Data Streams: The State of Data Collection and Marketing, Protecting Data, and Responding to Data Breach*

Michael G. Morgan**
Jessica M. Sawyer
Eli A. Alcaraz

** Michael G. Morgan is Of Counsel and Jessica M. Sawyer is an Associate in the Business and Tort Litigation group at Jones Day in its Los Angeles office. Eli A. Alcaraz is an Associate in the New Lawyers Group at Jones Day in its Los Angeles office.

Imagine you are living in 1914. It's a warm spring afternoon and you are craving ice cream, so you head to the local ice cream parlor to get your favorite scoop. You pay for your ice cream. Back then, it is possible that little information was exchanged and no data was created. The data stream was simple and nonaggregative. Now, you are in 2014, same transaction. Your credit card company knows how much you paid and where the transaction occurred. Perhaps you've tweeted or posted a status update to Facebook, now those companies and users know where you were or places you like to visit. If you used a map app on your phone, your gps location is now known. It's possible that the ice cream parlor now has more information about your via a customer loyalty account. The list continues. We are constantly creating data streams in our daily lives. This article examines the use of this data, the obligations placed on entities holding this data, and what should be done in the event of breach of this personal information.

I. Data Collection: It's Growing, It's Keeping Customers, It's Attracting New Ones.

The New York Times Magazine ran a cover story in 2012 titled "How Companies Learn Your Secrets," an in-depth look at consumer data analysis and how companies use predictive marketing techniques. It was merely the tip of the Big Data Iceberg. Headlines in January 2014, showed Big Data has only continued to grow as a topic of conversation: "Big Data in Brazil: the year ahead,"[1] "How the Marine Corps Enlists Big Data for Recruitment Efforts,"[2] and "What Does Big Data Look Like,

---

[1] Angelica Mari, *Big Data in Brazil: a year ahead*, ZD NET, http://www.zdnet.com/big-data-in-brazil-the-year-ahead-7000025093/ (last visited Jan. 16, 2014, 10:32 AM).

[2] *How the Marine Corps Enlists Big Data for Recruitment Efforts*, AD AGE: DATAWORKS, http://adage.com/article/datadriven-marketing/marine-corps-enlists-big-data-recruitment/291009/?utm_source=DataWorks&utm_medium=feed&

Visualization Is Key for Humans."[3] MIT students have created software that analyzes your email history and provides a visual map of your communications.[4] Amazon and Netflix provide new suggestions for movies, books, even steam cleaners, every time you log in to your accounts with them. Smartphone users can check all of their financial activity in one application, which handily suggests new financial products to them based on that activity. Traffic applications collect real-time gps information from millions of drivers. Consumers offer up personal information through any number of websites and applications, much of which is available to companies. In sum, data collection has become ubiquitous.

A. Targeted Marketing to Existing Consumers.

Companies collect growing amounts of data from their customers with many customers freely offering this data on their own accord. This information allows companies not only to contact their customers, but to track consumer habits and preferences, and market accordingly. Consumers are increasingly disinterested in mass-mailed advertisements as they look to companies to provide them with offers and information more closely targeted to the individual. Seventy-eight percent of the respondents in an Infosys survey on digital consumers stated that they would prefer offers tailored to their "interests, wants or needs," and 71% would prefer offers tailored to their location.[5]

Loyalty cards and programs are one of the most common ways to track individual customer's habits. By 2012, American

---

utm_campaign=Feed:+AdvertisingAge/DataWorks, (last visited Jan. 16, 2014, 10:46 AM).

[3] David Hoffer, *What Does Big Data Look Like? Visualization Is Key for Humans*, WIRED http://www.wired.com/insights/2014/01/big-data-look-like-visualization-key-humans/ (last visited Jan. 16, 2014, 10:49 AM),.

[4] https://immersion.media.mit.edu/, (last visited Jan. 16, 2014, 10: 50 AM)).

[5] *Engaging with Digital Consumers: They're Ready, Are You?*, INFOSYS, *available at* http://www.infosys.com/marcom/digital-consumer-study/Engaging-with-Digital-Consumers.pdf,at 5.

consumers had signed up for over 2.5 billion loyalty memberships.[6] Retailers not only use the contact and purchase information gathered from these programs to provide offers or coupons tailored to a specific consumer, but also use aggregate data to drive store-wide specials and offers, and even determine where to place products within the store.[7]

But companies do not even need to use loyalty cards to collect this kind of information. Every point of contact, from credit card purchases, coupon usage, and survey responses to emailed advertisements and website usage, can be tracked.[8] Information not provided by consumers or inferred from their purchases can often be purchased from other sources, and integrated with a company's own data.[9]

Online shopping provides a built-in process for tracking customers –online retailers commonly process purchases through a user profile set up by the customer. These profiles contain, at the very least, contact information and purchase history, but some retailers store payment information and preferences or "favorites." Amazon is possibly the most well known of these companies, but even small business use similar procedures. This allows a company to track all of a user's purchases over time. Instead of sending blanket email promotions to all of its customers, a company can target specific advertising to each individual.

Even without making purchases or joining loyalty programs, consumers can provide companies with personal information. A consumer gives information by checking-in at a store on Foursquare, posting a tweet or Facebook status update

---

[6] Tyrell Linkhorn, *Retailers use variety of ways to track consumer habits through loyalty programs*, THE BLADE, http://www.toledoblade.com/Retail/2013/08/11/Retailers-use-variety-of-ways-to-track-consumer-habits-through-loyalty-programs.html, (last visited Jan. 16, 2014, 10:54 AM).
[7] *Id.*
[8] Charles Duhigg, *How Companies Learn Your Secrets*, THE NEW YORK TIMES, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all, (last visited Jan. 16, 2014, 10:57 AM).
[9] *Id.*

with the location of a store, or reposting images from a particular brand on Tumblr or Pinterest. This data may be more difficult to gather, but it is freely given by the consumer, and allows a company to interact directly with its consumers.

B. Targeting New Customers.

Social networking platforms, such as Facebook, are increasingly able to offer advertising services that take advantage of the data generated by their users. By advertising through social networking platforms, companies can target specific customers without needing to collect a single data point themselves.

Consumers provide large amounts of information regarding their habits through the ordinary use of online services. For example, over a few hours on a typical Sunday, one of the authors of this piece provided the following information to a major online service provider: (1) that she was going to a concert the following weekend (email), (2) that she was looking for restaurants in Los Angeles (search engine), (3) that she likes cat videos (online video library), (4) directions from her house to a local restaurant (mapping application), (5) the names of many of her friends (social networking platform), and (6) the birthdays of every member of her immediate family (calendar). None of this is information that the author would be comfortable providing directly to a retailer or grocery store, but Google can provide access to the author for those companies. This information is now available to the average company through the online service provider.

Google AdWords is a service providing targeted advertising to consumers using Google web products, including Google's search pages, social networking pages, video services, and email. Advertisements are displayed prominently on these pages based on the content the user is accessing and targets user locations and languages depending upon the preferences set by the

advertiser.[10] The service is a primary revenue generator for Google with total advertising revenues of $42.5 billion in 2012.[11]

Similarly, Facebook carries advertising targeted to user profiles. But it also allows advertisers to increase brand awareness through interactive services and games, which spread from a targeted consumer to his or her online friends through the consumer's activity.[12] Total Facebook revenues from advertising in 2012 were $5 billion.[13] Smaller applications such as Foursquare or Mint allow advertisers to reach targeted groups of users in similar ways. Foursquare allows businesses to advertise to potential customers who are searching for specific keywords in specific locations. Mint's free financial service is sponsored by financial institutions who advertise their account services through the program's personalized recommendations.[14]

In February 2013, as a power outage in Louisiana turned the lights out on the Superbowl, Nabisco's Oreo Cookie Twitter sent out a tweet with an image of an Oreo in shadow, and the message "You can still dunk in the dark."[15] Over 15,000 people retweeted the image, with overwhelmingly positive responses. It's possible that Nabisco earned thousands of new customers.

---

[10] *Success Stories*, GOOGLE: ADWORDS, (last visited Jan. 16, 2014, 11:02 AM), http://www.google.com/adwords/success-stories.html.
[11] *2013 Financial Times*, GOOGLE: INVESTOR RELATIONS, (last visited Jan. 16, 2014, 11:03 AM), http://investor.google.com/financial/tables.html.
[12] *See Adertise on Facebook*, FACEBOOK, (last visited Jan. 16, 2014, 11:06 AM), https://www.facebook.com/advertising/how-it-works.
[13] *See Investor Relations*, FACEBOOK, (last visited Jan. 16, 2014, 11:10 AM), http://investor.fb.com/releasedetail.cfm?ReleaseID=736911.
[14] *See Instant savings? Yes, please.*, MINT, https://www.mint.com/how-it-works/save/, (last visited Jan. 16, 2014, 11:13 AM).
[15] https://twitter.com/Oreo/status/298246571718483968, (last visited Jan. 16, 2014, 11:13 AM).

II. Legal Limits of Data Collection: The United States and European Models.

The rapid pace of technological advances and the widespread adoption of online and cloud services has increased exponentially over the past decade, resulting in the potential for consumer data and tracking metrics largely unimaginable when companies first started to establish their web presences.

A. Consent-Based Model.

In the United States, current consumer data collection is generally governed by a model of information and consent. Websites, and other software which track user data, usually present their policies through a Terms of Use/Service agreement presented to the user at signup/installation. It should be noted that using data for purposes other than those for which consent has been given has begun to attract the attention of the FCC[16] and FTC,[17] with the first fines handed down in 2012.[18]

There has been considerable discussion between privacy advocates, web developers, and the legislature, for example, about what data can be collected. As early at 2009, the Do Not Track[19] draft standard emerged, which requests that web applications disable either their tracking or cross-site user tracking of an

---

16 *See* Amy Schatz, *FCC Proposes Fines Over Data Protection*, THE WALL STREET JOURNAL, http://online.wsj.com/news/articles/SB123552946213366401?, (last visited Jan. 16, 2014, 11:17 AM).

17 *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission, (last visited Jan. 16, 2014, 11:19 AM).

18 Edward Wyatt, *U.S. Penalizes Online Company in Sale of Personal Data*, THE NEW YORK TIMES, http://www.nytimes.com/2012/06/13/technology/ftc-levies-first-fine-over-internet-data.html?_r=1&, (last visited Jan. 16, 2014, 11:20 AM).

