 689703 (S.D. Ohio, Feb. 10, 2014) (dismissing putative class action brought against an insurance company stemming from theft of personal information from its network, and rejecting that plaintiffs who did not have actual identity theft were injured; court held increased risk of further injury was too speculative to confer standing, and discussed the existing case law arising from data breaches).

639 *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 613 F. Supp. 2d 108 (D. Me. 2009), *rev'd*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011). The court allowed the case to proceed as to a single named plaintiff who had allegedly suffered a fraudulent charge that had allegedly not been removed from her account and which she had to pay. *See also Rowe v. Unicare Life and Health Ins. Co.*, No. 09-C-2286, 2010 U.S. Dist. LEXIS 1576 (N.D. Ill. Jan. 5, 2010), in which the court, citing the liberal pleading requirements of Illinois law, declined to dismiss common law and statutory claims related to the inadvertent disclosure of the plaintiffs' Personal Information on the Internet although there were no allegations of theft of Personal Information.

Court held that, under Maine law, in the absence of physical harm or economic loss or identity theft, time and effort alone spent in a reasonable effort to avoid harm do not constitute a cognizable injury for purposes of negligence or implied contract.[640] The federal court accordingly entered judgment in favor of the defendant. Plaintiffs appealed that decision to the United States Court of Appeals for the First Circuit, which overturned the lower federal court decision as to certain categories of alleged damages, at least insofar as holding allegations were sufficient to withstand a motion to dismiss. The First Circuit held that consumer claims for reimbursement of the cost of identity theft insurance and of fees for replacement of credit and debit cards following a breach of their personal information can be a cognizable injury, under certain circumstances.[641] The court determined that certain categories of costs incurred by the plaintiffs were "reasonably foreseeable mitigation costs" and thus constitute a cognizable harm (under Maine law). The court held, however, that not all mitigation costs in all circumstances would be recoverable but, rather, that plaintiffs need to show that the efforts to mitigate were reasonable, and that those efforts constitute a legal injury "such as actual money lost, rather than time or effort expended."[642] The First Circuit made a distinction between breaches involving inadvertently misplaced or lost data that has not been accessed or misused by third parties, from a large-scale criminal operation in which credit or debit card information was deliberately taken by sophisticated thieves to use the information to their financial advantage and had resulted in reports of actual fraudulent use of many (1,800) of the stolen card accounts, and held that: "[i]t was foreseeable, on these facts, that a customer, knowing that her credit or debit card data had been compromised and that thousands of fraudulent charges had resulted from the same security breach, would replace the card to mitigate against misuse of the card data. … Similarly, it was foreseeable that a customer who had experienced unauthorized charges to her account … would reasonably purchase insurance to protect against the consequences of data misuse."[643] The court also noted that "the principle of reasonableness" imposes a boundary on recovery of costs by claimants and noted, by way of example, that where neither the plaintiff nor those similarly situated have experienced fraudulent charges resulting from theft or loss of data, the purchase of credit monitoring services may be unreasonable and not recoverable. It also affirmed the lower court's holding that there can be situations in which there is no foreseeable loss as a matter of law. Therefore, the court upheld the district court's finding that damages such as loss of award points and change fees for pre-authorized credit transactions are not foreseeable and not compensable.[644]

---

640 *In re Hannaford Bros. Co. Customer Data Security Breach Litig.*, 2010 Me. 93, 4 A.D.3d 492, 497 (Me. 2010) ("Unless the plaintiffs' loss of time reflects a corresponding loss of earnings or earning opportunities, it is not a cognizable injury under Maine law of negligence").

641 *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011).

642 *Id.*

643 *Anderson v. Hannaford Bros. Co.*, 659 F.3d at 164-65. For an analysis of the First Circuit's decision in *Hannaford Bros. Co.*, *see Edwards Wildman Palmer LLP Client Advisory*, "*Foreseeable and Reasonable Mitigation Costs Can Constitute Cognizable Injury from a Data Breach – At Least Under Maine Law*," Oct. 2011, http://www.edwardswildman.com/newsstand/detail.aspx?news=2659.

644 On remand, the district court denied plaintiffs' motion for class certification, finding that plaintiffs had failed to meet the predominance requirements of Fed. R. Civ. P. 23(b)(3). *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, No. 2:08-MD-1954, 2013 WL 1182733 (D. Me. Mar. 20, 2013). The court in its decision denying class certification noted the plaintiffs' failure to provide expert testimony supporting its theory of class-wide damages, which meant that common issues would not predominate with regard to damages.

A similar result was reached in a federal decision construing the Federal Trade Commission Act ("FTCA") as it found that lost time and expense constitutes "substantial injury" under FTCA.[645] However, jurisdiction and factual allegations count, and other courts have held that a claim for credit monitoring costs following a theft of a laptop or other computer hardware containing Personal Information, without evidence that the information had been accessed or used, is alone not sufficient to sustain a claim for negligence under applicable common law.[646]

For their lawsuits to survive, plaintiffs asserting claims of financial injury as a result of a data breach must sufficiently allege not only cognizable legal injury, but also adequately allege facts supporting causation between a breach due to improper conduct by a plaintiff (such as failure to provide reasonable security) and the injury (identity theft and associated financial loss). While survival of a motion to dismiss does not mean that the plaintiff would ultimately prevail at the end of the case, the costs of litigation and associated risks can generate substantial settlements.[647]

---

645 *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1105 (S.D. Cal. 2008) (finding that the affected consumers "often spent a considerable amount of time and resources contesting the checks at their banks, protecting their accounts, and attempting to get their money back" and that "the time consumers spent in these efforts was valuable"), *aff'd,* 604 F.3d 1150 (9th Cir. 2010).

