# Data Privacy and Security:

## A Practical Guide for In-House Counsel

## 2017 Edition

David Zetoony

BRYAN CAVE

bryancave.com | A Global Law Firm

# TABLE OF CONTENTS


TABLE OF CONTENTS ..... 2
INTRODUCTION ..... 6
I. Data Privacy ..... 6
A. Data Maps and Data Inventories ..... 6
B. Website Privacy Policies ..... 8
C. Social Security Number Privacy Policies ..... 9
D. Mobile App Privacy Policies ..... 10
E. Privacy Certifications and Trustbrands ..... 11
F. Employer Privacy Policies ..... 12
G. Bring Your Own Device (“BYOD”) Policies ..... 14
H. Employee Monitoring ..... 16
I. Social Media Privacy Concerns ..... 17
J. Online Behavioral Advertising ..... 19
K. Video Viewing Information ..... 20
L. Geo-Location Tracking ..... 21
M. Radio Frequency Identification (“RFID”) ..... 22
N. Email Marketing ..... 24
O. Email Marketing In Canada (CASL) ..... 25
P. Collecting Information From Children ..... 27
Q. Facial Recognition Technology ..... 29
R. Fingerprint Identification Technology ..... 30
S. Passing Data Between Retailers To Facilitate Transactions ..... 31
T. Privacy Due Diligence In A Merger Or Acquisition ..... 33
U. Vehicle Event Data Recorders ..... 34
V. Self-Driving Vehicles ..... 35
W. FTC Tracking Of Privacy Complaints ..... 36
X. Companies Perceived By The FTC as Top Violators ..... 37
Y. Companies Perceived By FTC As Emerging Threats ..... 39
Z. Organizing Data Privacy Within A Company ..... 39
AA. Responding To Government Subpoenas And Document Requests That Ask For Personal Information ..... 41
BB. Responding To National Security Letters That Ask For Personal Information. ..... 42
CC. Responding To Third Party (Non-Government) Civil Subpoenas And Document Requests That Ask For Personal Information ..... 44
II. Data Security ..... 46

A. Written Information Security Policies ..... 46
B. De-Identification, Anonymization, and Pseudonymization ..... 47
C. Encryption ..... 48
D. Document Retention Periods ..... 50
E. Cyber Insurance ..... 51
F. Bounty or Bug Programs ..... 52
G. Cyber-Extortion ..... 54
H. Ransomware ..... 55
I. FDIC Cybersecurity Examinations ..... 56
J. Wire Transfer Fraud ..... 58
K. Tax Filing Fraud ..... 59
L. Incident Response Plans ..... 60
M. Forensic Investigators ..... 61
N. Credit Monitoring Services ..... 63
O. Reputation Management ..... 64
P. Data Breach Notification Laws ..... 65
Q. Cybersecurity Disclosures ..... 66
R. Class Action Litigation Trends ..... 68
S. Credit Cards and the Payment Card Industry Data Security Standard ..... 69
T. Selecting a Qualified Security Assessor ("QSA") ..... 71
U. Negotiating Payment Processing Agreements ..... 72
V. Credit Card Breaches ..... 75
W. Causes of Healthcare Data Breaches ..... 76
X. Healthcare Data Breach Litigation Trends ..... 77
Y. Healthcare Data Breach Enforcements and Fines ..... 78
Z. Healthcare Business Associates ..... 79
AA. Ransomware May Be a Reportable HIPAA Breach ..... 80
BB. How to Develop a HIPAA Incident Response Team ..... 81
CC. Third Party Vendor Management Programs ..... 83
DD. Cloud Computing ..... 84
EE. Sharing Threat Indicators With The Government ..... 86
FF. Security Due Diligence In A Merger Or Acquisition ..... 87
III. Data Transfers From Other Countries ..... 88
A. EU-US Data Transfers ..... 88
B. Privacy Shield ..... 89
C. EU Model Clauses ..... 90

D. EU Binding Corporate Rules ..... 92
E. Data Transfers From Asia ..... 92
GLOSSARY ..... 94
CONTRIBUTORS ..... 96

# ABOUT THE AUTHOR

**David Zetoony** is a partner at Bryan Cave LLP where he leads the firm's international data privacy and security practice. Mr. Zetoony has helped hundreds of clients respond to data security incidents, and has defended inquiries concerning the data security and privacy practices of corporations. He is the author of a leading handbook on data breach response – the Washington Legal Foundation's Data Security Breaches: Incident Preparedness and Response – and the premier research handbooks on data privacy and security class action litigation. He represents clients from a variety of industries ranging from national department stores to international outsourcers.

# INTRODUCTION

Five years ago few legal departments were concerned with – let alone focused on – data privacy or security. Most of those that were aware of the terms assumed that these were issues being handled by IT, HR, or marketing departments.

The world has changed. Data privacy class action litigation has erupted and data security breaches dominate the headlines. It is now well accepted that data privacy and data security issues threaten the reputation, profitability, and, sometimes, the operational survival of organizations. It is therefore perhaps not surprising to find that in almost every survey conducted of boards and senior management, data issues rank as one of their three top concerns, if not their single greatest concern. With that backdrop, organizations increasingly look to general counsel to manage data privacy and security risks.

The result has been that many in-house attorneys unexpectedly find themselves responsible for a topic about which they have little experience or training. Coming up-to-speed can be difficult. There are well over 200 laws (just in the United States) that have data privacy and security implications. It's simply not possible to sit down and read a statute to get caught up.

When we published this handbook for the first time in 2016 in conjunction with the Washington Legal Foundation it received an overwhelming response. In less than a year it had been downloaded by over 3,500 in-house attorneys – attorneys in 194 of the Fortune 500 downloaded it alone. We are extremely proud of the fact that it has become a desk reference for in-house attorneys worldwide.

The 2017 version includes updates to most sections to account for changes in the law and includes a number of new sections dealing with topics that have grown in popularity, or entered the data privacy and security scene. The discussion under each topic is not intended to be a legal treatise. Instead, each section provides a straight-forward overview of the law relevant to that topic, statistics to help understand the issue and benchmark it's importance, and a functional list of bullet points or questions to immediately break down an issue. We hope that the handbook provides useful and practical guidance when addressing data-related issues.

# I. DATA PRIVACY

## A. Data Maps and Data Inventories

Knowing the type of data that you collect, where it is held, with whom it is shared, and how it is transferred is a central component of most data privacy and data security programs. The process of answering these questions is often referred to as a “data map” or a “data inventory.”

Although the questions that a data map tries to solve are relatively straightforward, the process of conducting a data map can be daunting for many organizations. In addition, it is important to remember that data constantly changes. As a result, organizations must consider how often to invest the time to conduct a data map and, once invested, how long the information will be useful.

| No. 1 | 100% | 33% | 17% |
|---|---|---|---|
| Maintaining a data map was ranked as the number one priority by privacy officers.[1] | The percentage of companies that identified maintaining a data map as relevant.[2] | The percentage of companies that have a data map.[3] | The percentage of companies that have a data map and use it to track the flow of data between systems.[4] |

What you should think about when deciding whether to conduct a data map or a data inventory:

1. Which departments within your organization are most likely to have data?

2. Who within each department would you need to speak with to find out what data exists?

3. Is it more efficient to send the relevant people a questionnaire or to speak with them directly?

4. What is the best way to receive information from each person in the organization that collects data so that the information provided can be organized and sorted with information received from others?