19 http://donottrack.us/, (last visited Jan. 16, 2014, 11:20 AM).

individual user. While the user who implements Do Not Track shows a preference to limit tracking activity, participation by visited websites is voluntary and the Digital Advertising Alliance does not require members to honor the standard.[20] California has recently passed Assembly Bill AB 370 requiring commercial websites and online services to disclose how they respond to an Internet browser's "do not track" signals without imposing any requirement to act on preferences.[21]

Web cookies (small pieces of data sent and stored on users' computers from a website the user has visited), when used for tracking, allow advertisers access to users' browsing histories. There are no nationwide requirements for websites to notify visitors of tracking cookies although California Assembly Bill AB 370 will require websites to inform visitors how third parties collect personally identifiable information from consumers who visit those sites.[22] Federal agencies are also limited in their use of tracking cookies with government guidance published on how to disable cookies.[23]

The FTC has provided guidelines and suggested practices for data collection, but with the exception of particular types of data (healthcare, financial, etc), there is no unified regulatory structure for the collection and use of consumer data. This is not necessarily a bad thing, as the development of laws generally lags the development of technology, and a rigid regulatory structure could hinder innovation. But in the absence of such a structure, the consent model means companies must develop their own

---

[20] Loue Mastria, *Digital Advertising Alliance Gives Guidance to Marketers for Microsoft IE10 'Do Not Track' Default Setting*, ADS, http://www.aboutads.info/blog/digital-advertising-alliance-gives-guidance-marketers-microsoft-ie10-%E2%80%98do-not-track%E2%80%99-default-set, (last visited Jan. 16, 2014).

[21] Assemb. B. 370, (Cal. 2013), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

[22] *Id.*

[23] *Web Measurement and Customization Opt-out*, USA.gov, http://www.usa.gov/optout-instructions.shtml, (last visited Jan. 16, 2014, 11:13 AM).

structure for the collection and retention of data that may create a risk to the company by failing to satisfy the protection needs their consumers are looking for or the regulatory limitations that do apply to consumer data.

B. Consent-"Plus" in Europe.

In Europe, the consent model is narrowed slightly, and may be considerably narrowed in the future. Currently, Europe requires that companies provide consumers with enough information about their data collection and processing policies and the purposes for this processing for the consumer to give informed consent to the collection of his or her data.[24] The EU has drafted further legislation to regulate the collection and processing of consumer data, and is moving toward more rights for consumers, such as a right to deletion or transfer of data, the right to access a consumer's own data, and increased requirements for informed consent.[25]

Empirical evidence shows that EU data protection authorities may assess the data privacy policies of a given company to determine whether the polices meet EU standards. Several individual country authorities have sanctioned a major company asserting it failed to comply with the EU framework. The major issues identified include insufficient information provided to consumers and impermissible use of data across services, as well as failure to comply with the obligation to obtain consent for certain types of data collection. It is likely that if these sanctions are successful in forcing change, the data regulation authorities will turn to smaller data collectors, possibly focusing on other American companies doing business with European consumers.

---

[24] *French Data Protection Regulator Levies Maximum Fine Against Google*, INFOSECUIRTY, http://www.infosecurity-magazine.com/view/36367/french-data-protection-regulator-levies-maximum-fine-against-google/, (last visited Jan. 16, 2014, 11:35 AM).
[25] *See Commission proposes a comprehensive reform of the data protection rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm, (last visited Jan. 16, 2014).

Other countries such and Australia and Hong Kong are beginning to regulate other uses of consumer data, such as direct marketing. As consumer data collection and processing becomes increasingly international, it will be critical for companies to carefully follow global regulatory frameworks.

III. Consumer Perception of Data Collection: Growing Comfort.

Some consumers appear quite willing to share personal information with retailers and other companies, if they think they will get a benefit out of it. For example, when Forbes ran an article discussing targeted marketing, many users commented—several of whom were signed in with their real names, with links to their commenter profiles on Forbes.com—were positive about the trend:

> "As a consumer, I (pretty much) like the trend. Sending me a coupon for golf balls is a waste, but sending me a coupon for sailing gear would be a winner."[26]

> "I couldn't agree more. To me this is all about competition and in this case [the company] is doing its best to give you the products you need most. As a software engineer and technology enthusiast I'm happy to see companies doing all they can to make my experience easier and less time consuming."[27]

---

[26] Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES, Comment of Bill Conerly, http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/, (last visited Jan. 16, 2014, 11:41 AM).
[27] *Id.*, Comment of Tom Petracca.

Other consumers are less comfortable with data mining, and make changes to their behavior to try to protect their personal information. Some consumers make purchases only in cash, or on prepaid gift or credit cards.[28] But these consumers appear to be the minority: although nearly 40% of consumers in a 2013 study reported that they see consumer data analysis as "invasive," the next most popular descriptions were "helpful" (35%), "convenient" (33%), "time-saving" (32%) and "good service" (27%). Only 26% of consumers described data analysis as "dangerous."[29]

It seems that consumers are willing to allow companies access to their data, but in return, they expect some increased security. Eighty-two percent of the respondents in the Infosys study said that they expect their banks to use data analysis to protect against fraud, and 76% said that they would consider switching to a competitor who could offer assurances that their financial information would be safer.[30] As consumers become increasingly aware of data security issues, companies may be able to leverage their data privacy and security measures to attract consumers.

Companies should take care not to lose the trust of their consumers. In 2008, CA Technologies released the results of a survey of American opinions about data security. In that survey, only 8% of respondents reported feeling "very confident" that their personal information was safe in the hands of retailers, financial

---

[28] Sarah Kessler, *Think You Can Live Offline Without Being Tracked? Here's What It Takes*, FAST COMPANY, http://www.fastcompany.com/3019847/think-you-can-live-offline-without-being-tracked-heres-what-it-takes, (last visited Jan. 16, 2014, 11:44 AM).

[29] *Engaging with Digital Consumers: They're Ready, Are You?*, INFOSYS, *available at* http://www.infosys.com/marcom/digital-consumer-study/Engaging-with-Digital-Consumers.pdf,at 10.

[30] Ayaz Nanji, *When Consumers Will (and Won't) Share Personal Data [Infographic]*, MARKETINGPROFS, http://www.marketingprofs.com/charts/2013/11512/when-consumers-will-and-wont-share-personal-data-infographic, (last visited Jan. 16, 2014, 11:48 AM).

institutions and the government.[31] There is empirical data that following a data breach, brand ranking drops.[32] Consumers expect security and protection, and are likely to make purchasing decisions based on their sense of security.

IV. Data Security Obligations: A Trend Toward Common Practices and Obligations.

The United States and the European Union exemplify two different schemes for applying data security obligations on those that possess or control sensitive personal information. Obligations to keep data secure in the United States exist in a patchwork of federal and state statutes with many sectors not having specific statutes setting forth obligations with respect to that sector. The European Union approach is more comprehensive in that it issues directives and regulations that apply to the member states.

A. The United States Current Scheme.

This part highlights in a simplified summary, a portion of the data security obligations framework present in the United States. To introduce just how varied the US scheme is, we discuss the Fair Credit Reporting Act of 1970 ("FCRA"),[33] Gramm-Leach-Bliley Act of 1999 ("GLB"),[34] Video Privacy Protection Act of 1988 ("VPPA"),[35] Health Insurance Portability and Accountability Act of 1996 ("HIPPA"),[36] Children's Online Privacy Protection

---

[31] *Only Eight Percent of Americans are 'Very Confident' Their Personal Data is Safe With Retailers, Banks and Governments*, BUSINESS WIRE, *available at* http://investor.ca.com/releasedetail.cfm?releaseid=322475, (last visited Jan. 16, 2014, 11:50 AM).

[32] *See generally* YOUGOVBRANDINDEX, http://www.brandindex.com, (last visited Jan. 16, 2014, 11:51 AM).

[33] 15 U.S.C. §§ 1681 *et seq.* (2012).

[34] 15 U.S.C. §§ 6801—09 (2012).

[35] 18 U.S.C. §§ 2710 *et seq.* (2002).

[36] 42 U.S.C. § 1320d-6 (2012).

Act of 1998 ("COPPA"),[37] Family Educational Rights and Privacy Act of 1974 ("FERPA"),[38] and Driver's Privacy Protection Act of 1994 ("DPPA").[39]

FCRA regulates the collection, dissemination, and use of consumer information, including consumer credit information. With FCRA, Congress sought to "require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[40] The personally identifiable information that the FCRA protects is any information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living to be used in establishing the consumer's eligibility for personal, family, or household credit or insurance and employment purposes.[41]

GLB imposes on financial institutions the obligation to protect nonpublic personal information from foreseeable threats to security and data integrity.[42] GLB requires financial institutions to furnish a written disclosure to consumers at least annually of its policies regarding disclosing nonpublic information to affiliates and nonaffiliated third parties, disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution, and protecting the nonpublic personal information of consumers.[43] GLB requires financial institutions to develop a written security plan that must include designating an employee to manage the safeguards, creating a risk analysis of each department's handling of nonpublic information, developing, monitoring, and testing the program to secure the information, and

---

[37] 15 U.S.C. §§ 6501 *et seq.* (2012).
[38] 20 U.S.C. § 1232g (2012).
[39] 18 U.S.C. §§ 2721 *et seq.* (2012).
[40] 15 U.S.C. § 1681(b).
[41] *Id.* § 1681a (d).
[42] 15 U.S.C. § 6801.
[43] *Id.* § 6803.

keep safeguards current with how information is collected, stored, and used.[44]

VPPA protects renters, purchasers, or subscribers of video tape service providers.[45] Specifically, it prohibits a video tape service provider from knowingly disclosing personally identifiable information, including which specific video materials or services were requested or obtained, of the protected group of individuals.[46] Any affected consumer can bring a civil action against the video service provider for damages not less than $2,500 in addition to punitive damages and attorneys' fees.[47] VPPA also imposes the duty on the video service provider to destroy any personally identifiable information no later than one year after the information is no longer necessary for the purpose it was collected.[48] A question for the future, is whether the VPPA will be applied to online streaming services that process and collect similar data?