646 *See, e.g.* Compare *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012) (where computer system containing personal information was stolen, the "costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a "concrete and particularized" or "actual or imminent" injury;, *Hammond v. The Bank of N.Y. Mellon Corp.,* No. 1:08-CV-06060 (S.D.N.Y. Jun. 25, 2010) (granting defendant's motion for summary judgment on claims of negligence, breach of fiduciary duty, breach of implied contract, and state consumer protection law concerning the theft from the defendant of computer backup tapes containing Personal Information of the plaintiffs; the court held that the plaintiffs lacked Article III standing because their claims of increased risk of future harm were "future-oriented, hypothetical, and conjectural," and thus there was no case or controversy); *Ruiz v. Gap, Inc. and Vangent Inc.*, 622 F. Supp. 2d 908 (N.D. Cal. 2009), *aff'd*, 380 Fed. App'x. 689 (9th. Cir. 2010) (granting defendants' motion for summary judgment of claims for negligence and breach of contract seeking compensation for credit monitoring services, which claims arose from theft of laptop computers from the offices of a vendor of Gap that processed job applications, resulting in loss of Personal Information of plaintiffs; the court held that under California law, the increased risk of future theft did not rise to the level of appreciable harm necessary to assert a negligence claim, and plaintiff's assertion that his credit monitoring costs were a compensable attempt to mitigate damages failed because he had no damages to mitigate since he had never been a victim of identity theft); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273 (S.D.N.Y. 2008) (dismissing the claim for negligence and breach of fiduciary duty brought by an employee against his employer's vendor who lost a laptop; however, the court did allow to go forward the claim for breach of contract to allow discovery on the issue of whether the employee was a third-party beneficiary of the contract between his employer and the vendor; the plaintiff had withdrawn his other claims for misrepresentation and breach of privacy); *Shafran v. Harley Davidson, Inc.,* No. 07-CV-01365, 2008 WL 763177 (S.D.N.Y. Mar. 20, 2008) (granting motion to dismiss claims for future credit monitoring arising from loss of a laptop containing Personal Information, and noting that "[c]ourts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy"). These decisions also identify case law in other jurisdictions addressing the issue of what is a legally cognizable injury of an individual whose Personal Information was breached, but who has not sustained actual identity theft or financial loss; *Stollenwerk v. Tri-West Health Care Alliance*, 254 Fed. Appx. 664 (9th Cir. 2007) (upholding summary judgment against plaintiffs whose Personal Information was contained on a stolen hard drive, and denying credit monitoring costs as damages, as the plaintiffs did not claim any actual misuse of their Personal Information). *See also Randolph v. ING Life Ins. and Annuity Co.*, 486 F. Supp. 2d 1 (D.D.C. 2007) (finding that the plaintiffs' increased risk of identity theft and the cost of protecting against identify theft, following the theft of a laptop containing their private Personal Information, did not rise to the level of an "injury in fact" for constitutional standing purposes).

647 For example, in *Resnick v. AvMed, Inc.*, No. 10-cv-24513 (S.D. Fla. Filed Dec. 17, 2010), plaintiffs alleged that AvMed failed to secure personal plaintiffs' personal information including protected health information on company laptops, two of which were stolen from the AvMed's office conference room that contained personal information for over one million customers. Although the district court initially dismissed the case based on a lack of cognizable injury, the Eleventh Circuit reversed, holding that plaintiffs in issue had sufficiently alleged a nexus between the data theft and their identity theft; the Eleventh Circuit also upheld a claim for unjust enrichment which did not have a causation requirement, based on allegations that the plaintiffs had conferred a monetary benefit on AvMed in the form of monthly premiums that included an element for administrative costs of data management and security that they allegedly failed to implement. 693 F. 3d 1317 (11th Cir. 2012). The parties subsequently settled the claim for

In the face of the challenges in establishing common law damages, consumer attorneys have been pressing statutory claims as an avenue for recovery.[648] Companies facing potential data breach cases, therefore, must navigate a briar patch of federal and state data breach, privacy and consumer protection laws, many of which include a private right of action.[649] As demonstrated by the cases cited in this paper, recent court decisions demonstrate a trend of alleging unjust enrichment based on plaintiffs' financial payments to defendants for services that included data protection, and for violation of state unfair trade practice or consumer protection statutes. [650] A recent decision found that class action plaintiffs' claims survived at least this initial hurdle under California's Consumers Legal Remedies Act when they alleged that the defendant disclosed highly sensitive Personal Information; the statute requires only that a consumer has suffered "any damage," defined by California decisions as a "low but nonetheless palpable threshold of damage."[651] Another federal court decision interpreting California law, however, limited plaintiffs' potential recovery by requiring that all members of a class action establish a pecuniary loss resulting from a data breach or privacy violation.[652] Moreover, given the differences in state statutes, plaintiffs may recast certain claims under more favorable state statutes.[653]

$3 million. See order Granting Motion for final Approval of Class Action Settlement Agreement, February 28, 2014, Case No. 10-cv-24513-JLK. (United States District Court, Southern District of Florida).

[648] In the case of *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 908 (9th Cir. 2011), quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992), observed, "a concrete 'injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.'").

[649] *See* U.S. CHAMBER INSTITUTE FOR LEGAL REFORM, THE NEW LAWSUIT ECOSYSTEM 102-03 (Oct. 2013) (citing DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY FUNDAMENTALS 150, 172-74 (Int'l Ass'n of Privacy Prof'ls, 2nd ed. 2013).

[650] Some state statutes rely on interpretations of the federal FTCA, and apply its reasoning. *See, e.g.*, Conn. Gen. Stat. § 42-110(b); 5 Me. Rev. Stat. Ann. Tit. 5, § 207(1).

[651] *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102 (N.D. Cal. 2010); *see also Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524 (Cal. 2011) (holding that requesting and recording a cardholder's ZIP Code violates California's Song-Beverly Credit Card Act); *Gaos v. Google Inc.*, No. 5:10-CV-4809, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (holding that plaintiff sufficiently alleged injury in fact under the Stored Communications Act (part of the Electronic Communications Privacy Act) against Google Inc.); it was consolidated with *In Re Google Referrer Header Privacy Litigation*, 5:10-cv-0489-EJD (N.D. Cal.), and recently received preliminary approval of a class action settlement, 2010 WL 1266091 (N.D. Cal. March 26, 2014).

[652] *In re Google Inc. Street View Electronic Comm. Litig.*, 794 F. Supp. 2d 1067 (N.D. Cal. 2011), *affirmed*, *Joffee v. Google*, Inc., 746 F.3d 920 (as amended Dec. 27, 2013), plaintiffs case argued that Google used sophisticated equipment not available to the public when taking photographs to be incorporated in its Google Maps and Google Earth programs in order to determine what websites were being visited by users whose data had been collected. They claimed that Google violated wiretapping statutes and laws, and that Google's actions constituted an unfair and deceptive trade practice in violation of California law. The court denied Google's motion to dismiss the federal wiretapping claim, granted the motion to dismiss the state wiretap claims and granted the motion to dismiss the unfair and deceptive trade practice claim. Moreover, the recent decision of *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 185 L. Ed. 2d 515 (2013), reminds lower courts to employ "a rigorous analysis" of the commonality requirements of a putative class, including that damages can be measured class wide. In *Harris v. comScore, Inc.*, 292 F.R.D. 579, 589 (N.D. Ill. 2013), however, the court recently certified a class, rejecting comScore's argument that "issue of whether each individual plaintiff suffered damage or loss from comScore's actions precludes certification." The court held this argument had "no applicability to the ECPA or SCA claims, both of which provide for statutory damages." *Id.*

[653] *See, e.g., Grigsby v. Valve Corp.*, No. C12-0553JLR (W.D. Wash. Mar. 18, 2013). In *Grigsby*, the plaintiff had previously alleged violations of California state statutes, including the California Consumer Legal Remedies Act, the California Unfair Business Practices Act, and the California Song-Beverly Consumer Warranty Act. The court held that the plaintiff had failed to state a claim upon which relief may be granted, but allowed the plaintiff 30 days to amend the complaint. In response, the plaintiff alleged violations of the Washington Consumer Protection Act, alleging that he and other class members would not purchase Valve's services or would have done so at a different price if they had they known that Valve was not reasonably protecting its customers' Personal Information, as promised.