5. How much time will it take to complete the data map?

What information should you consider including in your data map:

1. The types of data collected.

2. Where the data is physically housed (*e.g.,* the building or location).

3. Where the data is logically housed (*e.g.,* the electronic location within a server).

4. Whether encryption is applied to the data in transit (*i.e.,* when it is moving). If it is, what encryption standard is being used?

5. Whether encryption is applied to the data at rest (*i.e.,* when it is being stored). If it is, what encryption standard is being used?

6. The custodian of the data (*i.e.,* who is responsible for it).

7. Who has access within the organization to the data.

8. Who has access outside of the organization to the data.

---

1 Nymity, Privacy Management Program Benchmarking and Accountability Report, (2015), https://www.nymity.com/data-privacy-resources/data-privacy-research/privacy-management-benchmarking-report.aspx.

2 *Id.*

3 *Id.*

4 *Id.*

9. Whether the data crosses national boundaries.

10. The retention schedule (if any) applied to the data.

## B. Website Privacy Policies

Although financial institutions, health care providers, and websites directed to children are required to create consumer privacy policies under federal law (see, *e.g.,* section discussing collecting information from children), other types of websites are not. In 2003 California became the first state to impose a general requirement that most websites post a privacy policy.

Under the California Online Privacy Protection Act ("CalOPPA"), all websites that collect personal information about state residents must post an online privacy policy if the information is collected for the purpose of providing goods or services for personal, family, or household purposes.[5] Since the passage of the CalOPPA, most websites that collect information – whether or not they are directed at California residents or are otherwise subject to the CalOPPA – have chosen to post an online privacy policy. Recently, California's Attorney General announced the release of a new form that allows consumers to report potential violations of CalOPPA online. This online reporting tool will increase California's ability to identify and notify entities in violation of CalOPPA.

On January 1, 2016, Delaware followed suit by enacting the Delaware Online Privacy and Protection Act ("DOPPA"). Similar to CalOPPA, DOPPA requires that website and app operators that collect personally identifiable information of Delaware residents conspicuously post a comprehensive privacy policy and conform to other privacy related requirements.[6]

| 2 | 10 minutes | 244 hours | $0.59 |
|---|---|---|---|
| Number of states that require operators of websites that collect PII to disclose a privacy policy.[7] | Average time it takes for a person to read a privacy policy.[8] | The amount of time it would take a person to read the privacy policies of all the unique websites they visit in a year.[9] | The premium that study participants were willing to pay to purchase a $15 item from a website that proactively displayed strong privacy protections from one with no privacy position.[10] |

5 Cal. Bus. & Prof. Code § 22575, *et seq.*

6 6 Del.C. § 1201C, *et seq.*

7 California and Delaware.

8 Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4(3) I/S: A Journal of Law and Policy for the Information Society, 541 (2008).

9 *Id.*

10 Janice Tsai, et al., The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, 6th Workshop on the Economics of Information Security (WEIS), (June 2007), http://www.econinfosec.org/archive/weis2007/papers/57.pdf.

What to think about when drafting or reviewing a privacy policy:

1. Is your organization subject to a federal law that requires that a privacy policy take a particular form, or include particular information?

2. Does the privacy policy describe the main ways in which your organization collects information?

3. Does the privacy policy describe the ways in which your organization shares information with third parties?

4. Does the privacy policy discuss data security? If so, is the level of security indicated appropriate?

5. Would the privacy policy interfere with a possible merger, acquisition, or sale of your organization's assets?

6. Would the privacy policy interfere with future ways in which your organization may want to monetize data?

7. Does the privacy policy use terms that might be misunderstood or misinterpreted by a regulator or a plaintiff's attorney?

8. Does the privacy policy comply with the laws in each jurisdiction in which your organization is subject (*i.e.,* CalOPPA or DOPPA)?

9. Should the privacy policy only govern information collected via your organization's website, or all information collected by your organization?

10. Does the privacy policy appropriately disclose and discuss network marketing and behavioral advertising?

11. Does the privacy policy need to discuss the tracking that your organization may conduct of its clients or website visitors?

12. Could the privacy policy be understood by the average person?

13. Can the privacy policy be easily viewed on a smartphone or a mobile device?

14. Does the policy provide information to users concerning how they can contact your organization about privacy related questions or complaints?

15. Does the policy discuss what information may be modified or changed by a user?

## C. Social Security Number Privacy Policies

Social Security Numbers ("SSN") were originally established by the Social Security Administration to track earnings and eligibility for Social Security benefits. Because a SSN is a unique personal identifier that rarely changes, federal agencies use SSN for purposes other than Social Security eligibility (*e.g.,* taxes, food stamps, etc.). In 1974, Congress passed legislation requiring federal agencies that collect SSN to provide individuals with notice

regarding whether the collection was mandatory and how the agency intended to use the SSN.[11] Congress later barred agencies from disclosing SSN to third parties. Federal law does not, however, regulate private-sector use of SSN.

In response to concerns that SSN can be used to perpetrate identity theft, some state legislatures passed statutes regulating the private sector's use of SSN. Among other things, state statutes often mandate organizations that collect SSN take specific steps to protect SSN such as not printing SSN on consumer cards, sending SSN through the mail, requiring that a consumer transmit SSN unencrypted over the internet, or requiring that individuals use their SSN to access a website without multi-factor authentication. Many states also have statutes that require that companies securely destroy SSN when the information is no longer in use.

| 1936 | $30 | $500 / month |
|---|---|---|
| Year Social Security Numbers were created.[12] | Cost on the black market to obtain a dossier with a consumer's SSN.[13] | Civil penalty imposed by one state for failing to adopt a privacy policy when collecting SSN.[14] |

Some states have gone beyond regulating the use, disclosure, and destruction of SSN and require that organizations that collect SSN publicly post a privacy policy that explains the following:

(1) how the organization collects SSN,

(2) how the organization uses SSN,

(3) who within the organization will have access to SSN,

(4) how the organization will protect SSN, and

(5) the organization's limitations on SSN disclosure.

Other states require organizations to internally publish privacy policies as part of their employee handbook or procedures manual. In addition to the topics listed above, the internal policy must establish penalties for employees that misuse SSN.[15]

## D. Mobile App Privacy Policies

Many of the most popular mobile apps collect personally identifiable information. Although most app developers are not required to display a privacy policy under federal law, they are contractually required to do so pursuant to the terms and conditions of the websites that market most major mobile device applications (*e.g.,* the Apple Store, or Google Play). In

[11] The Privacy Act of 1974, 5 U.S.C. § 552a.

[12] Social Security Administration, The First Social Security Number and the Lowest Number, http://www.ssa.gov/history/ssn/firstcard.html.