HIPPA addresses the security and privacy of health data.[49] HIPPA's Privacy Rule regulates the use and disclosure of "protected health information" held by "covered entities."[50] Protected health information is information that concerns provision of health care, health status, or payment for health care that can be linked to an individual.[51] A covered entity is either a health care provider, a health plan, or a health care clearinghouse. There are instances where it is permissible for a covered entity to disclose protected health information. For example, a covered entity can disclose information to law enforcement as required by law, or to facilitate treatment, payment, or health care operations.

COPPA applies to the online collection of personal information of children under the age of thirteen and applies to any person who operates a website located on the internet or an online

---

[44] 16 C.F.R. 314.
[45] 18 U.S.C. § 2710(a)(1).
[46] *Id.* §§ 2710(a)(3), (b)(1).
[47] *Id.* § 2710(c).
[48] *Id.* § 2710(e).
[49] 42 U.S.C. § 1320d-6.
[50] 45 C.F.R. Part 160; 45 C.F.R. Part 164, Subparts A, E.
[51] *Id.*

service and who collects or maintains personal information from or about the users where the website is operated for commercial purposes.[52] Anyone collecting personal information from a child is required to provide notice on the website of what information is collected, how it is used, and disclosure practices and to obtain parental consent for the collection, use, or disclosure of personal information from children.[53] COPPA requires operators to provide detail of their practices upon parental request and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, and prohibits conditioning a child's participation in a game upon disclosing more information than is necessary to participate in such activity.[54]

FERPA protects the privacy of student education records. FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Any such school is required to allow parents of students who are or have been in attendance at the school the right to inspect and review the education records of their children.[55] It also requires that state educational agencies allow parents of students the right to inspect and review the educational records maintained by a state educational agency.[56]

Finally, DPPA governs privacy and the disclosure of personal information gathered by the Department of Motor Vehicles. The DPPA prohibits any officer, employee, or contractor of the DMV from disseminating any information that identifies an individual, including a photograph, social security number, driver identification number, name, address, phone number, and medical or disability information.[57]

As one can see, the US scheme is sector specific and imposes security obligations based on the individual and the type

---

[52] 15 U.S.C. § 6501.
[53] *Id.* § 6502.
[54] *Id.*
[55] 20 U.S.C. § 1232g.
[56] *Id.*
[57] 18 U.S.C. §§ 2721, 2725(3).

of information available as opposed to an emphasis on the practice of data security.

The FTC has recently initiated a prosecution of a major hotel chain for failure to protect consumers' personal information. The prosecution appears to focus more on the practice of data security than the specific sector. The FTC brought the action under the Federal Trade Commission Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive acts or practices in or affecting commerce, asserting the hotel chain "fail[es] to maintain reasonable and appropriate data security for consumers' sensitive personal information."[58] The FTC alleges that hotel chain has been responsible for creating information security policies for itself and its subsidiaries as well as providing oversight of their information security programs.[59] It alleges the hotels have a system that stores personal information about consumers, including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes.[60] The FTC's complaint quotes the privacy policies or statements disseminated by the hotel chain, which include statements explaining it safeguards customer personally identifiable information, describing its 128-bit encryption of confidential information, and asserting it makes commercially reasonable efforts to create and maintain firewalls.[61] The FTC argues that hotel chain "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and them."[62] The FTC makes ten allegations of the hotel chain's "inadequate data security practices." *Id.* Some of the FTC's allegations include failing to use firewalls, storing payment information in clear readable text, failing to remedy known vulnerabilities on servers, failing to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess, failing to adequately inventory computers connected to its network, and

---

[58] First Amended Complaint ¶ 2, *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.
[59] *Id.* at ¶ 14.
[60] *Id.* at ¶ 15.
[61] *Id.* at ¶ 21.
[62] *Id.* at ¶ 24.

failing to follow proper incident response procedures.[63] The FTC asserts that the breaches led to 619,000 consumer payment card number accounts being compromised and $10.6 million in fraud loss.[64] The FTC claim relies on unfair practices and deceptive acts and it outlines how procedures and actions did not maintain reasonable data security. This prosecution appears to depart from the traditional United States patchwork framework towards an emphasis on the practice of data security procedures.

B. The EU Scheme: Comprehensive.

The EU directive scheme takes a more overarching approach. EU Directive 95-46-EC, also known as the Data Protection Directive, announced in 1995, is designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data.[65] The Directive protects "'personal data' .. . . [which] mean[s] any information relating to an indentified or identifiable natural person ('data subject'); an identifiable person is 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."[66] It applies to all "controllers" which are "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and the means of the processing of personal data."[67] The responsibility for compliance with the Directive is placed on those holding the data.[68] The Directive applies to a controller established in the EU and those that are not established within the EU but process data in the EU.[69] The Directive dictates that personal data should not be processed at all except in certain circumstances.

---

[63] *Id.*
[64] *Id.* at ¶ 40.
[65] Council Directive 95/46, 1995 O.J. (L281) 31 (EC).
[66] *Id.* (art. 2), (L281) 38.
[67] *Id.*
[68] *Id.*
[69] *Id.* (art. 4), (L281) 39.

The first set of circumstances in which processing data is permitted is when the data is "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[70] This is known as legitimate purpose.

The second set of circumstances in which the processing of data is permitted is when: (1) the data subject has given consent, (2) when processing is necessary for the performance of a contract or entering into one, (3) when processing is necessary for compliance with a legal obligation of the controller, (4) when processing is necessary in order to protect the vital interests of the data subject, (5) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of officially authority vested in the controller or in a third party to whom the data are disclosed, and (6) where processing is necessary for the purposes of the legitimate interests pursued by the controller unless overridden by the interest for fundamental rights.[71] This is known as transparency.

The final set of circumstances in which the processing of data is permitted is called proportionality. The data must be processed fairly and lawfully. Processing must be adequate, relevant, and not excessive in relation to the purposes for which they are collected. It must be accurate and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[72]

While the European Union's directive scheme is already more encompassing than the United States, once the European Commission's European General Data Protection Regulation of January 25, 2012,[73] takes effect, the EU scheme will become even more comprehensive and unified. Implementing the regulation

---

[70] *Id.* (art. 6), (L281) 40.
[71] *Id.* (art. 7), (L281) 40.
[72] *Id.* (art. 6), (L281) 40.
[73] *Commission Proposal for Regulation Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century,* COM (2012) 9 final (Jan. 1, 2012).

will further the EU down the path of regulating the practices of data protection instead of regulating specific sectors. The Commission's regulation proposed "a strong and consistent legislative framework across Union policies, enhancing individual's rights."[74] The Commission noted that under Directive 95/46/EC, "data protection are not sufficiently harmonized across Member States . . . [and t]his means that actually exercising such rights is more difficult in some Member States than in others, particularly online."[75] The proposed rules will increase an individual's ability to control their data by requiring consent, giving internet users the right to be forgotten in the online environment, guarantee easy access to one's own data, and reinforce the right to information.[76] The rules will also improve the means for individuals to exercise their rights by strengthening national data protection authorities' independence and powers and enhance administrative and judicial remedies available when data protection rights are violated.[77] The regulation also encourages using privacy enhancing-technologies, privacy-friendly default settings, and privacy certification schemes, and introduces a general obligation for data controllers to notify both data protection authorities and the individuals concerned without undue delay when a data breach occurs.[78] The Commission seeks to create a single digital market across the member states that unify the regulatory environment.[79] To address globalism, the rules define EU law as applicable to data controllers established in developing countries and simplify rules on international transfers. These rules do not apply to one sector over another or one group over another, but are focused on the procedure for protecting all data.

---

[74] *Id.* at 4.
[75] *Id.*
[76] *Id.* at 6.
[77] *Id.*
[78] *Id.*
[79] *Id.* at 8.

V. Data Breach Response: 8 Key Steps.[80]

PC World published a piece labeling 2013 "the year of the personal data breach."[81] Certainly 2013 finished with an unwelcome surprise for a couple American companies that suffered large data breaches at the hands of hackers who obtained the personal and financial information of millions of consumers. These companies will spend months, likely years responding to these breaches. The companies have had to provide consumers, law enforcement, and the media with accurate information, and to regain the trust of their consumers. What follows are eight essential steps for any company engaged in the collection and retention of consumer data.

1. Prepare for the Worst.

No matter how secure your systems, or how minor the types of data you collect, you should prepare for a data breach by

---

[80] Compiled from Chris Preismesberger, *Data Breaches: 10 Common Mistakes That Put Enterprises at Risk*, EWEEK, http://www.eweek.com/security/slideshows/data-breaches-10-common-mistakes-that-put-enterprises-at-risk.html, (last visited Jan. 16, 2014, 12:05 PM); *Common data breach handling mistakes*, HELP NET SECURITY, http://www.net-security.org/secworld.php?id=15681, (last visited Jan. 16, 2014, 12:06 PM); *Data Breach Response Guide*, Experian, *available at* http://www.experian.com/assets/data-breach/brochures/response-guide.pdf; *If Customer Data is Stolen or Lost- What to Do Next*, Better Business Bureau, *available at* http://www.bbb.org/data-security/what-to-do-if-consumer-data-is-stolen/checklists/; Jeff Goldman, *How to Respond to a Data Breach, ESECURITY PLANT,* http://www.esecurityplanet.com/network-security/how-to-respond-to-a-data-breach.html, (last visited Jan. 16, 2014, 12:07 PM); *Responding to a Data Breach: Communications Guidelines for Merchants*, Visa, *available at* http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf.

[81] Tony Bradley, *Why 2013 was the year of the personal data breach*, PCWORLD, http://www.pcworld.com/article/2082961/why-2013-was-the-year-of-the-personal-data-breach.html, (last visited Jan. 16, 2014, 12:10 PM).

assuming that it *will* happen. Create a breach response plan, including:

- Create an internal response team of employees from all different areas of the company, from IT to Legal, PR to Customer Service. Make sure that this team is fully briefed on the response plan.
- Make sure that the company has good legal advice, either from an internal legal department that is comfortable with applicable laws and legislation, or through engagement with expert outside counsel.
- Establish partnerships with external services such as security forensics experts, credit reporting agencies and notification services. Credit reporting agencies can also help you establish a breach response plan.[82] These relationships should be in place before any breach. Will you need to send large mailings to consumers? Set up hotlines? Provide credit reports? Make sure you have these services available on short notice.
- Create a database of contact information, notification requirements, and prepared content for notifications.