3. Breach-Related Lawsuits

As demonstrated by cases and studies identified above, large breaches of consumer Personal Information are often followed by data breach litigation. Moreover, data breaches have not been isolated to a particular sector of the economy; instead, they plague every industry, including entertainment, education, retail, banking, and health industries, among others.[654] Such suits continue to be filed, despite the significant hurdles that plaintiffs face in terms of establishing standing and legally cognizable claims for recoverable damages discussed above.

As generally a single consumer's claim is not financially significant enough to support litigation, whether consumer litigation in the U.S. is pursued often turns on whether a plaintiffs' attorney will be able to obtain class certification for all – or a large number of – consumers affected by a breach. Thus, in addition to the hurdles of standing and damages, another obstacle that plaintiff consumers' and their counsel face is class action certification. The hurdles to be overcome in certifying a class, which requires demonstrating that common issues predominate, in the data breach context, are discussed in the class certification decision arising out of the Hannaford breach.[655] There, plaintiffs moved to certify a class consisting of customers who incurred out-of-pocket costs in mitigating efforts in response to the breach. The court reviewed the factors necessary for plaintiffs to demonstrate to obtain class certification, and denied certification, on the grounds that common questions of as to damages did not predominate, particularly with regard to the impact of the breach in issue on individual proposed members of the class and the costs they incurred. The court noted that the fact that damages may have to be ascertained on an individual basis is not alone sufficient to defeat class certification, but noted that while plaintiffs contended they could demonstrate total damages sustained by the class by statistical proof, their lack of an expert opinion on their ability to prove total damage was fatal to class certification. The decision does not rule out the possibility of class certification if the proper demonstration is made, but does demonstrate the uphill battle plaintiffs face in obtaining class certification.

That said, the current spate of litigation over the past few years is not likely to end soon, and some entities faced with the costs of breach litigation decide to settle with the putative class or otherwise privately resolve the dispute, resulting in further costs to a breached entity.[656]

---

654 *See, e.g.*, *Bell v. Blizzard Entertainment, Inc.*, No. 12-09475 (C.D. Cal. 2012) (class action lawsuit against video game company); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. MDL-11MD2258, 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012) (class action against entertainment company); *Faircloth v. Adventist Health System/Sunbelt, Inc.*, No. 6:13-cv-00572 (M.D. Fla. filed Apr. 9, 2013) (class action filed against hospital); *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 613 F. Supp. 2d 108 (D. Me. 2009) (grocery chain), *rev'd*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011); *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 893 F. Supp. 2d 1058 (D. Nev. 2012) (online retailer); *In re LinkedIn User Privacy Litig.*, No. 5:12-CV-03088 EJD, 2013 WL 844291 (N.D. Cal. Mar. 6, 2013) (online social networking site); *o Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (class action against company that delivers healthcare services through health plans and government sponsored managed care plans). See also Section V.b. above, The Industries, Assets, and Types of Data Most Frequently Compromised.

655 *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, No. 2:08-MD-1954, 293 F.R.D. 21 (U. S. Dist. Ct, D. Me., Mar. 20, 2013). Another decision initially denying class certification in the data breach context, under a state class action statute, *Tabata v. Charleston Area Medical Center*, 2013 WL 8210917 (W. Va. Cir. Ct., June 24, 2013), was recently reversed and remanded in a decision that states it is to be narrowly construed and is not to be considered an indicator of ultimate success of the claims, *Tabata v. Charleston*, Supreme Court of Appeals of West Virginia, Case No. 12-076 (May 28, 2014).

656 For example, dozens of suits have already been filed against Target Corp. as a result of a data breach which began in the closing weeks of 2013 in which data related to tens of millions of credit cards was potentially compromised by hackers. *See, e.g.*,

Consumer claims are not the only legal proceedings faced by a breached entity. The number and variety of lawsuits that can be faced by a breached entity is demonstrated by the TJX breach, one of the earlier and larger retail security breaches, in which hackers stole data relating to over 45 million credit and debit cards used at TJX stores[657], as well as the Heartland Processing Systems breach discussed above, and more recently by the late 2013 Target breach also discussed above. These demonstrate that particularly in mega breaches, resulting proceedings will include not only consumer lawsuits, but also potentially suits by shareholders and investors, banks and card brands if payment cards are involved, vendors or others entities involved, and an array of regulatory investigations by state attorneys general and any federal or other government entities with oversight authority over the type of entity that sustained the breach.

As discussed above in the section on third party losses arising from data breaches, bank issuing payment cards that are the subject of a breach have asserted claims for losses arising from fraudulent charges on stolen credit cards, although they also face a number of substantial hurdles in establishing legally cognizable claims. (See Section V.3. c. ii above, Bank Claims; see also Section III. 3. above, PCI, discussing the Payment Card Industry contractual assessments arising from data breaches and related litigation).

Plaintiffs in data breach cases continue to develop new strategies and theories of liability, particularly in the face of the obstacles presented by standing and damages issues.[658] Newer theories include claims for misrepresentation based on inaccuracies in notice letters as to the breach or any continuing risks it presents, in communications from call centers established by the breached entity, and in statements regarding security practices in privacy policies.[659] Taking a different approach, one academic commented on the potential use of product liability law and claims of product defect in privacy-related claims, particularly in the area of social media.[660] While many of these theories have yet to be fully tried and tested, as breaches continue and this area of law develops, plaintiffs' lawyers will undoubtedly explore new theories of recovery, and defendants' lawyers in turn will assert new defenses to them.

Ala. State Empl. Credit Union v. Target Corp., No. 13-cv-952 (M.D. Ala. filed Dec. 30, 2013); *First Choice Fed. Credit Union v. Target Corp.*, No. 14-146 (W.D. Pa. Filed Jan. 31. 2014); *Council v. Target Corp.*, No. 13-CV-03479, 2014 WL 859326 (D. Colo. Mar. 5, 2014). The lawsuits against Target have been consolidated in a Multi-District Litigation venued in St. Paul Minnesota, Target's home state, in *In Re Target Corporation Customer Data Breach Litigation*, Case No. 02522, United States District Court, Minnesota.

657 *In re TJX Companies Retail Sec. Breach Litig.*, 584 F. Supp. 2d 395, 397-98 (D. Mass. 2008).

658 Plaintiffs have also had some success in resurrecting older theories. *See, e.g., Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421 (5th Cir. 2013) (economic loss doctrine did not bar banks' negligence claim).