[13] Jeanine Skowrinski, What your information is worth on the black market, Bankrate.com, (July 27, 2015), http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx.

[14] Tex. Bus. & Com. Code § 501.052(a), 501.053(a).

[15] Michigan Compiled Laws § 445.84(1)(e), (2).

addition, the California Attorney General has taken the position that applications that collect personal information are required to post a privacy policy pursuant to the CalOPPA discussed in the previous section.

| $2,500 | 11% | >60% |
|---|---|---|
| Possible penalty under California law for each app downloaded without a privacy policy.[1] | Percentage of banking related apps that contain harmful code.[2] | Percentage of popular dating apps vulnerable to hacker exfiltration of PII.[3] |

Consider the following privacy issues when developing a mobile app:

1. **Does the app have a privacy policy?** Privacy policies are a best practice if the app will be used in connection with personally identifiable information. As discussed above, there is also an argument that they may be required if they solicit information from California residents.

2. **Is the app directed to users younger than 13?** Under the Children's Online Privacy Protection Act ("COPPA"), if the app collects information from children it must include a privacy policy as well as comply with additional requirements imposed under that Act. See the section titled Collecting Information From Children for more information.

3. **How is personally identifiable information stored by the app?** Apps can store data in multiple places, including the device, backups of the device, and the app provider's servers. A best practice is for a mobile app's privacy policy to state accurately where personally identifiable information is stored.

4. **Does the app communicate personally identifiable information to others?** A useful privacy policy accurately states whether data that the user provides is relayed to anyone else.

5. **Does the mobile app provider securely communicate any personally identifiable information?** A 2013 study concluded that 18 percent of apps sent usernames and passwords by non-encrypted communications.[4] Consider stating within the app's privacy policy whether the app transmits personally identifiable information, and, if so, whether the information is encrypted in transit.

6. **If the app crashes, does diagnostic data about the crash include personally identifiable information?** Some apps do not transmit personally identifiable information in their normal operation, but diagnostic data may inadvertently capture such information in an unencrypted manner.

## E. Privacy Certifications and Trustbrands

Privacy certifications, or "trustbrands," are seals licensed by third parties for organizations to place on their homepage or within their privacy policy. The seals typically state, or imply, that the organization which has displayed the seal has high privacy or security standards, or has had its privacy or security practices reviewed by a third party. Some seals

also imply that the organization has agreed to join a self-regulatory program that may provide consumers with additional rights, such as a mechanism for resolving privacy-related disputes.

| 92% | 76% | ~50% | 2 |
|---|---|---|---|
| Percentage of consumers that are worried about online privacy.[16] | Percentage of consumers who claim they look for privacy certifications and seals on a website.[17] | Percentage of consumers who say that they would share their interests with advertisers *if* the advertiser's privacy policy was "certified."[18] | The number of agencies the FTC alleged offered deceptive seals.4 |

What to think about when considering whether your organization should purchase a privacy certification:

1. Does the certifying agency have its own privacy or security standards?

2. Do the certifying agency's standards exceed legal requirements?

3. Do your organization's practices meet the certifying agency's standards?

4. If the certifying agency's standards change, is your organization prepared to modify its practices accordingly?

5. Has the certifying agency been investigated by the FTC, or another consumer protection authority, for deceptive or unfair practices?

6. If so, are you confident that the certifying agency's seal and review process is non-deceptive and that association with the agency will not result in negative publicity?

7. Have consumers complained to the FTC about the certifying agency?

8. Does your organization have a mechanism in place to ensure that the license for the seal is renewed each year and/or that the seal is removed from your website if the license expires?

9. Have plaintiff's attorneys used the seal against other organizations by alleging that those organizations agreed to a higher standard of care by adopting the seal?

## F. Employer Privacy Policies

In 2005 Michigan became the first state to pass a statute requiring employers to create an internal privacy policy that governs their ability to disclose some forms of highly sensitive

[16] TRUSTe, TRUSTe 2014 US Consumer Confidence Privacy Report Consumer Opinion and Business Impact, (2014), http://www.slideshare.net/marketing4ecommerce/privacidad-30859419.

[17] *Id.* at 10.

[18] TRUSTe, TRUSTe Privacy index, Advertising Edition – Consumer Interests, (2014), https://www.truste.com/resources/privacy-research/us-consumer-interests-index-2014/.

information about their employees. Michigan's Social Security Number Privacy Act expressly requires employers to create policies concerning the confidentiality of employees' social security numbers ("SSN") and to disseminate those policies to employees. New York adopted a similar statute. Several other states – Connecticut, Massachusetts, and Texas – have statutes mandating the establishment of privacy policies that could also apply in the employer-employee context.

Companies should check whether they have a written policy concerning the use and disclosure of protected employee personal information. If they do not, they should confirm that none of the states in which they operate currently require such a policy or are planning to do so through new legislation.

| 5 | $500 | $275,000 |
|---|---|---|
| The number of states that have enacted statutes that may require employers to create employee privacy policies.[19] | The fine assessed under New York's statute to employers who unlawfully disseminate an employee's SSN.[20] | The damages awarded to a group of Michigan employees who sued their union after it failed to safeguard their SSN.[21] |

What to think about when drafting or reviewing an employee privacy policy:

1. Does the privacy policy capture the main ways in which your organization collects personal information from its employees?

2. Does the privacy policy ensure the confidentiality of employee SSN and other personal information?

3. Does the privacy policy explain how employee SSN and other personal information are protected?

4. Does the privacy policy limit who has access to information or documents that contain employee SSN and other personal information?

5. Does the privacy policy describe how to properly dispose of documents that contain employee SSN and other personal information?

6. Does the privacy policy describe the disciplinary measures that may be taken for violations of the policy?

7. Will the privacy policy be published in an employee handbook, procedures manual, or similar document?

8. Can the average employee understand the privacy policy?

[19] These states are: Connecticut (Conn. Gen. Stat. § 42-471), Massachusetts (201 Mass. Code Regs. 17.03), Michigan (Mich. Comp. Laws § 445.84), New York (N.Y. Lab. Law § 203-d), and Texas (Tex. Bus. & Com. Code Ann. § 501.052).

[20] N.Y. Lab. Law § 203-d(3).

[21] John F. Buckley & Ronald M. Green, State by State Guide to Human Resources Law § 1.36 (2015).

9. Does the privacy policy use terms that might be misunderstood or misinterpreted by a regulator or a plaintiff's attorney?