2. Put Your Data Breach Team to Work.

Notify your internal response team as soon as a breach is detected. Communication will be extremely important, so this team will take the lead on making sure that both internal stakeholders and outside services are kept in the loop. The team should be integrated across the company, allowing information about the breach to get to those who need it quickly and efficiently, without confusion or misinformation.

---

[82] *Data Breach Response Guide,* Experian*, available at* http://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

3. Document.

When a breach is identified, immediately take steps to stop additional damage. Containing the data breach is critical. Then begin the process of documentation and analysis. Although you should never delay responding to the breach until you have all of the information, you should make it a priority to thoroughly investigate and understand the breach. Not only will you need specific information in order to fulfill legal and regulatory obligations and take steps to prevent future breaches, but you will need to fully document and analyze your response to the breach.

4. Report the Breach.

The legal members of your data response team should prepare a plan to identify and meet all of the legal and regulatory obligations incurred by the breach. Depending on the size and type of the breach, you may be required to report it to state or federal government agencies and credit reporting agencies. You may also want to involve law enforcement, even if you do not have any obligation to report. Reporting information should be part of your Breach Response Plan, so that you can meet the often quite short reporting deadlines. Refer to Section 6 to begin building your database of reporting requirements.

5. Notify Customers.

Notification requirements are determined by the residence of your customers, not your business. You will need to notify consumers in fairly short timeframes (some as short as 30-45 days), and preparation will be key. Section 6 will help you build a database of notification requirements for all of the jurisdictions in which your customers reside. You should already have a basic notification template created as part of your data response plan, and can now tailor them to the specifics of your situation. This is where a standing contract with a data breach notification service may serve you well.

6. Monitor and Update.

Investigating the breach will take time. Convene regular meetings of the breach response team, and make sure that updates go out regularly to all stakeholders, including updates to any notification obligations. Make sure that customer-facing employees are kept up-to-date, and are able to give consumers accurate information and directions.

7. Provide Customers with Information and Protection.

Don't assume that the breach won't be public. You should make sure that information is available to consumers through as many avenues as possible—create web pages to disseminate information and updates, and link them to the pages that your consumers generally access. Provide information in stores and through call centers. Use your partnerships with financial institutions to get information to consumers. If you are able to, provide affected consumers with services—partner with Credit Reporting Agencies such as Experian to provide access to credit reports or credit protection services.[83] Create goodwill by treating the breach seriously and addressing consumer concerns.

8. Be Transparent.

If the breach is big enough, you will not be able to avoid public scrutiny. Even smaller breaches may come to the attention of specific sectors- you do not want to be the company that publicly dismisses security concerns, only to have a breach made public by reporters. Instead, make sure that information about the breach and your response is coming directly from the company. This will allow you to make apologies and explain the steps you are taking to address the breach. Transparency and honesty may allow your company to maintain (or later regain) the trust of your consumers.

---

[83] *Data Breach Response Guide*, Experian, *available at* http://www.experian.com/assets/data-breach/brochures/response-guide.pdf

VI. Data Breach Notification Laws.

A. State Laws.

Data breach notification requirements in the United States are a creature of state law. There is legislation in forty-six states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands that requires entities, both governmental and private, to notify individuals of data breach involving personally identifiable information. The four states without data breach notification legislation are Alabama, Kentucky, New Mexico, and South Dakota. Data breach legislation, if anything, seems to be increasing as at least twenty-three states introduced data breach legislation, eight of those states enacted the legislation, in 2013.[84] States that amended current legislation expanded definitions of "personal information," added new notification requirements, or altered penalties.[85] The case can be made that protecting sensitive personal information is a priority nationwide.

See Appendix A for a table of state data breach notification laws, including information on to whom the laws apply, what triggers a data breach, and what constitutes personal information.

B. International Laws.

Internationally, data breach notification laws are reminiscent of US state data security obligations: many are sector specific. Aside from EU's general comprehensive approach to privacy, very few nations have made an overarching legal obligation to notify in the case of data breach.

---

[84] *2013 Security Breach Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES, (Jan. 10, 2014, 9:20 AM), http://www.ncsl.org/research/telecommunications-and-information-technology/2013-security-breach-legislation635200257.aspx.
[85] *Id.*

See Appendix B for a table of laws, regulations, or decisions within a country that impact or deal with privacy. The chart also outlines whether there is a general legal obligation to notify any affected individuals or a related data protection authority.

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
Alabama	None	N/A	N/A	N/A
Alaska	Alaska Stat. § 45.48.010 *et seq.*	State and local governmental agencies, individuals, and persons employing more than 10 employees.	Reasonable belief of or actual unauthorized acquisition of personal information that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and an unencrypted (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password.
Arizona	Ariz. Rev. Stat. § 44-7501	People or entities that conduct business in the state and that license or own unencrypted personal information.	Unauthorized acquisition or access to unencrypted data that compromises confidentiality or security of the personal information and that is reasonably likely to cause substantial economic loss to the individual.	A first name or initial with a last name and any of the following when unencrypted or unsecured by other means: (1) social security number, (2) nonoperating identification license or driver's license number, or (3) credit/debit/account number with security code or password.
Arkansas	Ark. Code § 4-110-101 *et seq.*	People, businesses, or state agencies that license, own, or acquire computerized personal information.	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password, or (4) medical information when either the name or other personal information is not encrypted.
California	Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*	People, businesses, or state agencies doing business in the state and that license or own computerized personal information.	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and any of the following when unencrypted or unsecured by other means: (1) social security number, (2) nonoperating identification license or driver's license number, (3) credit/debit/account number with security code or password, (4) medical information, or (5) health insurance information.
Colorado	Colo. Rev. Stat. § 6-1-716	People or commercial entities doing business in the state and that license or own computerized personal information.	Unauthorized acquisition of unencrypted data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name of a resident and any of the following when unencrypted, unsecured or not redacted by other means: (1) social security number, (2) identification card or driver's license number, or (3)

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
				credit/debit/account number with security code or password.
Connecticut	Conn. Gen Stat. § 36a-701b	People, businesses, or agencies doing business in the state and that license, own, or maintain computerized personal information.	Unauthorized acquisition or access to media, computerized data, databases, or electronic files containing personal information that is not encrypted or otherwise made unreadable or unusable.	A first name or initial with a last name and (1) social security number, (2) CT identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*	People or commercial entities doing business in the state and that license or own computerized personal information about a resident.	Unauthorized acquisition of unencrypted data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name of a resident and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password when either the name or other personal information is not encrypted.
District of Columbia	D.C. Code § 28-3851 *et seq.*	People or entities doing business in the state and that license or own computerized personal information.	Unauthorized acquisition of (1) electronic or computerized data or (2) equipment or a device containing personal information that compromises confidentiality, security, or integrity of the personal information..	A first name or initial with a last name, or phone number or address and (1) social security number, (2) DC identification card or driver's license number, (3) credit/debit number, (4) any code, number, or combination thereof that provide access to a credit or financial account.
Florida	Fla. Stat. § 817.5681	People, joint ventures, firms, associations, partnerships, syndicates, corporations and all other groups doing business in the state and possessing computerized personal information.	Unauthorized acquisition of data that materially compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name, or middle name and last name and any of the following when unencrypted: (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214	Persons or entities that collects, evaluates, compiles, reports, transfers, assembles, communicates, or transmits personal information for fees	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, (3) credit/debit/account number with security code or

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
		or dues, and state and local agencies.		password, (4) account password or PIN, or (5) any of the above without any portion of the individual's name if it is sufficient to perform identity theft.
Guam	9 GCA § 48-10 *et seq.*	Corporations, estates, LPs, partnerships, business trusts, LLPs, LLCs, associations, joint ventures, governments, organizations, governmental agencies, or any other legal entity.	Unauthorized acquisition or access to unencrypted data that compromises confidentiality or security of the personal information when there is a reasonable belief it will cause or has caused identify theft or fraud.	A first name or initial with a last name and any of the following when unencrypted: (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*	Sole proprietorships, corporations, associations, partnerships, or other groups or any governmental agency that license or own personal information in any form of a Hawaii resident.	Unauthorized acquisition or access to unencrypted data when it creates a risk or harm to a person or it is used or is reasonably likely to be used illegally.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Idaho	Idaho Stat. §§ 28-51-104 to -107	Persons, commercial entities, or agencies doing business in the state that license or own personal information about a resident.	Illegal acquisition of unencrypted data that materially compromises confidentiality, security, or integrity of the personal information.	A resident's first name or initial with a last name, or middle name and last name and any of the following when unencrypted: (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Illinois	815 ILCS §§ 530/1 to 530/25	Any data collectors (further defined) that license or own personal information about a resident.	Unauthorized acquisition of unencrypted data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name, or middle name and last name and any of the following when unencrypted: (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*	Persons, business trusts, corporations, trusts, associations, partnerships, estates, nonprofit	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal	An unencrypted social security number, or a first name or initial with a last name and any of the following when unencrypted: (1) identification

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
		organizations , cooperatives, or state or local agencies that license or own personal information.	information.	card or driver's license number, (2) credit card number, or (3) debit/financial account number with security code or password.
Iowa	Iowa Code §§ 715C.1, 715C.2	Persons, business trusts, corporations, trusts, associations, partnerships, LLCs, joint ventures, estates, nonprofit organizations, cooperatives, governmental agencies, public corporations or other legal or commercial entities that license or own personal information about a resident.	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name, or middle name and last name and any of the following when not encrypted: (1) social security number, (2) driver's license number or other unique ID number created by a government body, (3) credit/debit/account number with security code or password, (4) unique electronic identifier or routing code that allows access to financial account, or (5) unique biometric data.
Kansas	Kan. Stat. § 50-7a01 *et seq.*	Persons, corporations, estates, partnerships, trusts, associations, cooperatives, government or agencies doing business in the state that license or own personal information.	Unauthorized acquisition of or access to unencrypted data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and any of the following when unencrypted: (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Kentucky	None	N/A	N/A	N/A
Louisiana	La. Rev. Stat. § 51:3071 *et seq.*	Persons, partnerships, sole proprietorships, corporations, joint ventures, joint stock companies, agencies, or any other legal entity doing business in the state that license or own personal information.	A compromise of the confidentially, security, or integrity of personal information when there is a reasonable basis to conclude there is unauthorized acquisition of the personal information.	A first name or initial with a last name and any of the following when unencrypted: (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
Maine	Me. Rev. Stat. tit. 10 § 1347 *et seq.*	Persons, corporations, LLCs, estates, trusts, partnerships, associations or other entities that collect, evaluate, compile, report, transfer, assemble, or transmit personal information for fees or dues.	Unauthorized acquisition, use, or release of personal information that compromises the confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, (3) credit/debit/account number with security code or password, (4) account passwords or access codes, or (5) any of the above without a name if it is sufficient to perform identity theft when any of the