659 *See, e.g., Steinberg v. CVS Caremark Corp.*, No. 11-2428, 2012 WL 507807 (E.D. Pa. Feb. 16, 2012) (in which plaintiff sued under Pennsylvania's Consumer Protection Act, claiming that defendant materially misrepresented its privacy policies on data handling; the court dismissed the suit and held that, among other things, the plaintiff did not suffer cognizable loss did not allege justifiable reliance on defendant's representations). *See also Worix v. Medassets, Inc.*, No. 11 C 8088, 2012 WL 1419257 (N.D. Ill. Apr. 24, 2012) (dismissing plaintiff's causes of action under the Stored Communications Act, HIPAA, and the Illinois Personal Information Act, but allowing discovery as to allegations under the State Consumer Fraud Act in a situation in which a computer hard drive containing personal information was stolen); *In Re Michaels Pin Pad Litigation*, 2011 WL 5878373 (N.D. Ill. Nov. 23, 2011) (also dismissing statutory claims, as well as negligence claim, although allowing consumer claim of breach of implied contract to proceed).

660 James Grimmelmann, *Privacy as Product Safety*, 19 Widener L. Symp. J. 793 (2010).

4. Privacy Practices Lawsuits

A number of cases have recently targeted the business practices of companies in collecting and using information, and the companies' disclosures (or lack of disclosures) of their collection and usage of information about individuals, rather than the failure to protect that information from breach. These cases involve various data collection practices implicating privacy concerns and issues of compliance with state and federal statutes and regulations that are only now being tested in the courts. For instance, plaintiffs are increasingly challenging data collection practices of various retailers at points of sale, the recording of telephone conversations between customers and service personnel, and challenging the collection of information of various types from smartphones and other mobile computing devices by application developers. While many of these challenges have been dismissed by the courts for various reasons, others are beginning to gain traction.

The types of claims discussed here are illustrative of the growing trend of privacy-related lawsuits based on business practices and state statutes. While many of these are based on California state statutes, that jurisdiction tends to be the precursor to new privacy claim trends.

a. Point of Sale Data Collection Practices

Two states have recently been at the forefront of challenges to the collection of data by retailers at the point of sale – California and Massachusetts. The highest appellate courts of both states have now weighed in on the fairly common practice by retailers of collecting and often recording ZIP code information from customers in the process of making merchandise purchases using credit cards at store premises, finding that certain aspects of ZIP code collection and recording practices can violate some states' statutes limiting retailers' rights to request and record personal information during a credit card transactions, with some exceptions.

In California, the state Supreme Court considered a challenge to a retailer's practice of collecting ZIP code information from customers at the point of sale.[661] Lower courts that had considered the case did not find that the collection of ZIP code information constituted "personal identification information" prohibited from collection by the Song-Beverly Credit Card Act of 1971 ("Song-Beverly Act"), which limits the right to request or require a customer to provide personal information, defined as including addresses, as a condition to accepting a credit card as payment, if the information is unnecessary to the credit card transaction. Based in part on the availability of software that allows a retailer to obtain a customer's full address by using the name and ZIP code, collection of ZIP codes was found to violate the statutes if unnecessary to complete the credit card transaction. The California Supreme Court reversed lower court holdings, holding that ZIP code information constitutes "personally identifiable information" under the Song-Beverly Act, and thereby opening the door to a plethora of consumer class actions against retailers.[662]

---

[661] *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 246 P.3d 612, 120 Cal. Rptr. 3d 531 (2011). See also *Dardarian v. Office Maxx North America, Inc.*, 875 F. Supp. 2d 1084 (2012) (holding that the *Pineda* opinion applied retrospectively). See *California Supreme Court's Zip Code Decision Exposes Retailers to New Litigation Hazard, Statutory Fines,* Edwards Wildman Client Advisory, April 2011, www.edwardswildman.com/newsstand/detail.aspx?news+2302.

[662] There are exceptions, however, such as where a company requests ZIP code information to prevent fraud, such as during transactions at gas pumps. *See, e.g., Flores v. Chevron, U.S.A., Inc.*, 217 Cal. App. 4th 337 (2013).

On the other hand, a California district court recently refused to certify a class in a suit against Wal-Mart, where the putative class alleged that Wal-Mart had collected phone numbers at the point of sale in violation of the Song-Beverly Act.[663] The court made a distinction between business use cards and consumer use, and observed that the California Court of Appeal has held that "purpose for which the card was issued, rather than the way in which the card was used, was the relevant inquiry in classifying" a credit card under the Song-Beverly Act, which only applies to natural persons and not to businesses. Thus, before liability could be established with respect to each class member, individualized proof regarding whether each class member's credit card was issued as a consumer or as a business card would have to be produced.

The Supreme Judicial Court of Massachusetts also recently considered a similar challenge to a retailer's practice of requesting ZIP code information at the point of sale.[664] Although interpreting a Massachusetts statutory scheme somewhat different than California's Song-Beverly Act, the court reached a similar result. In the Massachusetts case, the plaintiff challenged a retailer's practice of obtaining ZIP code information at the point of sale. Under the Massachusetts Unfair and Deceptive Business Practices Statute, a business entity that accepts a credit card for a transaction may not "write, cause to be written or require that a credit card holder write personal identification information, not required by the credit card issuer, on the credit card transaction form."[665] The court found that ZIP code information is, in fact, personal identification information within the meaning of the statute. According to the court, even though ZIP code information does not directly identify the consumer, it is possible to combine ZIP code information with other sources to obtain the customer's address and telephone number. Since the court found that the purpose of the statute was not merely to protect against identity fraud, but served the larger purpose of safeguarding consumer privacy, the court concluded that ZIP code information fell within the meaning of personal identification information that the statute was designed to protect. The court did also point out, however, that the mere collection of ZIP code information would not be enough to establish a claim under the statute. Thus, if ZIP code information were merely collected, but not used for any purpose thereafter, a cause of action for damages would not lie. Instead, the court required a plaintiff to show some harm flowing from the data collection which is more than just a violation of the statute itself. This, the court noted, could be shown in circumstances where a merchant uses personal identifying information to send unwanted solicitations to a consumer, or where a merchant sells personal identifying information to a third party. Finally, the Massachusetts Supreme Judicial Court made clear that the Unfair and Deceptive Business Practices Statute would apply to prevent writing personal identification information on a credit card transaction form whether the "writing" takes place in a paper or electronic format. In this regard, the court noted that electronic transactions are now pervasive and the legislature did not intend to limit the reach of the statute to antiquated forms of business transactions.

---

663 *Leebove v. Wal-Mart Stores, Inc.*, No. 13-01024 R(SHx), slip op. 37 (C.D. Cal. Oct. 4, 2013) (Real, J.)

664 *Tyler v. Michaels Stores, Inc*., 464 Mass. 492, 984 N.E.2d 737 (Mar. 11, 2013). See *Massachusetts Supreme Judicial Court Expands Zip Code Privacy Protection in Tyler v. Michaels Stores*, Edwards Wildman Client Advisory, March 2013, www.edwardswildman.com/newsstand/detail.aspx?news=3620.