10. Does the privacy policy comply with the laws in each jurisdiction in which your organization is subject?

## G. Bring Your Own Device ("BYOD") Policies

Many companies permit their employees to use personal mobile devices, such as smartphones and tablets, to access company-specific information, such as email, under a Bring Your Own Device ("BYOD") policy. BYOD policies can be popular for employees that want to use hand-picked devices and for employers that want to avoid the cost of providing, and maintaining, company-owned devices. Nonetheless, the use of company data on non-company devices implicates both security and privacy considerations.

| | | |
|---|---|---|
| 328 million<br>Estimate of the number of people that bring smartphones to work.[22] | 39%<br>Percentage of companies that reported "security concerns" were the main inhibitor to full BYOD adoption.[23] | 40%<br>The percent of companies that offer BYOD to all employees.[24] |
| 72%<br>Percent of organizations that reported data leakage as their main security concern.[25] | 52%<br>Percent of organizations that reported malware as their main security concern.[26] | 39%<br>Percent of organizations with BYOD policies that reported that malware was downloaded via a BYO or corporate owned mobile device.[27] |

Consider the following when deciding upon a BYOD policy:

1. **Is the scope of your organization's control over employees' mobile devices consistent with the organization's interest?** Organizations should consider why they have an interest in knowing about their employees' mobile devices; that interest should be the basis from which a BYOD policy should emerge. If the organization simply wants to allow an employee to access work email on a mobile device, then the policies and restrictions should proceed with that focus.

2. **To what extent and for what purpose does the organization monitor employees' use of mobile devices?** Many servers create logs showing when an

[22] Matt Hamblen, With BYOD smartphones on the rise, IT headaches will become migraines, Computerworld, (January 27, 2014), http://www.computerworld.com/article/2487005/byod/with-byod-smartphones-on-the-rise--it-headaches-will-become-migraines.html.

[23] Crowd Research Partners, BYOD & Mobile Security at 9 (2016), http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf.

[24] Id. at 7.

[25] Teena Hammond, Research: 74 percent using or adopting BYOD, ZDNet, (January 5, 2015), http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/.

[26] Id. at 11.

[27] Id. at 16.

employee's device accessed the organization server using certain authentication credentials. As security measures such logs are often appropriate. To the extent that the organization wants to monitor more substantive actions by an employee on a mobile device, such monitoring should be in line with an appropriate purpose.

3. **What procedures are in place to restrict the transfer of data from the organization's network by way of the mobile device?** Organizations often protect against the risk that organization data will be "floating" on multiple devices by (a) limiting the types of data accessible to mobile devices (*e.g.*, email) and (b) restricting, to the extent possible, how that data can be used on the mobile device (*e.g.*, policies on copying and requiring certain security settings).For example, some organizations use sandboxed applications for accessing work-related email. Such apps open email in a program that is separate and apart from the native email system that is built-into the device and control aspects of the user's experience. For example, they may restrict the user from locally saving any emails, or attachments, to the user's device.

4. **For security purposes, does the organization require a minimum version of the operating system and/or software before an employee can use a mobile device?** Minimum versions ensure that certain security protections and bug fixes are present on the device.

5. **Can data on a mobile device be remotely wiped? By whom?** A best practice for devices that contain confidential or sensitive organization information is to ensure that the data can be remotely deleted from the device by the organization if, for example, the device is stolen or the employee is terminated. To the extent that the employee only accesses work-related data when accessing a sandboxed application, it may be relatively easy to restrict the device from accessing such data remotely. To the extent that an employee was permitted to locally store work-related data (*e.g.,* cache work emails locally, or download attachments), an employer should consider whether it has the right, and technical means, to remotely wipe the entire device.

6. **What procedure is in place for an employee to report a missing mobile device?** Accidents happen to everyone, but their aftermath can determine whether they become catastrophes. Employees should report a missing device to someone – perhaps the IT department or help desk – so that the organization's device removal policy can be followed.

7. **What steps does the organization take to proliferate its mobile device policies?** Organizations often rely on their IT staff, self-help materials, and employee certifications to ensure (a) employee awareness of the organization policies and (b) enforcement of organization policies.

8. **Do the security measures in place match the sensitivity of the data accessed through the mobile device?** For some employees that receive non-sensitive information minimal restrictions may be appropriate. For employees that receive sensitive or confidential information higher restrictions may be appropriate.

9. **Is BYOD required of the employee?** Although BYOD programs are widely lauded for increased productivity and "off-the-clock" accessibility, this benefit can expose employers to potential wage-and-hour issues if the BYOD user is a nonexempt employee.

10. **Does the employee have a means of tracking and recording his time?** If a nonexempt employee is permitted to use a mobile device for work related purposes after working hours, is there a policy that mandates that the employee must report the time that he or she worked? Is there an effective and efficient means for the employee to report such time?

## H. Employee Monitoring

Federal laws prohibit the interception of another's electronic communications, but these same laws have multiple exceptions that generally allow employers to monitor employees' email and internet use on employer-owned equipment or networks. As a result, under federal law, when private-sector employees use an organization's telephone or computer system, monitoring their communications is broadly permissible, though there may be exceptions once the personal nature of a communication is determined. For example, under the National Labor Relations Act, employers cannot electronically spy on certain types of concerted activity by employees about the terms and conditions of employment.

Although monitoring is broadly permitted under federal law, some states require that employers notify employees that they may be monitored. Even in states that do not require notice, employers often choose to provide notice since employees who know they are being monitored are less likely to misuse corporate systems. It is good practice for an employer to have employees sign a consent or acknowledgment that monitoring may occur and to inform them that personal calls may not be made from particular telephones.

Employers may also monitor what an employee posts to social media. However, under some state laws employers cannot request that an employee provide his or her username and password to a social-media account in order for the employer to see content that was not published publicly. This would include, for example, posts that were made available only to an employees friends, or personal network. In addition, some state laws prohibit employers from requiring that their employees accept a friend request that would permit the employer to view friends-only social media posts.

Finally, some states prohibit monitoring of telephone calls on an employer's telephone network without the consent of one or both parties to the communication.

| 80% | 2 | 16 |
|---|---|---|
| Percent of employers who actively monitor their employees electronically.[28] | States that require notice to employees of electronic monitoring.[29] | States that introduced or considered legislation in 2016 prohibiting employers from requesting passwords to social media accounts.[30] |

[28] SpectorSoft, Is Employee Monitoring Legal?, In Context: The Official SpectorSoft Corporate Blog (February 10, 2014), http://www.spectorsoft.com/blog/20140210-is-employee-monitoring-legal.html.

[29] National Conference of State Legislatures, State Laws Related to Internet Privacy, (January 9, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx; these states are: Connecticut (Conn. Gen. Stat. § 31-48d) and Delaware (Del. Code § 19-7-705).

[30] National Conference of State Legislatures, Access to Social Media Usernames and Passwords, (January 9, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

What to consider when crafting employee monitoring policies:

1. Does your organization publish an acceptable use policy?

2. Does the acceptable use policy explain what employees may and may not do over the Internet while at work?

3. Does the acceptable use policy explain the disciplinary consequences of violating the policy?

4. Do you have the ability to block or otherwise restrict access to Internet sites that are barred under the acceptable use policy?

5. Does your employee handbook make employees aware of monitoring?

6. Does the state in which the employee works require single or dual consent for monitoring telephone conversations, and have your employees consented?

7. If your organization monitors phone calls, do you have a policy to cease monitoring when a call is clearly personal in nature, and do you follow it?