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
				above information is not encrypted.
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.*; Md. State Govt. Code §§ 10-1301 to -1308	Sole proprietorships, corporations, partnerships, associations, or any other businesses that license or own personal information.	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and any of the following when unencrypted, unsecure, or not redacted by another means: (1) social security number, (2) driver's license number, (3) credit/debit/account number with security code or password, or (4) individual taxpayer ID.
Massachusetts	Mass. Gen. Laws § 93H-1 *et seq.*	Persons, associations corporations, partnerships or other legal entities, or any agency, department, board, commission, executive office, bureau, division or state authority, or any subdivision thereof that license, maintain, own, or store personal information.	Unauthorized acquisition or use of unencrypted data, or encrypted data with the accompanying key, that compromises confidentiality, security, or integrity of the personal information and creates a substantial risk of identity theft or fraud against a resident.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, or (3) credit/financial account number with security code or password.
Michigan	Mich. Comp. Laws §§ 445.63, 445.72	Persons, corporations, LLCs, partnerships, associations, or other legal entities, or any department, commission, office, board, agency, authority, or unit of state government that license or own personal information about a resident.	Unauthorized acquisition of and access to data that compromises confidentiality or security of the personal information.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/demand deposit/financial account number with security code or password.
Minnesota	Minn. Stat. §§ 325E.61, 325E.64	Persons or businesses doing business in the state that license or own personal information.	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password when not encrypted or secured by another means.
Mississippi	Miss. Code § 75-24-29	Persons doing business in the state that license, own, or maintain personal information about residents.	Unauthorized acquisition of media, computerized data, databases, or electronic files containing personal information that is not	A first name or initial with a last name and any of the following when unencrypted or unsecured by other means: (1) social security number, (2) identification card or driver's license

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
			encrypted or otherwise made unreadable or unusable.	number, or (3) credit/debit/account number with security code or password.
Missouri	Mo. Rev. Stat. § 407.1500	Persons, business trusts, corporations, trusts, associations, partnerships, estates, LLCs, joint ventures, cooperatives, government, governmental subdivisions or agencies or instrumentalities, or other legal or commercial entities doing business in the state that license or own personal information about a resident.	Unauthorized acquisition of or access to data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and any of the following when unencrypted or unsecured by other means: (1) social security number, (2) driver's license number or unique identification number created by a government body, (3) credit/debit/account number with security code or password, (4) medical information, (5) unique electronic identifier or routing code that allows access to financial account, or (6) health insurance information.
Montana	Mont. Code § 2-6-504, 30-14-1701 *et seq*.	Persons or businesses doing business in the state that license or own personal information.	Unauthorized acquisition of data that materially compromises confidentiality, security, or integrity of the personal information and causes or is reasonably believed to cause loss or injury to a resident.	A social security number; A name, signature, address, or phone number with (1) passport number, (2) state identification, tribal, or driver's license number, (3) insurance policy number, (4) credit/debit/account number, or (5) passwords or PINs required to access an individual's finances.
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807	Persons, corporations, business trusts, trusts, estates, partnerships, government agencies, LLPs, LPs, LLCs, associations, joint ventures, organizations, governmental subdivisions, agencies, and instrumentalities, or other legal entity doing business in the state that license or own personal information.	Unauthorized acquisition of encrypted data that compromises confidentiality, security, or integrity of the personal information.	A first name or initial with a last name of a resident and (1) social security number, (2) identification card or driver's license number, (3) credit/debit/account number with security code or password, (4) unique electronic identifier or routing code that allows access to financial account, or (5) unique biometric data when either the name or the personal information are not encrypted or secured by another means.
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183	Governmental agencies, institutions of higher education, financial institutions, retail operators,	Unauthorized acquisition of data that materially compromises confidentiality, security, or integrity of the	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account

Appendix A

State	Statute	Applies to	Data breach Trigger	Personal Information Covered
		corporations, or any other type of business that license or own personal information.	personal information.	number with security code or password when the name and the data are not encrypted.
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21	Persons, trusts, corporations, incorporated or unincorporated associations, LLCs, or other entities, or agencies, boards, courts, authorities, divisions, commissions, departments, institutions, bureaus, or other estate governmental agencies doing business in the state that license or own personal information.	Unauthorized acquisition of data that compromises confidentiality or security of the personal information.	A first name or initial with a last name and (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password when either the name or other personal information is not encrypted.
New Jersey	N.J. Stat. § 56:8-163	The state and any political subdivisions, sole proprietorships, corporations, associations, partnerships, or other entities, any other state, the United States, or any other country doing business in the state that maintain or compile personal information.	Unauthorized access to media, data, or electronic files that compromises confidentiality, security, or integrity of personal information when the information is not encrypted or made unreadable or unusable.	A first name or initial with a last name and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password.
New Mexico	None	N/A	N/A	N/A
New York	N.Y. Gen. Bus. Law § 899-aa, N.Y. Stat. Tech. Law 208	Persons, businesses, or state entities (with some exceptions) doing business in the state that license or own private information.	Acquisition without valid authorization or unauthorized acquisition of data that compromises the confidentiality, security, or integrity of private information.	A name, number, personal mark, or other identifier and (1) social security number, (2) identification card or driver's license number, or (3) credit/debit/account number with security code or password when either the personal information is not encrypted or is encrypted and the encryption key was also acquired.
North Carolina	N.C. Gen. Stat. § 75-61, 75-65	Sole proprietorships, corporations, associations, partnerships, or other groups, but not including any	Unauthorized acquisition of or access to unencrypted personal information that crates a material risk of harm	A first name or initial with a last name and (1) social security number, (2) identification card, driver's license, or passport number, (3)

Appendix A

State	Statute	Applies to	Data breach Trigger	Personal Information Covered
		government or governmental agency doing business in the state that license or own personal information.	to the individual or when illegal use has occurred or is reasonably likely to occur.	checking/savings/credit/debit card numbers, (4) PINs, (5) digital signatures, (6) any information that can be used to access financial resources, (7) biometric data, or (8) fingerprints.
North Dakota	N.D. Cent. Code § 51-30-01 *et seq*.	Any entity that does business in the state that licenses or owns personal information.	Unauthorized acquisition of personal information that is not encrypted or secured by other means to make it unreadable or unusable.	A first name or initial with a last name and (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password, (4) date of birth, (5) maiden name of the individual's mother, (6) medical information, (7) health insurance information, (8) an identification number assign to the individual by the employer, or (9) electronic signature. when the name and other personal information are not encrypted.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192	Persons, business trusts, corporations, trusts, estates, partnerships, or associations doing business in the state that license or own personal information.	Unauthorized acquisition of or access to data that compromises the confidentiality or security of the personal information and is reasonably believed to have caused or reasonably believed to cause a material risk of identity theft or other fraud.	A first name or initial with a last name and any of the following when not unencrypted or unreadable: (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password.
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166	Corporations, estates, LPs, business trusts, partnerships, LLPs, LLCs, joint ventures, organizations, associations, government, governmental agencies, subdivisions, or instrumentalities or other legal entities that license or own personal information about residents.	Unauthorized acquisition of or access to unencrypted data that compromises the confidentiality or security of personal information and causes or reasonably will cause identity theft or other fraud on the individual.	A first name or initial with a last name of a resident and any of the following when unencrypted or not redacted: (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password.
Oregon	Oregon Rev. Stat. § 646A.600 *et seq*.	Persons, corporations,	Unauthorized acquisition of	A resident's first name or initial with a

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
		cooperatives, partnerships, estates, LLCs, associations, organizations or other entities that maintains, owns or otherwise possesses personal information.	data that materially compromises the confidentiality, security, or integrity of personal information.	last name and (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password, (4) ID number issued by foreign nation, or (5) passport or other US-issue ID number when either the name or other personal information is not encrypted or is encrypted but the encryption key has also been acquired.
Pennsylvania	73 Pa. Stat. § 2301 *et seq.*	Any state agency, political subdivision, person, or business doing business in the state that manages, maintains, or stores personal information about residents.	Unauthorized acquisition of or access to unencrypted data that materially compromises the confidentiality or security of the personal information and causes or reasonably will cause loss or injury to any resident.	A first name or initial with a last name of a resident and any of the following when unencrypted or not redacted: (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password.
Puerto Rico	10 Laws of Puerto Rico § 4051 *et seq.*	Any entity that is the custodian or owner of personal information about residents.	Unauthorized access to data that compromises the confidentiality, security, or integrity of personal information.	A first name or initial with a last name and any of the following when unencrypted: (1) social security number, (2) voter identification, driver's license, or other official identification number, (3) any bank or financial account numbers, (4) usernames and passwords to private or public information systems, (5) medical information, (6) tax information, or (7) work-related evaluations.
Rhode Island	R.I. Gen. Laws § 11-49.2-1 *et seq.*	State agencies, corporations, joint ventures, and partnership associations that license, maintain, or own personal information.	Unauthorized acquisition of unencrypted data that compromises confidentiality, security, or integrity of personal information.	A first name or initial with a last name of a resident and (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password when either the name or personal information are not encrypted.
South Carolina	S.C. Code § 39-1-09, 2013 H.B. 3248	Persons, corporations, trusts,	Unauthorized acquisition of	A first name or initial with a last name