665 Mass. Gen. Laws c. 93, § 105(a).

The District Court for the District of Columbia recently reached a different result, dismissing a complaint, with prejudice, after it found the retailers did not violate District of Columbia law[666] by asking for customers' ZIP codes at the point of sale.[667] The court observed, in interpreting the applicable statute, that "a ZIP code cannot be considered the 'address' of the 'cardholder' since a ZIP code, at best, merely indicates an area in which multiple addresses may be located,"[668] Moreover, the defendants recorded ZIP codes in the point of sale register, rather than into the credit card swipe machine. Thus, "the defendants took steps specially designed to adhere to the law by affirmatively separating the ZIP code information from the credit card information" and thus failed to plead a requisite element of a violation of the statute.[669] In reaching this decision, the court specifically noted that similar cases in Massachusetts and California serve to illustrate "restricted nature" of the statute it was considering, as compared to the statutes in issue in those states.[670]

b. Call Recording Practices

Data collection practices of merchants have also been challenged by plaintiffs in call recording cases.[671] Recently, there has been a rash of cases alleging that a company's recording of calls with its customers, usually alleged to be without notice or consent, violate the California Invasion of Privacy Act,[672] among other causes of action. The inquiry generally focuses not only on the content of the information, but on whether the parties had an "objectively reasonable expectation that the conversation is not being overheard or recorded."[673]

Typically, plaintiffs assert such claims and seek class certification, alleging a company secretly recorded conversations with customers transacting business by telephone. Plaintiffs alleged violations of the California Invasion of Privacy Act based on the recording or monitoring of their telephone conversations without their consent, and allege that, for example, in calls on "consumer-facing" toll-free lines consumers revealed personal identification information or confidential financial information, and that neither the operator or others on the line from the company informed customers that telephone calls were being recorded by monitoring software. Such suits generally

---

666 Plaintiffs alleged violations of the D.C. Use of Consumer Identification Information Act ("CII Act"), D.C. Code §§ 47-3151, *et seq.*, and the D.C. Consumer Protection Procedures Act ("DCCPPA"), D.C. Code §§ 28-3901 *et seq.*

667 *Hancock v. Urban Outfitters, Inc.*, No. 13-939, slip op. at 13 (D.D.C. Mar. 14, 2014).

668 *Id*. at 7.

669 *Id*. at 9.

670 *Id*. at 10.

671 *See, e.g., Faulkner v. ADT Security Services, Inc.*, 706 F.3d 1017 (9th Cir. 2012).

672 California Penal Code Section 630, *et seq.*

673 *See Faulkner* , 706 F.3d at 1019 (affirming the dismissal of the complaint in an action removed to federal court, but also remanding for the district court to consider allowing the plaintiff to amend his complaint to make the requisite allegations of circumstances and particulars of conversation to support that an objectively reasonable expectation of confidentiality would have attended a communication such as the one in issue). Recently, in *Young v. Hilton Worldwide, Inc.*, No. 12-56189, 2014 WL 1087777 (9th Cir. Mar. 20, 2014), a divided Ninth Circuit recently reinstated a class action against Hilton, in which plaintiffs allege the hotel chain violated the California Invasion of Privacy Act when it allegedly recorded calls without consent. In doing so, the Court observed that the order below dismissing the case "purported to do so on grounds that are applicable to § 632 only—namely, because the complaint failed to allege that the recorded communications were confidential and subject to a reasonable expectation of privacy." The court noted that "[t]he California Supreme Court has unequivocally held that no such requirement applies to § 632.7, and the district court's failure to recognize this was reversible error. *Id.* (citing *Flanagan v. Flanagan*, 27 Cal.4th 766, 776 (2002) (explaining that § 632.7's "prohibition applies to all communications, not just confidential communications")).

seek statutory damages of, for example, $5,000 for each violation, plus costs and attorney's fees, as well as an injunction against further violations.[674]

c. Data Collection Practices by Application Developers

In another growing trend, consumers are challenging the data collection practices of certain software applications ("apps") in collecting and recording information about mobile device users. Often, the target of such claims are large consumer electronics manufacturers, social media sites and major online retailers who allegedly failed to prevent apps that are sold through their services from uploading consumer information from plaintiffs' mobile devices without their consent.[675] However, app developers themselves are also becoming targets for these claims.[676]

As demonstrated by cases cited above in discussions of standing and damages, in such lawsuits, plaintiffs generally seek to challenge apps that operate as "tracking software," recording details about a consumer's use of their mobile devices. Plaintiffs have also alleged that certain apps access Personal Information on a user's mobile device, such as contact address books, and upload that information to the developer without the user's knowledge or consent. Some plaintiffs allege that certain apps install software on their mobile devices that record a user's interactions with social networking sites. Others allege surreptitious tracking of users by tagging digital images and video with GPS location coordinates, uploading photographs taken by the user on his or her mobile device, or using a mobile device to track a user's location. This information, according to the plaintiffs' allegations, is then transmitted to the developer by the app and may be stored on the developer's servers without encryption, creating a further security risk.

While some of these cases have been dismissed on the ground that plaintiffs failed to show an economic harm resulting from the practice,[677] others have allowed creative allegations of unjust enrichment and similar claims as demonstrated by one putative class action that was allowed to

---

[674] *See, e.g., Ades v. Omni Hotels Management Corp.*, No. 13-cv-02468 (C.D. Cal. filed Apr. 8, 2013).

[675] *See, e.g., Pirozzi v. Apple, Inc.*, 2012 WL 6652453 (N.D. Cal. Dec. 20, 2012). In a win for Apple and other manufacturers, a court recently held that mobile devices are not facilities through which electronic communication service is provided under the Stored Communications Act (SCA) and that location data is not "electronic storage" under the SCA. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012). There, a putative class of IPhone and IPad users brought an action against Apple, alleging Apple and others unlawfully allowed third party apps to collect and use personal information without user consent or knowledge. In the same decision, the court also dismissed the putative class's claims for invasion of privacy and trespass, as well as statutory violations of the Wiretap Act and Computer Fraud and Abuse Act (CFAA). It allowed the state claims under the Consumer Legal Remedies Act (CLRA) and the Unfair Competition Law (UCL) to remain, but later dismissed those claims, finding plaintiffs had failed to demonstrate they had relied on any alleged misrepresentations made by Apple. *In re iPhone Application Litig.*, No. 11-md-02250-LHK, slip op. No. 294, at 13 (N.D. Ca. Nov. 25, 2013). In doing so, the court found that a general issue of material fact existed as to whether plaintiffs' claims that they overpaid for their iDevices and that Apple's alleged actions affected battery list, storage space and bandwidth constituted an injury, but that as a matter of law, plaintiffs could not establish that these alleged injuries were causally linked to Apple's alleged misrepresentations. *Id*. at 11-13. Google faced similar claims in another case. *In re Google Android Consumer Privacy Litig.*, No. 11-md-02264, slip op. 78 (Mar. 10, 2014). There, Plaintiffs alleged that apps collected personal data and shared the data with Google without their knowledge. The court reaffirmed its previous holding that plaintiffs' allegations of adverse effects on battery charge and phone performance were sufficient to establish Article III standing. *Id.* at 5. The Court concluded, however, that these alleged injuries were insufficient to state a claim under the Computer Fraud and Abuse Act and partially dismissed claims under the California Unfair Competition Law. *Id*. at 7-10.