8. Have you considered whether an employee might be able to argue that they have an expectation of privacy to their work emails or to their work phone calls?

9. Are you monitoring emails to or from password-protected personal accounts?

10. Are your employees using their own computer equipment to send emails or view the Internet?

## I. Social Media Privacy Concerns

The majority of organizations utilize social media to market their products and services, interact with consumers, and manage their brand identity. Many mobile applications and websites even permit users to sign-in with their social media accounts to purchase items or use the applications' services.

While using third party social media websites has significant advantages for businesses, it also raises distinct privacy concerns. Specifically, the terms of use that apply to social media platforms may give the platform the right to share, use, or collect information concerning your business or your customers. To the extent that the social media platform's privacy practices are not consistent with the practices of your own organization, they may contradict or violate the privacy notice that you provide to the public.

| 74% | 93% |
|---|---|
| Percentage of Fortune 500 companies on Facebook.[31] | Percentage of Fortune 500 companies with a corporate presence on LinkedIn.[32] |

[31] Nora Ganlm Barnes, Ava M. Lescault and Glenn Holmes, The 2015 Fortune 500 and Social Media: Instagram Gains, Blogs Lose, http://www.umassd.edu/cmr/socialmediaresearch/2015fortune500/.

[32] *Id.*

| 76% | 500 million |
| --- | --- |
| Percentage of online adults using social networking sites.[33] | Number of accounts stolen in Yahoo's 2014 data breach.[34] |

What to consider when evaluating your organization's use of social media:

1. How would a data breach of social media platforms affect your organization? Do you have a plan if your social media account is breached?

2. Does your organization share information with an intermediate service provider, such as a social media analytics company, to provide or analyze social media services?

3. Is your internal data or customer personal information protected under your agreements with third parties, including social media platforms?

4. What types of customer personal information are solicited, collected, maintained, or disseminated via your social media platforms (*e.g.*, geo-location)?

5. Do you display information or images of users or other people, including your employees? Did the people in the images give their permission and/or sign a release?

6. Is your client list private? Do your employees connect to your clients on social media?

7. How is information about your customers that is collected from social media sites being stored? Do any third parties have access to that information?

8. Do users log-in to your services or make purchases through a social media platform?

9. What type of personal information do your customers share with you on social media platforms?

10. Does your use comply with the platform's policy for collecting data from users? Do you review the platform's policies regularly?

11. Does your organization have a social media policy governing employees' use of social media, particularly pertaining to sharing confidential customer and organizational data on the platform?

12. How does your IT team manage the security and passwords for your social media sites?

---

[33] Pew Research Center, Social Networking Fact Sheet, http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/.

[34] Seth Fiegerman, Yahoo says 500 million accounts stolen, CNN, (September 22, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/.

## J. Online Behavioral Advertising

Behavioral advertising refers to the use of information to predict the types of products or services of greatest interest to a particular consumer. Online behavioral advertising takes two forms. "First party" behavioral advertising refers to situations in which a company's website uses information that it obtains when interacting with a visitor. "Third party" behavioral advertising refers to situations in which a company permits others to place tracking cookies on the computers of people who visit the company's website, so that those individuals can be monitored across a behavioral advertising network.

Two self-regulatory associations – the Network Advertising Initiative ("NAI") and the Digital Advertising Alliance ("DAA") – have created standards for companies engaged in third party online behavioral advertising, as well as promoted mechanisms for consumers to opt-out of being tracked. In addition to the self-regulatory effort, on January 1, 2014, a California statute went into effect that requires a company to notify consumers if such company permits third party behavioral advertising in certain situations.

| | | | |
|---|---|---|---|
| 2<br>Number of state statutes that may require companies to disclose the use of third party behavioral advertising.[35] | 104<br>Number of companies that are members of NAI.[36] | 292<br>Number of companies that are members of DAA.[37] | 73<br>Number of references on FTC's website to "behavioral advertising."[38] |
| 2 - 60<br>The number of tracking cookies placed by the top 5 retailers on their websites.[39] | | | |

What to think about when evaluating your organization's online behavioral advertising practices:

1. Does your privacy policy comply with state law requirements concerning the disclosure of first party online behavioral advertising?

2. Does your privacy policy comply with state law requirements concerning the disclosure of third party online behavioral advertising?

3. Does your organization state or imply that it only permits behavioral advertisers to use its website if those advertisers utilize the opt-out mechanisms of NAI and/or DAA?

---

35 Cal Bus. & Prof. Code §§ 22575(b)(5)-(7); Del. Code 1204C

36 Companies listed on http://www.networkadvertising.org/participating-networks as of January 2017

37 Companies listed on http://www.aboutads.info/participating as of January 2017.

38 Based upon Google search restricted to FTC.gov conducted in January 2017.

39 Top 5 eCommerce retailers as identified by the National Retail Federation in May of 2016. Quantity of cookies identified by Ghostery on retailer home page on May 6, 2016.

4. If so, do all of the behavioral advertisers that you permit to use your website permit opt-out via the NAI and/or DAA mechanisms?

5. Who within your organization has the authority to permit third parties to place cookies on your website?

6. Who within your organization maintains a comprehensive list of all cookies placed on your website?

7. Has the legal department reviewed the contracts with each behavioral advertiser with whom your organization has a relationship to verify that their privacy practices comply with law and with the standards of your organization?

8. Have you audited the cookies that are placed, or tracked, on your website?

9. Have you verified the accuracy of the description of behavioral advertising contained on your website?

## K. Video Viewing Information

The Video Privacy Protection Act ("VPPA") was passed in 1988 in reaction to a fear that people other than a consumer and a video rental store could collect information on a consumer's video rental history. This was not an academic concern at the time. Immediately prior to the passage of the VPPA, Judge Robert Bork, who had been nominated to the Supreme Court, had his video rental history published by a newspaper that was investigating whether he was fit to hold office.

Among other things, the VPPA protects consumers by limiting disclosure of rental and sales records by video tape service providers to the consumer, people who have the consumer's consent, and law enforcement agencies who have a warrant, subpoena, or court order. Recently, the plaintiff's bar has tried to revive the VPPA by applying its provisions to websites that stream movies and digital content, such as iTunes, Amazon Video, and Netflix.

| 53% | >151 hours | $2,500 |
|---|---|---|
| Percentage of US homes with access to a subscription-based video-on demand (SVOD) service.[40] | The amount of time spent by an average consumer viewing video content each month.[41] | Potential liability per violation of the VPPA.[42] |

If your organization rents, sells, or streams video content consider the following steps to reduce your risk of liability under the VPPA:

1. Does your organization fall under the definition of a video tape service provider or a provider of similar audio visual materials as those terms are defined under the VPPA?

[40] Nielsen, The Total Audience Report Q2 2016, (September 26, 2016), http://www.nielsen.com/us/en/insights/reports/2016/the-nielsen-total-audience-report-q2-2016.html.

[41] *Id.* at 11.

[42] 18 U.S. Code § 2710(c)(2)(A).