Appendix A

State	Statute	Applies to	Data breach Trigger	Personal Information Covered
		partnerships, estates, cooperatives, associations, government or governmental agencies doing business in the state that license or own personal information.	or access to unencrypted data that compromises confidentiality, security, or integrity of personal information when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm.	of a resident and any of the following when unencrypted: (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password, or (4) other information that may be used to access financial accounts or used by governmental or regulatory entities for identification.
South Dakota	None	N/A	N/A	N/A
Tennessee	Tenn. Code § 47-18-2107	Persons or businesses doing business in the state and any state agency or subdivision that license or own personal information.	Unauthorized acquisition of unencrypted data that materially compromises the confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and (1) social security number, (2) driver's license number, or (3) credit/debit/account number with security code or password when either the name or other personal information is not encrypted.
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053, Tex. Ed. Code § 37.007(b)(5)	Persons doing business in the state that license or own sensitive personal information.	Unauthorized acquisition of unencrypted data, or encrypted data if the accessing person has the decryption key, that materially compromises the confidentiality, security, or integrity of the personal information.	A first name or initial with a last name and (1) social security number, (2) government identification or driver's license number, or (3) credit/debit/account number with security code or password when both the name or data are not encrypted.
Utah	Utah Code §§ 13-44-101 *et seq.*	Entities that license or own personal information about residents.	Unauthorized acquisition of data that compromises the confidentiality, security, or integrity of personal information.	A first name or initial with a last name and (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password when either the name or other personal information is not encrypted or rendered unreadable by other means.
Vermont	Vt. Stat. tit. 9 § 2430, 2435	Any data collector, including but not limited to, the state and its agencies, LLCs, corporations, retail operators, and financial institutions that	Unauthorized acquisition of or a reasonable belief of unauthorized acquisition that compromises the confidentiality, security, or	A first name or initial with a last name and (1) social security number, (2) nondriver identification or driver's license number, (3) credit/debit/account number with

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
		license or own personal information about a resident.	integrity of personal information.	security code or password, or (4) account passwords or PINs to financial accounts when either the name or other personal information is not encrypted nor rendered unreadable by other means.
Virgin Islands	V.I. Code § 2208	Agencies that license or own personal information about a resident.	Unauthorized acquisition that compromises the confidentiality, security, or integrity of personal information.	A first name or initial with a last name and (1) social security number, (2) driver's license number, or (3) credit/debit/account number with security code or password when either the name or other personal information is unencrypted.
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05	Persons, business trusts, partnerships, corporations, estates, LLPs, LPs, LLCs, organizations, joint ventures, associations, governmental agencies or instrumentalities and other legal entities that license or own personal information.	Unauthorized acquisition of or access to unencrypted data that compromises the confidentiality or security of the personal information and is reasonably believed to have caused or reasonably will cause a material risk of identity theft or other fraud.	A first name or initial with a last name and any of the following when unencrypted: (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password.
Washington	Wash. Rev. Code § 19.255.01, 42.56.590	Any state or local agency, or persons or businesses doing business in the state that license personal information.	Unauthorized acquisition of data that compromises confidentiality, security, or integrity of personal information.	A first name or initial with a last name and (1) social security number, (2) state identification or driver's license number, or (3) credit/debit/account number with security code or password when either the name or other personal information is not encrypted.
West Virginia	W.V. Code §§ 46A-2A-101 *et seq*.	Persons, business trusts, partnerships, estates, corporations, LPs, LLCs, LLPs, joint ventures, associations, organizations, governmental agencies or any other legal entity that license or own personal information.	Unauthorized acquisition of or access to unencrypted data that compromises the confidentiality or security of the personal information and is reasonably believed to have caused or reasonably will cause identity theft or other fraud.	A first name or initial with a last name and any of the following when unencrypted: (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password.
Wisconsin	Wis. Stat. § 134.98	The state and any body in state government and	Unauthorized acquisition when the entity is in the state	A first name or initial with a last name and any of the following when

Appendix A

STATE	STATUTE	APPLIES TO	DATA BREACH TRIGGER	PERSONAL INFORMATION COVERED
		persons doing business in the state, licensing personal information in the state, residing in the state, or lending money to a resident of the state.	and unauthorized acquisition of data of a resident when the entity is located outside of the state but has its principal place of business in the state.	unencrypted or unsecured by another means: (1) social security number, (2) nonoperating identification license or driver's license number, (3) credit/debit/account number with security code or password, (4) DNA profile, or (5) unique biometric data.
Wyoming	Wyo. Stat. § 40-12-501 *et seq*.	Persons or commercial entities doing business in the state that license or own personal information about a resident.	Unauthorized acquisition of data that materially compromises the confidentiality, security, or integrity of the personal information and causes or reasonably causes loss or injury.	A first name or initial with a last name and (1) social security number, (2) state identification or driver's license number, (3) credit/debit/account number with security code or password, (4) tribal identification card, or (5) federal or state government-issued ID when either the name or other personal information is not encrypted.

Appendix A

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
Argentina	Section 43 of the Constitution; Law No. 25,326 and Reg. Decree No. 1558/2001; Law No. 25, 326 Section 9; Section 117 bis and 157 bis of the Criminal Code; Dispositions Nos. 2/2005, 7/2005, 11/2006, 10/2008, 4/2009.	No	No	DPA must keep track of any security incidents of which it learns.
Australia	Privacy Act (Cth) 1988; Privacy Amendment (Enhancing Privacy Protection) Act (Cth) 2012.	No	No	Introduced legislation in 2013 proposing requirement of notification of significantly affected individuals where reasonable risk of harm.
Austria	Protection of Personal Data (DPA 2000) Federal Act.	Yes, must notify immediately if data was seriously and systematically misused and harm may occur.	No	Special notification requirements exist for telecom and internet service providers.
Belgium	Data Protection Act of December 8, 1992; Electronic Communications Act of June 13, 2005.	No	No	Telecom industry data controllers must notify Belgian Institute for Postal Services and Telecommunications immediately upon breach; Must also notify the affected subscriber.
Bosnia and Herzegovina	Official Gazette of Bosnia and Herzegovina 49/06 and 76/11.	No	No	An individual may file a complaint with the DPA.
Brazil	Constitution; Consumer Defense Code; Criminal Code; Civil Code.	No	No	It is highly advised to notify individuals about security breaches especially if the individual is considered a consumer.
Canada	Alberta: Personal Information Protection Act, S.A. 2003, c. P-65; Manitoba: PIPITPA, S.M. 2013, c. 17; Ontario: PHIPA, S.O. 2004, c. 3 Sch. A.; Newfoundland and Labrador: PHIA, S.N.L. 2008, c. P-7.01; New Brunswick: PHIPAA, S.N.B. 2009, c. P-7.05; Nova Scotia: PHIA, S.N.S. 2010, c. 41.	No	No	Alberta: if required by Privacy Commissioner of Alberta; Ontario, Newfoundland and Labrador, New Brunswick, and Nova Scotia: for health-related personal information; Manitoba (PIPITPA): will require notification once in affect.
Chile	Personal Data Act Law No. 19,628; Law No. 20,575.	No	No (no authority exists)	Individuals enforce the law individually; Advisable to consider notification to limit potential damages under civil law.
China	PRC Constitution; General Principles of	No	No	Guidance for data security present in the Information

Appendix A

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
	the Civil Law of the PRC; Tort Liability Law of the PRC; PRC Criminal Law and Amendment VII; Rules Regarding the Protection of Personal Information of Telecommunications and Internet Use adopted July 16, 2013; Regulations on Credit Reporting Industry effective March 15, 2013; Interim Measures on Management of Personal Credit Information Basic Database effective October 1, 2005; Measures for Supervision and Administration of Credit Card Business of Commercial Banks effective January 13, 2011; Statistics law of the PRC effective January 1, 2010; Residential Identify Card Law of the PRC effective January 1, 2004; Social Insurance Law of the PRC effective July 1, 2011; Passport law of the PRC effective January 1, 2007.			Security Technology Guideline for Personal Information Protection within Information Systems for Public and Commercial Services (GB/Z 28828-2012); Specific obligations on telecommunications and internet services, and banking and finance.
Colombia	Constitution Art. 15; Statutory Laws 1266 (2008), 1581 (2012), and 1273 (2009).	No	Yes, statutory Law 1581 (2012) Articles 17(n) and 18(k) require notice to Superintendence of Industry and Trace.	N/A
Czech Republic	Act No. 101/2000 Coll., on Protection of Personal Data; Act. No. 127/2005 Coll., on Electronic Communications.	No	No	Obligation to notify DPA and individual only in electronic communications.
Denmark	Danish Act on Processing of Personal Data ("APPD"), cf. Act No. 429 of May 13, 2000; Guidelines issued by Danish Data Protection Agency.	No obligation under APPD, but caselaw says notification is good practice.	No	Specific notification requirements for public electronic communications services.
Finland	Act 516/2004.	No	No	Must notify users/subscribers of telecommunications services if specific violation or risk of violations; Only applies to telecommunications operators.
France	Act No. 78-17 of January 6, 1978.	No	No	Under certain conditions in public electronic communications there is legal obligation to notify

Appendix A

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
				individual and DPA.
Germany	German Federal Data Protection Act ("BDSG") Sections 42a, 43(2) ¶ 7, and 44; Telemedia Act ("TMG") Section 15a; Telecommunication Act ("TKG") Sections 93(3) and 109a(1).	No	No	Obligations arise to notify the individual and the DPA depending on the severity of the breach and the type of data; Applies to data controller irrespective of location of affected data subjects.
Greece	Law 2472/1997; Law 3471/2006.	No	No	Special obligations under Law 3471/2006 Art. 12, ¶ 5 imposed on electronic communications sector to notify DPA in event of a breach; Under ¶ 6 of same article, if data breach may have detrimental consequences on individual, then most notify individual; No individual notification if controller proves to authorities it had appropriate security.
Hong Kong	Personal Data (Privacy) Ordinance (Cap 486) enacted in 1995.	No	No	DPA issued guidance note that it is prudent and advisable to notify individuals after breach.
India	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.	No	No	N/A
Ireland	Personal Data Security Breach Code of Practice; European Communities (Electronic Communications Networks and Services); (Privacy and Electronic Communications) Regulations 2011; Data Protection Acts of 1988 and 2003.	No	No	Under the nonbinding Personal data Security Breach Code of Practice (applies to all data controllers), data controller must consider whether to notify individuals and must notify DPA baring three exceptions; Privacy and Electronic Communications Regulations 2011 imposes legal obligation on electronic communications service to notify individuals if likely to adversely affect them; No notice needed if data protection measures make data unintelligible;
Israel	Protection Privacy Law of 1981.	No	No	N/A
Italy	Legislative Decree 196/2003 "Personal Data Protection Code"; "Provisions in the matter of flows of banking information and tracking of banking operations" of May 12, 2011; "Guidelines in the matter of implementation of the provisions on data	No	No	Sector specific obligations to notify individuals and the DPA in banks and financial institutions, and public electronic communications providers.