[676] See, e.g., *Hernandez v. Path, Inc.*, No. 12-cv-01515, 2012 WL 5194120 (N.D. Cal. Oct. 19, 2012).

[677] *See, e.g., Pirozzi v. Apple, Inc.*, 913 F. Sup. 2d 840 (N.D. Cal. Dec. 20, 2012).

proceed.[678] In that case, a plaintiff successfully argued that it would cost as much as $12,500 to remove the tracking software code installed by the app from his mobile device. Accepting those allegations as true for purposes of resolving the app developer's motion to dismiss in that case, the court ruled that such an economic harm, if ultimately proven to be true, would be sufficient to state a privacy claim against the app developer. (See Section VII.1. Article II. Standing, and Section VII.2. Cognizable Injuries, for additional case law).

Such lawsuits allege that a host of federal and state statutes were violated by the app developers, including federal wiretap statutes, computer crime statutes and state privacy statutes, as well as common law claims. While many causes of action are often dismissed and even those that survive early dismissal may not survive later summary judgment, as with many of these types of suits they present a serious financial cost in defending. Moreover, they can generate regulatory scrutiny, with the risks and costs attendant to regulatory inquiries.

d. Suits Alleging Violations of California's "Shine the Light" Law

As noted in Section II above, California's Shine the Light Law[679] requires businesses to disclose, at the request of a customer, how the business has shared consumer information with third parties. To comply with the law, a business must designate certain contact information to enable consumers to make requests under the statute. Alternatively, businesses may comply with the law by providing the consumer with the right to prevent disclosure of his or her personal information to third parties. A business that provides this alternative need not disclose how it has shared information.

Plaintiffs in several class action lawsuits have recently attempted to establish claims against businesses that violate the law, but so far without substantial success.[680] In these cases, plaintiffs principally allege that a business violated the law by failing to provide the required contact information to enable consumers to make requests under the statute. In order to establish a sufficient injury to satisfy standing requirements, plaintiffs have relied on two theories: first, that they suffered an economic injury as a result of the violation because the sale of personal information by the business to third parties reduces the market value of that information to the plaintiff;[681] and second, that they suffered an "informational injury" because, by failing to provide the necessary contact information, the business deprived the plaintiffs of information to which they were statutorily entitled.[682]

These cases, as do many in the privacy arena, provide a challenge to plaintiffs in establishing standing and damages, particularly as California's Shine the Light Law does not prevent businesses from selling or otherwise sharing customer information, but rather requires businesses to disclose

---

678 *Hernandez v. Path, Inc.*, No. 12-cv-01515, 2012 WL 5194120 (N.D. Cal. Oct. 19, 2012).

679 Section 1798.83 of the California Civil Code. See O*ft-ignored California Law Spawns New Batch of Class Action – Companies Dealing with California Consumer Data Need to Audit Practices and Policies*, Edwards Wildman Client Advisory, January 2012, www.edwardswildman.com/newsstand/detail.aspx?=2743.

680 *See, e.g., Murray v. Time, Inc*., No. C-12-00432, 2012 WL 3634387 (N.D. Cal. Aug. 24, 2012); *King v. Conde Nast Publications*, No. 12-cv-0719, 2012 WL 3186578 (C.D. Cal. Aug. 3, 2012); *Miller v. Hearst Communications, Inc.*, 2012 WL 3205241 (C.D. Cal. Aug. 3, 2012).

681 *See, e.g., Boorstein v. Men's Journal, LLC*, No. 12-cv-771, 2012 WL 2152815 (C.D. Cal. Jun. 14, 2012).

682 *Id.*

how information was shared with third parties. Plaintiffs also face an uphill challenge in their "informational injury" theory. In those claims, plaintiffs must show that they actually made a request, or would have made a request, for the information provided by the Shine the Light Law if the business had provided the required contact information. Plaintiffs must allege more than a mere procedural injury.[683]

e. Collection of Data Regarding Video Viewing Selections

Plaintiffs have also challenged the data collection practices of online providers of video content. In a suit that survived a motion to dismiss, plaintiffs alleged that a video content provider installed tracking software on the computers of users who visited the provider's website.[684] The software would then track the user's video selections and transmit that information to third parties without obtaining the user's consent. The software would also track a user's web-browsing history, even when they were not logged into the provider's website, and transmit that history to third parties. According to the complaint, the third parties included social networking sites and online advertisers. The allegations of the complaint were found to state a claim under the Video Privacy Protection Act ("VPPA"), which protects the personal information of individuals who rent video materials. Under the VPPA, a "video tape service provider" may not disclose personally identifiable information to any third party. Personally identifiable information, for purposes of the statute, includes the viewing history of those who request or obtain video materials or services.[685]

In allowing the suit to proceed, the court found that the online content provider qualified as a "video tape service provider" under the VPPA, even though the content provider did not rent physical video tapes. According to the court, the statute is not limited by the form in which the video content is disseminated. Rather, the VPPA is designed to apply to future changes in technology, such as streaming online video content. The court also ruled that plaintiffs qualified as "subscribers" under the statute, even though the plaintiffs did not allege that they rented or purchased content from the service provider. A magistrate judge later denied defendant Hulu LLC's motion for summary judgment based on lack of injury, holding that, under the plain language of the VPPA, plaintiffs must only show wrongful disclosure, and not actual injury, to recover damages.[686] More recently, however, the court partially granted summary judgment to Hulu, finding that disclosures to comScore, Inc., "a metrics company that analyzes Hulu's viewing audience and provides reports that Hulu uses to get media content and sell advertising", were anonymous that "hypothetically could have been linked to video watching," which was "not enough to establish a VPPA violation."[687] The court reached this conclusion even though comScore could have used the IDs provided to access the user's profile pages in an attempt to identify the user, because there was no evidence that comScore attempted to do so. In contrast, the court denied Hulu's motion with respect to disclosure to Facebook, because there were genuine issues of fact as to whether the data,

---

683 *Id.* at 3.

684 *In re Hulu Privacy Litig.*, No. C11-03764, 2012 U.S. Dist. LEXIS 112916, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012).

685 18 U.S.C. § 2710(b)(1).

686 2013 WL 6773794 (N.D. Cal. Dec. 20, 2013),

687 *In re Hulu Privacy Litig.*, No. 11-03764 LB, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

including cookies and in some cases IP addresses and Facebook IDs, could tie a video to a user of Facebook, which would be a prohibited disclosure under VPPA. Hulu's competitor, Netflix, may have spared itself a great headache when it opted to settle similar claims that it violated the VPPA when it allegedly retained and disclosed its customers' viewing habits.[688]

f. TCPA

Plaintiffs have also brought suits for violations of the Telephone Consumer Protection Act of 1991 (TCPA), which is designed to restrict unsolicited telephone, fax and text message solicitations.[689] (See Section III. The U.S. Regulatory and Statutory Framework, 2.j, Telephone Consumer Protection Act, above, for further details of the statute and case law).