2. Does your organization share information concerning consumers' video viewing habits with any third parties?

3. Which platforms does your organization use to provide access to videos?

4. Does the video platform transmit personal information to third parties?

5. Does your organization obtain consent prior to sharing information about consumers that view video content?

## L. Geo-Location Tracking

Smartphones, smartphone apps, websites, and other connected devices (*e.g.,* "wearables") increasingly request that consumers provide their geo-location information. Geo-location information can refer to general information about a consumer's location, such as his or her city, state, zip code, or precise information that pinpoints the consumer's location to within a few feet, such as his or her GPS coordinates.

Organizations request geo-location information for a variety of reasons. For example, many apps – such as transportation or delivery services – require geo-location in order to provide services that are requested by the consumer. Other apps – such as mapping programs, coupon programs, or weather programs – require geo-location information in order to provide consumers with useful information. Because such information has become intertwined, in many cases, with products and services, some organizations require the user to "Accept" or '"Agree"' to the collection of geo-location information as a condition to using a device, application, or website.

Although there is currently no federal statute that expressly regulates the use, collection, or sharing of geo-location data, the FTC has taken the position that precise geo-location information is a form of "sensitive" personal information and has suggested that a failure to reasonably secure such information, or a failure to adequately disclose the collection or sharing of such information, may violate the FTCA's general prohibition against unfair or deceptive practices.[43] In addition, Congress and state legislatures have considered several proposals that would expressly regulate geo-location information.

| Every 10 Minutes | 91% |
|---|---|
| The frequency with which some apps, like weather apps, request geo-location information.[44] | Percentage of adults who "agree" or "strongly agree" that consumers have lost control over how often personal information is collected and used by companies.[45] |

[43] *See*, Jessica Rich, Prepared Statement of the Federal Trade Commission on S. 2171 The Location Privacy Protection Act of 2014 Before The United States Senate Committee on the Judiciary Subcommittee for Privacy, Technology, and the Law, (June 4, 2014), https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf.

[44] Almuhimedi et. al., Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging, http://www.normsadeh.com/file_download/179.

[45] Mary Madden, Privacy and Cybersecurity: Key findings from Pew Research, Pew Research Center, (January 16, 2015), http://www.pewresearch.org/key-data-points/privacy/.

| 73% | 19 |
|---|---|
| Percentage of times that an app will share geo-location information with an advertising network when asked.[46] | Number of FTC enforcement actions regarding geo-location practices.[47] |
| 10-20% | |
| How much more marketers pay for online ads that include geo-location information.[48] | |

What to consider if your organization collects geo-location information:

1. What is the purpose for which geo-location information is being collected?

2. Are you collecting the least granular (i.e., most general) location information possible in order to effectively provide a product or a service to the consumer?

3. How often do you need to collect geo-location information?

4. Is the user aware that geo-location information is being collected?

5. Does the user have the ability to disable the collection of geo-location information?

6. Does the user have the ability to control how long that information is maintained, how it is used, when it is shared, and whether it is associated with their name?

7. Will the geo-location information be shared with third parties such as advertisers? If yes, how much and how often will you share the information?

8. Is the geo-location information encrypted in transmission from the consumer and/or at rest within your organization?

## M. Radio Frequency Identification ("RFID")

Radio Frequency Identification ("RFID") technology uses electromagnetic fields to transfer data. RFID systems typically operate by attaching tags to objects, devices, or cards. Some tags can be powered by a local power source, such as a battery ("active RFID"). Their local power source permits them to transmit a signal that may be registered hundreds of meters from an RFID reader. Other tags do not have a local power source and are instead powered by electromagnetic induction from the magnetic fields that are produced by a RFID reading device in close proximity ("passive RFID").

---

[46] Elizabeth Dwoskin, Where were you 3 Minutes Ago? Your Apps Know, Wall Street Journal (May 23, 2015), http://blogs.wsj.com/digits/2015/03/23/where-were-you-3-minutes-ago-your-apps-know/.

[47] IAPP Resource Center, Geolocation (May 5, 2016), https://iapp.org/resources/topics/geolocation/?mkt_tok=eyJpIjoiT0RVNU5ERmpNakl6TWpVMCIsInQiOiJWNStcL2JsVmRweE9WbW13Z1NUVFBBeHBwN.

[48] Elizabeth Dwoskin, Where were you 3 Minutes Ago? Your Apps Know, Wall Street Journal (May 23, 2015), http://blogs.wsj.com/digits/2015/03/23/where-were-you-3-minutes-ago-your-apps-know/.

RFID tags have been utilized in many industries. In the manufacturing sector they are used to track parts within a factory, or the location of a final product in a production line. In the agricultural sector they can be implanted in livestock to allow for the identification of animals. In the payments sector, some payment cards were embedded with RFID chips to permit consumers to process a payment by holding their payment card within close proximity of a point of sale device that was enabled with an RFID reader. As payment cards have shifted toward embedded microprocessors ("EMV"), and the financial technology community has embraced alternative wireless transmission protocols, such as Near Field Communication ("NFC") utilized by ApplePay, the use of RFID technology has declined.

Privacy advocates have voiced concern that consumer products that contain personally identifiable information that is intended to be accessible using RFID technology may be susceptible to interception or eavesdropping. Specifically, the media has expressed concern that identity thieves could be able to use remote RFID readers to remotely steal information from RFID enabled payments cards or identification cards. To-date, however, there have been relatively few (if any) confirmed instances of identity theft from RFID eavesdropping.

| $12.6 Billion | 19 | 569 |
|---|---|---|
| Size of the market for RFID technology.[49] | Number of states that have enacted privacy statutes focused on RFID technology.[50] | The number of wallets advertised by a prominent retailer as containing RFID blocking technology.[51] |

If your organization is considering using RFID technology to track consumers, or to save personal information, you should consider the following:

1. What, if any, personal information does your organization intend to embed in an RFID tag?

2. If the personal information were accessed by an unauthorized party could it lead to identity theft?

3. Will consumers be notified about the type of information contained in the RFID tag?

4. Will consumers have any misconceptions concerning the security of their information?

5. Will consumers be provided a choice to opt-out of having an embedded RFID tag?

6. Can you assure consumers that the RFID tag cannot be eavesdropped?

---

[49] Source: Statista.com *available at* http://www.statista.com/statistics/299966/size-of-the-global-rfid-market/ (last checked Nov. 2016)

[50] National Conference of State Legislatures Survey of RFID Privacy Laws *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx (last viewed Nov. 2016).

[51] Search of Walmart.com for "RFID Wallet" conducted in November 2016.

7. Do you have a process for periodically evaluating any changes concerning the security of RFID tags?

8. Does your organization's proposed use of RFID technology comport with state laws?

## N. Email Marketing

Email is ubiquitous in modern life with billions of emails – wanted and unwanted – sent each day. Since its enactment in 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act has attempted to curb the number of unwanted emails and impose some rules on a largely unregulated frontier. When followed, CAN-SPAM Act's restrictions give email recipients some control over their inboxes and also maintain fairness in how emails present themselves. Failure to follow the CAN-SPAM Act can lead to penalties of up to $16,000 per violation.