Appendix A

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
	breach notifications – Public consultation" of July 26, 2012; "Implementing measures with regard to the notification of personal data breaches" of April 4, 2013.			
Japan	Act on the Protection of Personal Information ("APPI").	No	No	APPI Art. 20 provides that a business operator handling personal information must take necessary measures to prevent leakage, loss, or damage, and may be interpreted to legally require individual notification.
Luxembourg	Protection of Persons with regard to Processing of Personal Data law of August 2, 2002; Specific Provisions for the Protection of Persons with regard to the Processing of Personal Data of May 30, 2005 in the electronic communications sector.	No	No	Obligation in the electronic communications sector to notify individuals and the DPA.
Malaysia	Personal Data Protection Act 2010; Credit Reporting Agencies Act 2010.	No	No	N/A
Mexico	Federal Law for the Protection of Personal data in Possession of Individuals; Regulations of the Federal Law for the Protection of Personal Data in Possession of Individuals; Sector specific laws (General Health Law, Regulations on general Health Law, etc.).	Yes, Federal Law for the Protection of Personal Data in Possession of Individuals in Mexico Art. 20 and the Regulations of the Mexican data Privacy Law Art. 64 impose obligation when breach affects the financial and moral rights of the individual.	No	Data breach notification law is not dependent on the data subject being a Mexican national, so it may be applied to a data controller outside of Mexico.
Netherlands	Personal Data Protection Act; Telecommunications Act.	Yes (limited)	Yes (limited)	Telecoms must notify the DPA of all incidents that put individuals at risk, and must notify the individuals as well unless information is sufficiently encrypted; Banks and other financial institutions must report incidents to the Netherlands authority for the Financial Markets and the Nederlansche Bank.

Appendix A

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
Norway	Personal Data Act of April 14, 2000 No. 31; Personal Data Regulations of December 15, 2000 No. 1265.	No	Yes, businesses and enterprises processing personal data must notify DPA.	N/A
Peru	Peruvian Personal Data Protection Act (Ley 297733, Ley De Protección de Datos Personales).	No	No	N/A
Philippines	Republic Act No. 10173 (Data Privacy Act of 2012) engaged on August 15, 2012; Republic Act No. 8792 (Electronic Commerce Act of 2000); Republic Act No. 2382 (Medical Act of 1959) Section 24(12); Republic Act No. 8504 (AIDS Prevention and Control Act) Section 30; Republic Act No. 7277 (Magna Carta of Disabled Persons) Section 33 may apply.	No	No	Once National Privacy Commission is established, Republic Act No. 10173 (Data Privacy Act of 2012), Sec. 20(f) will required notification to the commission when sensitive personal information may be used for identify fraud and there is a belief of a risk of serious harm.
Portugal	Data Protection Law, Law 67/98 implementing Directive 95/46/EC; Communications Privacy Law, Law 46/2012 implementing Directive 2009/136/EC.	No	No	Obligations imposed only on electronic communications providers.
Russia	Federal Law No. 152-FZ "On Personal Data" of July 27, 2006.	No	No	Personal information controller is required to take immediate measures to remedy the breach.
Serbia	Personal Data Protection Law ("Official gazette of RS", Nos. 97/2008, 104/2009, 68/2012, and 107/2012); Law on the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Official gazette of FRY – International treaties", No. 1/92, "Official gazette of Serbia and Montenegro – International treaties", No. 11/2005, "Official gazette of RS – International treaties", Nos. 98/2008 and 12/2010).	No	No	If the data breach has elements of a crime, then the police must be notified.
Singapore	Personal Data Protection Act of 2012	No	No	It is considered prudent of financial institutions

Appendix A

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
	(Parts III – VII become enforceable in mid-2014); Guidelines and Circulars issued by the Monetary Authority of Singapore ("MAS"); Code of Practice for Competition in the Provision of Telecommunication Services 2012.			regulated by the MAS to notify it of any data breach.
Slovokia	Act No. 122/2013 Coll.	Yes, pursuant to Act No. 428/2002 Coll.	Yes, if the data controller does not act upon the notification provided by a personal data officer, the personal data officer must notify the DPA.	Personal data officers must be appointed in organizations employing five or more individuals.
Slovenia	Personal Data Protection Act (Zakon o varstvu osebnih podatkov; ZVOP-1); Electronic Communications Act (Zakon o elektoniskih komunikacijah; ZEKom-1); Slovenian Criminal Code.	No	No	If the breach constitutes a crime and is detected by a public authority, the authority must file a criminal complaint with the prosecuting authority; Public available electronic communication services must inform the DPA and the individual if the breach may harm the individual.
South Korea	Personal Information Protection Act of March 2011; Personal Information Protection Act ("PIPA"); Act on Promotion of Information and Communications Network Utilization and Information Protection (IT Network Act).	Yes, pursuant to PIPA and IT Network Act.	Yes	The duty to report to any specific DPA arises only if 10,000 people or more are affected.
Spain	Organic Act 15/1999 of December 13, 1999 on the Protection of Personal Data; Royal Decree 1720/2007 of December 21, 2007.	No	Yes, all incidents that put personal data at risk should be reported.	Specific breach notification obligations apply to public electronic communications services.
Sweden	Personal Data Act 1998:204.	No	No	Specific breach notification obligations apply to publicly available electronic communication services with respect to the DPA; Must notify individuals if incident is likely to be detrimental to individuals or DPA requests notification to individuals.
Switzerland	Federal Data Protection Act ("FDPA").	No	No	Obligations may arise from general obligation to mitigate damages, data controller obligation to implement security measures, principle of

Appendix A

COUNTRY	LAWS, REGULATIONS, DECISIONS THAT CONSIDER PRIVACY	GENERAL LEGAL OBLIGATION TO NOTIFY INDIVIDUAL OF DATA BREACH	GENERAL LEGAL OBLIGATION TO NOTIFY DATA PROTECTION AUTHORITY (DPA) OF DATA BREACH	SPECIAL NOTES
				processing personal information in good faith pursuant to Art. 4, ¶ 2 FDPA.
Taiwan	Personal Information Protection Act of Taiwan ("PIPA") and Enforcement Rules	Yes, pursuant to PIPA Art. 12, if personal information is stolen, altered, disclosed, or infringed due to violation of law, then the individual should be notified.	No	N/A
Ukraine	Law of Ukraine "On Personal Data Protection" #2297-VI of June 1, 2009; Criminal Code of Ukraine #2341-III of April 5, 2001; Code of Administrative Offenses #8073-X of December 7, 1984.	No	No	The individual has a right to inform the DPA about the breach and request prosecution to validate his/her rights; DPA has a right to investigate and inspect.
United Kingdom	Data Protection Act of 1998; Privacy and Electronic Communications (EC) Directive Regulations 2003.	No	No	Sector notification requirements for financial services and the public sector that usually require DPA notification; Public electronic communications services must notify DPA of data security breaches.

Appendix B

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
Argentina	Section 43 of the Constitution; Law No. 25,326 and Reg. Decree No. 1558/2001; Law No. 25, 326 Section 9; Section 117 bis and 157 bis of the Criminal Code; Dispositions Nos. 2/2005, 7/2005, 11/2006, 10/2008, 4/2009.	No	No	DPA must keep track of any security incidents of which it learns.
Australia	Privacy Act (Cth) 1988; Privacy Amendment (Enhancing Privacy Protection) Act (Cth) 2012.	No	No	Introduced legislation in 2013 proposing requirement of notification of significantly affected individuals where reasonable risk of harm.
Austria	Protection of Personal Data (DPA 2000) Federal Act.	Yes, must notify immediately if data was seriously and systematically misused and harm may occur.	No	Special notification requirements exist for telecom and internet service providers.
Belgium	Data Protection Act of December 8, 1992; Electronic Communications Act of June 13, 2005.	No	No	Telecom industry data controllers must notify Belgian Institute for Postal Services and Telecommunications immediately upon breach; Must also notify the affected subscriber.
Bosnia and Herzegovina	Official Gazette of Bosnia and Herzegovina 49/06 and 76/11.	No	No	An individual may file a complaint with the DPA.
Brazil	Constitution; Consumer Defense Code; Criminal Code; Civil Code.	No	No	It is highly advised to notify individuals about security breaches especially if the individual is considered a consumer.
Canada	Alberta: Personal Information Protection Act, S.A. 2003, c. P-65; Manitoba: PIPITPA, S.M. 2013, c. 17; Ontario: PHIPA, S.O. 2004, c. 3 Sch. A.; Newfoundland and Labrador: PHIA, S.N.L. 2008, c. P-7.01; New Brunswick: PHIPAA, S.N.B. 2009, c. P-7.05; Nova Scotia: PHIA, S.N.S. 2010, c. 41.	No	No	Alberta: if required by Privacy Commissioner of Alberta; Ontario, Newfoundland and Labrador, New Brunswick, and Nova Scotia: for health-related personal information; Manitoba (PIPITPA): will require notification once in affect.
Chile	Personal Data Act Law No. 19,628; Law No. 20,575.	No	No (no authority exists)	Individuals enforce the law individually; Advisable to consider notification to limit potential damages under civil law.
China	PRC Constitution; General Principles of the Civil Law of the PRC; Tort Liability	No	No	Guidance for data security present in the Information Security Technology Guideline for Personal

Appendix B

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
	Law of the PRC; PRC Criminal Law and Amendment VII; Rules Regarding the Protection of Personal Information of Telecommunications and Internet Use adopted July 16, 2013; Regulations on Credit Reporting Industry effective March 15, 2013; Interim Measures on Management of Personal Credit Information Basic Database effective October 1, 2005; Measures for Supervision and Administration of Credit Card Business of Commercial Banks effective January 13, 2011; Statistics law of the PRC effective January 1, 2010; Residential Identify Card Law of the PRC effective January 1, 2004; Social Insurance Law of the PRC effective July 1, 2011; Passport law of the PRC effective January 1, 2007.			Information Protection within Information Systems for Public and Commercial Services (GB/Z 28828-2012); Specific obligations on telecommunications and internet services, and banking and finance.
Colombia	Constitution Art. 15; Statutory Laws 1266 (2008), 1581 (2012), and 1273 (2009).	No	Yes, statutory Law 1581 (2012) Articles 17(n) and 18(k) require notice to Superintendence of Industry and Trace.	N/A
Czech Republic	Act No. 101/2000 Coll., on Protection of Personal Data; Act. No. 127/2005 Coll., on Electronic Communications.	No	No	Obligation to notify DPA and individual only in electronic communications.
Denmark	Danish Act on Processing of Personal Data ("APPD"), cf. Act No. 429 of May 13, 2000; Guidelines issued by Danish Data Protection Agency.	No obligation under APPD, but caselaw says notification is good practice.	No	Specific notification requirements for public electronic communications services.
Finland	Act 516/2004.	No	No	Must notify users/subscribers of telecommunications services if specific violation or risk of violations; Only applies to telecommunications operators.
France	Act No. 78-17 of January 6, 1978.	No	No	Under certain conditions in public electronic communications there is legal obligation to notify individual and DPA.