The dismissal of one recent case, however, demonstrates there are limits to what will be considered a reasonable claim even in this heavily litigated area known for its plethora of class action litigation.[690] In that case, the plaintiff had initiated contact with the defendant to request that a text message he had written would appear on a scoreboard in a basketball arena. Plaintiff then received a confirmatory text in response, but alleged that he did not expressly consent to receive the confirmatory text message. The court dismissed the case, observing that, although the owners of the arena "allegedly failed to warn Plaintiff that he might receive a response, a 'common sense' reading of the TCPA indicates that, by sending his original message, Plaintiff expressly consented to receiving a confirmatory text…."[691]

g. Stored Communications Act

Unlike some other federal and state statutes, the federal Stored Communication Act[692] ("SCA") does not require proof of actual damages in order to establish standing. Under the SCA, an Internet Service Provider may be liable if it "knowingly" disclosed personal information to a third party.

In one recent case, a court held that Facebook posts were protected by the SCA.[693] There, a hospital employee set her Facebook account privacy settings such that her Facebook "friends" could view her posts. The employee then posted a statement on her "wall" criticizing first responders to a shooting in Washington, DC. Notably, those first responders were not employees of the hospital at which she worked. Nevertheless, her employer temporarily suspended her, claiming the post exhibited a "deliberate disregard for patient safety," after a fellow co-worker, who was a "Facebook friend," printed the page and showed it to hospital managers. The employee sued for invasion of privacy under SCA. The court dismissed the claim, holding that, although the posts were covered by the SCA, the employee had voluntarily given them to her co-worker Facebook friend, who in

---

688 Settlement Agreement at p. 12, *In re Netflix Privacy litigation*, No. 5:11-cv-379, Dkt. No. 76-1 (N.D. Cal., May 25, 2012).

689 *See, e.g., Sterling v. Mercantile Adjustment Bureau, LLC.*, 11-CV-639, 2014 WL 1224604 (W.D.N.Y. Mar. 25, 2014) (adopting report and recommendation that calls made by automatic telephone dialing system were made in violation of TCPA); *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946 (9th Cir. 2009) (text messaging was "call" covered under TCPA).

690 *Emanuel v. Los Angeles Lakers, Inc.*, CV 12-9936, 2013 WL 1719035 (C.D. Cal. Apr. 18, 2013)

691 *Id.* at *3.

692 18 U.S.C. §§ 2701–2712.

693 *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659 (D.N.J. 2013).

turn voluntarily gave the post to hospital management. The court observed that "[t]his may have been a violation of trust, but it was not a violation of privacy."[694]

VIII. Mitigation of Exposures

Much of the discussion in studies and among professionals and insurers addressing privacy-related claims has turned to scrutinizing past claims for insights regarding practices and procedures that can be used to help companies reduce the likelihood of incidents and claims, and the resultant costs and damages.

1. Data Breach Exposures

a. Compliance with Applicable Data Security Requirements

Many of the state and federal data security statutes and regulations discussed above in Section III are designed to reduce the occurrence of data breaches involving the Personal Information subject to such restrictions. As such, ensuring compliance with applicable data security requirements serves to significantly reduce a company's data breach exposure, both by reducing the likelihood that a breach will occur, and by limiting the potential consequences if the company's security is breached. Failure to comply with applicable state or federal data security statutes and regulations, or with industry-established security requirements such as PCI-DSS, may be used by consumers and other claimants to demonstrate that the entity whose data was breached is responsible for the consequences of a breach. Compliance with applicable statutes, regulations, and industry standards is one of the strongest defenses a breached entity has against claims based on negligence.

b. Instituting Reasonable Security Procedures

A 2013 study of data breaches reported that 78% of breaches were low or very low in difficulty and none were highly difficult; 76% of network intrusions exploited weak or stolen credentials.[695] While data security regulations require companies to institute security procedures designed to reduce the risk of data breach, security plans and procedures must be implemented to be effective. As discussed below, training employees to adhere to privacy and data security policies and procedures is critical to the implementation of such policies and procedures, and to the reduction of data breach exposures.

c. Limiting Access to Personal Information

Studies show that the frequency, scope and cost of breaches can be reduced by limiting the following: (i) access to Personal Information and other types of confidential information only to those with a need for that access; (ii) the amount of information collected and stored; and (iii) the length of time Personal Information is retained, to only that which is necessary. These limitations are the focus of both data security regulations and risk management protocols.

---

694 *Id*. at 674.

695 Verizon, *2013 Data Breach Investigations Report, supra.*

d. Training/Awareness

Human error (by employees, suppliers or other third parties) has been the reported cause of a large number of breaches. Employee negligence or maliciousness persists as the root cause of many data breaches, ranging from loss of laptops or other devices to mishandling of data. Human factors, including insufficiently robust passwords and poor password management, and computers left unattended or viewable in public venues, are among the factors contributing to many breaches that can be mitigated with training. Many breaches still are attributed to participation by insiders.[696]

Data breaches often occur when companies and their employees fail to consider the risk of data breaches from routine conduct, or fail to comply with applicable data security requirements. Resultant claims arise from lack of awareness by companies and their employees of applicable governmental data security requirements, and their own non-compliance.

Relatively simple measures that can reduce the risk of data breach, many of which may be required by applicable data security statutes and regulations, include the following:

- Educating company executives as to applicable legal requirements governing data security and the importance of establishing a team of appropriate internal personnel and external resources to: (i) identify the type and location of protected Personal Information collected, used, stored and transmitted by the company; (ii) assess the risks related to such information; and (iii) draft and propose appropriate and compliant procedures for security;

- Ensuring that paper records with Personal Information and other confidential information are properly disposed of in compliance with applicable requirements and data security best practices;

- Terminating an employee's access to computer terminals and company databases onsite and offsite immediately upon termination of the employee's employment;

- Instituting robust password requirements for access to databases with Personal Information and other confidential information, and prohibiting password sharing;

- Instituting robust password requirements for laptops and PDAs, which are susceptible to being lost or stolen, and reminding employees not to store the password with the laptop or PDA;

- Encrypting portable devices, and encrypting electronic documents with sensitive information before transmitting;

- Considering data security as an important factor in vendor selection and vendor management, and requiring data security and privacy measures in vendor contracts.

---

[696] Verizon, 2013 Data Breach Investigations Report, *supra;* Ponemon Institute, LLC, *The Human Factor in Data Protection*, Jan. 2012.

Implementing the recommendations above, followed by regular updates, evaluation and employee training, can dramatically reduce data breach exposures at relatively low cost to companies.