As a practical matter, many organizations use vendors for their email marketing and other email services, and those vendors often assist the organizations in complying with the requirements of the CAN-SPAM Act. Nonetheless, the party whose content is promoted via email must supervise the conduct of its vendors and employees in abiding by CAN-SPAM, or else risk possible sanctions.

| $44.25 | 139.4 Billion | 2.5 Billion | 9,185 |
|---|---|---|---|
| Average return on each dollar of email marketing investment.[52] | Projected number of daily business emails in 2018.[53] | Estimated number of email users.[54] | Number of complaints received by the FTC in a year concerning unsolicited email.[55] |

The basic requirements of CAN-SPAM are:

1. Does your email message include: (a) complete and accurate transmission and header information; (b) a "From" line that identifies your business as the sender; (c) a "Subject" line that accurately describes your message; and (d) an effective "opt-out" mechanism?

2. Does your email either contain an email address, physical address, or other mechanism that the recipient may use for opting-out of future marketing emails?

---

52 Amanda Nelson, 25 Mind Blowing Email Marketing Stats, Salesforce Blog, (July 12, 2013), https://www.salesforce.com/blog/2013/07/email-marketing-stats.html.

53 Sara Radicati, Email Statistics Report, 2014-2018, (April 2014), http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf.

54 *Id*.

55 FTC, Consumer Sentinel Network Data Book for January – December 2014, (February 2015), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

3. Is your opt-out mechanism effective for at least 30 days after your email is sent?

4. Do you honor all requests to opt-out within 10 days?

5. Does your mailing list include any recipient that has asked not to receive email from your business (opted-out)?

6. Have you tested the effectiveness of your opt-out mechanism?

7. Have you reviewed your vendor contracts to determine each party's responsibilities with regard to CAN-SPAM compliance?

8. Are addresses of people that have opted-out transferred outside of your organization?

9. Does your organization use open relays or open proxies to send marketing email?

## O. Email Marketing In Canada (CASL)

On July 1, 2014, the central provisions of the Canadian Anti-Spam Law ("CASL") came into force. [56] These provisions generally prohibit the sending of a Commercial Electronic Message ("CEM") without a recipient's express consent, and unless the CEM contains certain sender identification information and an effective unsubscribe mechanism. CASL provides a number of nuanced exceptions to the express consent requirements of the law. The primary enforcement agency of CASL is the Canadian Radio-television and Telecommunications Commission (CRTC). The CRTC has several compliance tools to enforce CASL, including the issuance of Administrative Monetary Penalties (AMPs) against individuals and organizations that have violated CASL's provisions.

Due to CASL's broad applicability, exacting standards, and potentially severe financial penalties, companies that do business in Canada are advised to implement appropriate compliance measures to address the provisions of CASL. Companies sending emails to recipients in Canada must tailor their compliance programs to CASL's complex set of consent exceptions and patchwork of guidelines, interpretations, and enforcement actions. To date, the CRTC has brought only a handful of major CASL enforcement actions, but many investigations are ongoing. Further clarification with regard to the most heavily utilized exceptions is expected. In October 2016, the CRTC assessed the scope of the "conspicuously published" implied consent exception in its first Compliance and Enforcement Decision (CRTC 2016-428).

| $10 million | $1.1 million |
|---|---|
| The maximum AMP that the CRTC can assess against a company for a violation of CASL.[57] | The largest AMP that has been issued since CASL came into force in July 1, 2014.[58] |

[56] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23, Assented to 2010-12-15 ("CASL"), http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html.

[57] CASL, Section 20(4).

| 200,000+ | July 1, 2017 |
| --- | --- |
| CASL related complaints filed with the CRTC between July 1, 2014 and January 6, 2015.[59] | The date that a private right of action for CASL violations becomes available.[60] |

Consent Exceptions:

1. CASL does not apply to electronic messages sent:

    a. Internally within an organization.

    b. Between organizations in a relationship, where the message concerns the recipient.

    c. In response to an inquiry from the recipient.

    d. To satisfy a legal right or obligation.

    e. From Canada and accessed in another "listed" country, and the message complies with the "listed" country's spam laws.

    f. By a sender who has a "family" or "personal" relationship with the recipient.

    g. By or on behalf of a charity soliciting donations.

    h. By or on behalf of a political party soliciting donations.

2. CASL applies, but consent is not required where a CEM only:

    a. Provides a quote or estimate.

    b. Facilitates, completes, or confirms an existing transaction.

    c. Provides a warranty, a product recall, or safety information.

    d. Provides factual information about products or services.

    e. Delivers products, updates, or upgrades that the recipient is entitled to receive.

3. CASL applies, but consent from the recipient is implied where:

    a. The recipient and sender have an "existing business relationship."

---

58 Government of Canada, CRTC Notice of Violation: 3510395 Canada Inc. (Compu.Finder), (March 5, 2015), http://www.crtc.gc.ca/eng/archive/2015/vt150305.htm.

59 Government of Canada, Canada's Anti-Spam Legislation – FAQs for Businesses and Organizations, (January 15, 2015), http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html.

60 CASL, Section 91.

b. The recipient and the sender have an "existing non-business relationship."

c. The recipient has conspicuously published or provided his or her email address.

Questions to consider when evaluating CASL:

1. Have you performed an assessment of your organization's electronic communications to determine if they qualify as CEMs?

2. Do any consent exceptions apply to your organization or your organization's CEMs, or do you have a special relationship with the recipient such that consent is implied?

3. If no consent exception applies, have you implemented a procedure to capture "express consent," including providing: (i) the purpose of requesting consent; (ii) the name of the entity requesting consent; (iii) a mailing address plus phone number, email, or web address; (iv) a statement that consent can be withdrawn; and (v) an affirmative opt-in mechanism?

4. Do your CEMs include the required sender indemnification information and a functioning unsubscribe mechanism?

5. Do you honor all requests to unsubscribe within 10 days?

6. Does your mailing list include any recipient that has either unsubscribed from your CEMs or no longer qualifies for a consent exception?

7. Do you scrub your mailing list against your organization's "do not e-mail list"?

8. Have you implemented procedures to test the effectiveness of your unsubscribe mechanism?

9. Have you reviewed your vendor contracts to determine each party's responsibilities with regard to CASL compliance?

10. Does your CASL compliance program include senior management involvement, a written policy, risk assessments, record keeping, staff training, and a complaint-handling process?