Appendix B

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
Germany	German Federal Data Protection Act ("BDSG") Sections 42a, 43(2) ¶ 7, and 44; Telemedia Act ("TMG") Section 15a; Telecommunication Act ("TKG") Sections 93(3) and 109a(1).	No	No	Obligations arise to notify the individual and the DPA depending on the severity of the breach and the type of data; Applies to data controller irrespective of location of affected data subjects.
Greece	Law 2472/1997; Law 3471/2006.	No	No	Special obligations under Law 3471/2006 Art. 12, ¶ 5 imposed on electronic communications sector to notify DPA in event of a breach; Under ¶ 6 of same article, if data breach may have detrimental consequences on individual, then most notify individual; No individual notification if controller proves to authorities it had appropriate security.
Hong Kong	Personal Data (Privacy) Ordinance (Cap 486) enacted in 1995.	No	No	DPA issued guidance note that it is prudent and advisable to notify individuals after breach.
India	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.	No	No	N/A
Ireland	Personal Data Security Breach Code of Practice; European Communities (Electronic Communications Networks and Services); (Privacy and Electronic Communications) Regulations 2011; Data Protection Acts of 1988 and 2003.	No	No	Under the nonbinding Personal data Security Breach Code of Practice (applies to all data controllers), data controller must consider whether to notify individuals and must notify DPA baring three exceptions; Privacy and Electronic Communications Regulations 2011 imposes legal obligation on electronic communications service to notify individuals if likely to adversely affect them; No notice needed if data protection measures make data unintelligible;
Israel	Protection Privacy Law of 1981.	No	No	N/A
Italy	Legislative Decree 196/2003 "Personal Data Protection Code"; "Provisions in the matter of flows of banking information and tracking of banking operations" of May 12, 2011; "Guidelines in the matter of implementation of the provisions on data breach notifications – Public consultation"	No	No	Sector specific obligations to notify individuals and the DPA in banks and financial institutions, and public electronic communications providers.

Appendix B

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
	of July 26, 2012; "Implementing measures with regard to the notification of personal data breaches" of April 4, 2013.			
Japan	Act on the Protection of Personal Information ("APPI").	No	No	APPI Art. 20 provides that a business operator handling personal information must take necessary measures to prevent leakage, loss, or damage, and may be interpreted to legally require individual notification.
Luxembourg	Protection of Persons with regard to Processing of Personal Data law of August 2, 2002; Specific Provisions for the Protection of Persons with regard to the Processing of Personal Data of May 30, 2005 in the electronic communications sector.	No	No	Obligation in the electronic communications sector to notify individuals and the DPA.
Malaysia	Personal Data Protection Act 2010; Credit Reporting Agencies Act 2010.	No	No	N/A
Mexico	Federal Law for the Protection of Personal data in Possession of Individuals; Regulations of the Federal Law for the Protection of Personal Data in Possession of Individuals; Sector specific laws (General Health Law, Regulations on general Health Law, etc.).	Yes, Federal Law for the Protection of Personal Data in Possession of Individuals in Mexico Art. 20 and the Regulations of the Mexican data Privacy Law Art. 64 impose obligation when breach affects the financial and moral rights of the individual.	No	Data breach notification law is not dependent on the data subject being a Mexican national, so it may be applied to a data controller outside of Mexico.
Netherlands	Personal Data Protection Act; Telecommunications Act.	Yes (limited)	Yes (limited)	Telecoms must notify the DPA of all incidents that put individuals at risk, and must notify the individuals as well unless information is sufficiently encrypted; Banks and other financial institutions must report incidents to the Netherlands authority for the Financial Markets and the Nederlansche Bank.
Norway	Personal Data Act of April 14, 2000 No.	No	Yes, businesses and	N/A

Appendix B

Country	Laws, Regulations, Decisions that consider privacy	General Legal Obligation to Notify Individual of data breach	General Legal Obligation to Notify Data Protection Authority (DPA) of Data Breach	Special Notes
	31; Personal Data Regulations of December 15, 2000 No. 1265.		enterprises processing personal data must notify DPA.	
Peru	Peruvian Personal Data Protection Act (Ley 297733, Ley De Protección de Datos Personales).	No	No	N/A
Philippines	Republic Act No. 10173 (Data Privacy Act of 2012) engaged on August 15, 2012; Republic Act No. 8792 (Electronic Commerce Act of 2000); Republic Act No. 2382 (Medical Act of 1959) Section 24(12); Republic Act No. 8504 (AIDS Prevention and Control Act) Section 30; Republic Act No. 7277 (Magna Carta of Disabled Persons) Section 33 may apply.	No	No	Once National Privacy Commission is established, Republic Act No. 10173 (Data Privacy Act of 2012), Sec. 20(f) will required notification to the commission when sensitive personal information may be used for identify fraud and there is a belief of a risk of serious harm.
Portugal	Data Protection Law, Law 67/98 implementing Directive 95/46/EC; Communications Privacy Law, Law 46/2012 implementing Directive 2009/136/EC.	No	No	Obligations imposed only on electronic communications providers.
Russia	Federal Law No. 152-FZ "On Personal Data" of July 27, 2006.	No	No	Personal information controller is required to take immediate measures to remedy the breach.
Serbia	Personal Data Protection Law ("Official gazette of RS", Nos. 97/2008, 104/2009, 68/2012, and 107/2012); Law on the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Official gazette of FRY – International treaties", No. 1/92, "Official gazette of Serbia and Montenegro – International treaties", No. 11/2005, "Official gazette of RS – International treaties", Nos. 98/2008 and 12/2010).	No	No	If the data breach has elements of a crime, then the police must be notified.
Singapore	Personal Data Protection Act of 2012 (Parts III – VII become enforceable in	No	No	It is considered prudent of financial institutions regulated by the MAS to notify it of any data breach.

Appendix B

COUNTRY	LAWS, REGULATIONS, DECISIONS THAT CONSIDER PRIVACY	GENERAL LEGAL OBLIGATION TO NOTIFY INDIVIDUAL OF DATA BREACH	GENERAL LEGAL OBLIGATION TO NOTIFY DATA PROTECTION AUTHORITY (DPA) OF DATA BREACH	SPECIAL NOTES
	mid-2014); Guidelines and Circulars issued by the Monetary Authority of Singapore ("MAS"); Code of Practice for Competition in the Provision of Telecommunication Services 2012.			
Slovokia	Act No. 122/2013 Coll.	Yes, pursuant to Act No. 428/2002 Coll.	Yes, if the data controller does not act upon the notification provided by a personal data officer, the personal data officer must notify the DPA.	Personal data officers must be appointed in organizations employing five or more individuals.
Slovenia	Personal Data Protection Act (Zakon o varstvu osebnih podatkov; ZVOP-1); Electronic Communications Act (Zakon o elektoniskih komunikacijah; ZEKom-1); Slovenian Criminal Code.	No	No	If the breach constitutes a crime and is detected by a public authority, the authority must file a criminal complaint with the prosecuting authority; Public available electronic communication services must inform the DPA and the individual if the breach may harm the individual.
South Korea	Personal Information Protection Act of March 2011; Personal Information Protection Act ("PIPA"); Act on Promotion of Information and Communications Network Utilization and Information Protection (IT Network Act).	Yes, pursuant to PIPA and IT Network Act.	Yes	The duty to report to any specific DPA arises only if 10,000 people or more are affected.
Spain	Organic Act 15/1999 of December 13, 1999 on the Protection of Personal Data; Royal Decree 1720/2007 of December 21, 2007.	No	Yes, all incidents that put personal data at risk should be reported.	Specific breach notification obligations apply to public electronic communications services.
Sweden	Personal Data Act 1998:204.	No	No	Specific breach notification obligations apply to publicly available electronic communication services with respect to the DPA; Must notify individuals if incident is likely to be detrimental to individuals or DPA requests notification to individuals.
Switzerland	Federal Data Protection Act ("FDPA").	No	No	Obligations may arise from general obligation to mitigate damages, data controller obligation to implement security measures, principle of processing personal information in good faith

Appendix B

COUNTRY	LAWS, REGULATIONS, DECISIONS THAT CONSIDER PRIVACY	GENERAL LEGAL OBLIGATION TO NOTIFY INDIVIDUAL OF DATA BREACH	GENERAL LEGAL OBLIGATION TO NOTIFY DATA PROTECTION AUTHORITY (DPA) OF DATA BREACH	SPECIAL NOTES
				pursuant to Art. 4, ¶ 2 FDPA.
Taiwan	Personal Information Protection Act of Taiwan ("PIPA") and Enforcement Rules	Yes, pursuant to PIPA Art. 12, if personal information is stolen, altered, disclosed, or infringed due to violation of law, then the individual should be notified.	No	N/A
Ukraine	Law of Ukraine "On Personal Data Protection" #2297-VI of June 1, 2009; Criminal Code of Ukraine #2341-III of April 5, 2001; Code of Administrative Offenses #8073-X of December 7, 1984.	No	No	The individual has a right to inform the DPA about the breach and request prosecution to validate his/her rights; DPA has a right to investigate and inspect.
United Kingdom	Data Protection Act of 1998; Privacy and Electronic Communications (EC) Directive Regulations 2003.	No	No	Sector notification requirements for financial services and the public sector that usually require DPA notification; Public electronic communications services must notify DPA of data security breaches.