2. Risks of Collecting/Using Personal Information Improperly

As noted in the discussions above, increasingly both litigation and regulatory investigations focus on the business practices of companies in collecting and using information about consumers, and contentions of inadequate disclosures to consumers of such practices. Information about customers and prospective customers can be the most important asset of a company, but it presents risks that are to be taken into account as well. Risks to be considered and balanced include:

Compliance risks. Organizations are increasingly subject to statutes and regulations – state, federal and international – regarding the use of information, and potentially face litigation or regulatory sanctions and consent decrees when they are not in compliance. Moreover, companies increasingly have contractual commitments that include privacy obligations and compliance with industry standards.

Reputational risks. In addition to legal enforcement, organizations also face reputational harm when they are subject to legal or regulatory proceedings alleging improper practices or inadequate security regarding consumer information, or that they failed to comply with their own announced privacy policies. An organization's most important assets are usually its brand and public trust.

Operational risks. While privacy programs are important to protect consumer information, to be effective they need to be administratively efficient and cost-effective, incorporating the needs of the business as well as the needs of the consumer. Otherwise, the organization may be exposed to unwarranted risk, or the cost of operational inefficiency or dysfunction.

Investment risks. The organization must be able to receive an appropriate return on its investments in information, information technology and information processing programs, in light of evolving privacy regulations, enforcement and expectations.

Compliance programs need to incorporate these risks and balance the needs of a company with those of its consumers and business partners. A growing number of companies have a Chief Privacy Officer, and particularly large ones may have a data privacy and security committee to oversee the increasingly complicated and burdensome challenges of compliance in this area, including educating and training company employees and vendors of their obligations, implementing privacy by design, and developing a culture that fosters awareness and concern about data privacy and security.[697]

Over time, Personal Information management has become vital to a large range of organizations. It is now increasingly common for companies to develop an information management program, in

---

[697] Privacy by design or "PbD," a concept developed by Ontario Canada Information & Privacy Commissioner Dr. Ann Cavoukian, calls for considering ways to protect consumer privacy during the product development process, rather than to address it as an afterthought. For more information visit www.privacybydesign.ca. The FTC and regulators in the E.U. have approved of Dr. Cavoukian's PbD principles and recommended their adoption by industry.

pursuit of a holistic approach to the risks and benefits of processing Personal Information. Common aspects of such programs include maintaining preference lists for direct marketing, developing appropriate security for human resources data, executing proper contracts to authorize data flows particularly when they are being transferred from one country to another, and publishing online privacy notices.

In creating an information management program, each company should have an understanding of what data it collects, stores, process, uses and transfers, and why, and an understanding of the risks associated with its practices. Executives overseeing data privacy and security can then help their organizations develop data privacy policy and practices in an organized way that meets company goals and preserves flexibility, while taking precautions against foreseeable risks. A challenge in doing so is to understand and anticipate future changes both in the regulatory environment and in the company's business needs.

3. Contract and Vendor Management

Many organizations elect to outsource information processing to an outside vendor or plan to sell information collected by the company to a third party. As further outlined below, specific precautions must be taken if a company plans to share personal data with a third-party data processor.

a. Vendor Contracts

A company is responsible for the actions of vendors with which it contracts to collect, analyze, catalog, or otherwise provide data management services on the company's behalf. The claims in a privacy policy also apply to third parties when they are working with an organization's data. To ensure the responsibility and security of data once it is in the hands of a contractor or vendor, precautions to consider incorporating in written contracts include the following:

- Confidentiality provisions.
- No further use of shared information.
- Identification of use of subcontractors and subcontract provisions for information privacy and security.
- Provisions for disclosure of a breach and notification obligations.
- Information security provisions.

b. Vendor Due Diligence

A procuring organization may have specific standards and processes for vendor selection. The following factors should be among those considered when selecting vendors:

- Reputation.
- Financial condition and insurance.
- Information security controls.
- Point of transfer of information
- Disposal of information.
- Vendor employee training and user awareness.

- Vendor incident response.

Consideration of these factors in vendor selection is an important part of any company's efforts to reduce its exposures and mitigate its risk of loss from privacy and security risks involving Personal Information.

Conclusion

These are difficult times for information management, and companies in all lines of business are faced with the need to address information and systems security, and evaluate and ensure their compliance with the growing global network of regulatory and legal requirements governing the collection, usage, disclosure and security of data.

Data breaches of all kinds, and resultant direct and indirect costs, continue to be a growing exposure in our society. Concomitant with that exposure is the increase in state and federal laws and regulations in the U.S., and the increase in regulation in other countries, imposing data security and breach response requirements, particularly when that data includes information about individuals.

Moreover, confidential information of all kinds is increasingly subject to cyber attacks, with resultant business losses to the targeted company and its clients. In addition, new technologies, social media practices, and online behavior tracking practices are raising new privacy issues, with increasing regulatory scrutiny, legislation, and litigation, and resulting exposures to assess and manage.

Companies in all lines of business are subject to these exposures, and to the increasing regulatory and other legal requirements designed to protect the privacy of individuals and the security of information and critical infrastructure.

Contact Information:

Mark E. Schreiber
Chair, Steering Committee
Privacy and Data Protection Group
Edwards Wildman Palmer LLP
111 Huntington Avenue
Boston, MA 02199
+1 617 239 0585
mschreiber@edwardswildman.com

Theodore P. Augustinos
Steering Committee
Privacy and Data Protection Group
Edwards Wildman Palmer LLP
20 Church Street
Hartford, CT 06103
+1 860 541 7710
taugustinos@edwardswildman.com

Laurie A. Kamaiko
Steering Committee
Privacy and Data Protection Group
Edwards Wildman Palmer LLP
750 Lexington Avenue
New York, NY 10022
+1 212 912 2768
lkamaiko@edwardswildman.com

Sarah Pearce
Steering Committee
Privacy and Data Protection Group
Edwards Wildman Palmer LLP
Dashwood, 69 Old Broad Street
London, United Kingdom EC2M 1QS
+44 (0) 20 7556 4503
spearce@edwardswildman.com

Edwards Wildman Palmer LLP's Privacy & Data Protection Group is an inter-disciplinary multi-jurisdictional team of attorneys with considerable experience in addressing matters related to data breaches and the obligations imposed by data protection laws in the US, UK, and other countries, as well as other cyber risk exposures.

The Members of the Steering Committee of the Edwards Wildman Data Protection Group acknowledge with appreciation the invaluable assistance provided by many of the firm's Partners, Counsel, Associates and Trainees in the preparation of this May 2014 edition of our White Paper. Our thanks to David Anderson, Karen Booth, Mark Deem, Jane Elphick, Jonny McDonald, Sharon Monahan, Ari Moskowitz, Matthew Murphy, Stephen Prignano, Nick Secara, Lisa Simmons, David Szabo, Kayla Tabela, Nora Valenza-Frost, and Barry Weissman.