## P. Collecting Information From Children

There are relatively few restrictions on collecting information from children off-line. Efforts to collect information from children over the internet, however, are regulated by the Children's Online Privacy Protection Act ("COPPA"). Among other things, COPPA requires that a website obtain parental consent prior to collecting information, post a specific form of privacy policy that complies with the statute, safeguard the information that is received from a child, and give parents certain rights, like the ability to review and delete their child's information. COPPA also prohibits companies from *requiring* that children provide personal information in order to participate in activities, such as on-line games or sweepstakes.

| 549 | $2.28 / Child | 20+ | $4 million |
|---|---|---|---|
| Number of complaints received by the FTC about companies violating COPPA.[61] | Estimate by one organization of the average fine per child imposed by the FTC .[62] | Number of enforcement actions taken by the FTC.[63] | The largest COPPA fine imposed by the FTC.[64] |

The following are the most common complaints about children's websites received by the FTC:[65]

| | |
|---|---|
| 48.45% | The website did not obtain proper parental consent |
| 43.72% | The website collected more personal information than was necessary |
| 41.35% | Parents were not given an opportunity to stop information from being disclosed to third parties |
| 24.77% | The website did not have a clear privacy policy |
| 17.67% | The website misrepresented how information was used |

What to think about when reviewing your website:

1. Does your website ask children to provide information?
2. If not, does your website automatically collect information about a child's computer or session?
3. Would your website appeal to children?
4. Has the FTC received complaints about your website? If so, how many and what issues were raised in the complaints?
5. Does your website ask for parents' permission to collect information about children?
6. Does your website verify that the parent is the actual parent of a child?
7. Has the verification mechanism been approved by the FTC?
8. Does your website's privacy policy comply with COPPA?
9. Can you limit liability by joining an FTC approved self-regulatory organization (sometimes called a "safe harbor" program)?
10. Which safe harbor program provides the most benefit to your organization?

---

61 Based upon analysis of consumer complaints received by the FTC between January 2008 and August 2013.

62 http://www.coppanow.com/averagecoppa/ (last viewed Nov. 2016).

63 FTC, 2014 Privacy and Data Security Update, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

64 United States v. InMobi Pte Ltd, Case No. 3:16-cv-03474 (N.D. Cal. June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf.

65 Based upon analysis of consumer complaints received by the FTC between January 2008 and August 2013.

## Q. Facial Recognition Technology

Facial recognition technology uses algorithms that map facial features – such as the distance between a person's eyes, or the width of a person's nose – and compares those features to a database of known individuals. Organizations may use the technology for security (*e.g.,* cameras that "ID" employees or criminals), marketing to consumers (*e.g.,* cameras that "ID" particular customers), or designing products that quickly categorize digital media (e.g., photograph sorting).

There is currently no federal statute that expressly regulates private-sector use of facial recognition technology. Nonetheless, the FTC, which has authority to prevent unfair and deceptive practices, has expressed interest in the privacy implications of facial recognition technology, has issued a set of best practices concerning its use, and has investigated organizations that it believes violated those recommendations.

At least two states have also enacted statutes that govern the technology. Those statutes require that a company (1) notify state residents that the technology is in use, and (2) obtain the consent of those subject to the technology.

| 1 | 30% | 80 | 5 |
|---|---|---|---|
| Number of years that an organization is allowed to keep biometric data under state law after the purpose for which it was collected has expired.[66] | Percentage increase in accuracy of facial recognition algorithms over a three year period.[67] | Number of public comments received following FTC workshop on facial recognition technology.[68] | Number of state data breach notification laws that may apply to facial recognition telemetry if lost or stolen.[69] |
| $5,000 - $25,000<br>The range of possible fines and damages that could be assessed under state law for each violation of a facial recognition statute.[70] | | | |

Practices recommended by the FTC when deploying facial recognition technology:

1. Security. Companies should maintain reasonable data security for consumers' images and facial geometry.

2. Retention and Disposal. Companies should establish and maintain appropriate retention and disposal practices for consumers' images and facial geometry.

66 Tex. Bus. & Com. Code § 503.001(b)(3).

67 National Institute of Standards and Technology, NIST: Performance of Facial Recognition Software Continues to Improve, (June 3, 2014), http://www.nist.gov/itl/iad/face-060314.cfm.

68 *See*, Public Comments, FTC Matter No. P115406.

69 Bryan Cave LLP, Data Breach Notification Survey (2015).

70 *See*, 740 ILCS 14/20 (1)-(4); Tex. Bus. & Com. Code § 503.001(d).

3. Sensitivity of Video-Feed. Companies should consider the sensitivity of the data that they capture including, specifically, not placing cameras in areas in which consumers would not expect them (*e.g.,* locker rooms, bathrooms, health care facilities, etc.).

4. Notice. Companies should provide "clear notice" when facial recognition technology is being utilized.

5. Opt-in Consent For Materially Different Use. Companies should obtain consumers' affirmative express consent if they use an image in a "materially different manner" than was represented when the facial geometry was collected.

6. Opt-in Consent For Sharing. Companies should obtain consumers' affirmative express consent if they identify anonymous images of a consumer to someone who could not otherwise identify the consumer.

## R. Fingerprint Identification Technology

Fingerprint identification technology uses fingerprints to uniquely identify individuals. The technology has been used by law enforcement agencies for decades, and dozens of statutes regulate when government agencies may collect fingerprints, how they are permitted to use them, and with whom they can be shared.

Advances in fingerprint recognition software have lead some private entities to begin using the technology to authenticate consumers. For example, some mobile devices have integrated fingerprint recognition technology to replace, or supplement, passwords or passcodes. Some employers are also using fingerprint recognition technology to increase the accuracy and efficiency of employee timekeeping systems.

There is currently no federal statute that expressly regulates private-sector use of fingerprint recognition software. Nonetheless, the FTC, which has authority to prevent unfair and deceptive practices, may proceed against companies that misrepresent the function of the technology, or how they use, secure, or disclose captured fingerprints or fingerprint geometry.

Numerous states have enacted statutes concerning the collection of fingerprints by government agencies, by accreditation boards, or in certain regulated industries (e.g., childcare and education). At least two states have also enacted statutes that govern the private sector's use of the technology outside of specific fields and applications . Those statutes generally require that if an organization "captures" a fingerprint it must provide the consumer with notice and obtain their consent. In addition, if an organization stores or "possesses" a fingerprint then it must limit its disclosure to third parties, enact measures to secure the fingerprint from unauthorized access, and limit its retention of the fingerprint after it is no longer needed. A number of additional states require that if a company collects fingerprints it take steps to prevent the fingerprint from being acquired when in the process of being destroyed.

| | |
|---|---|
| 2,941,036<br>Number of fingerprints processed by one government agency in a year.[71] | 1 in 50,000<br>Probability of a false match claimed by one mobile device in conjunction with fingerprint recognition software.[72] |
| $5,000 - $25,000<br>The range of possible fines and damages that could be assessed under state law for *each* violation of a fingerprint identification statute.[73] | |
| $1.5 Million<br>Largest class action settlement / judgment against a company for allegedly collecting fingerprints without providing proper notice and obtaining appropriate consent.[74] | |

Consider the following when using fingerprint identification technology:

1. Data Inventory. If your organization keeps a data inventory or a data map, you should include fingerprints and/or fingerprint geometry in that inventory.

2. Security. Assess the risk that fingerprints and/or fingerprint geometry may be compromised and consider what steps can be reasonably taken to attempt to keep the information secure.

3. Retention and Disposal. Review your retention and disposal practices to see if they specify how long such information should be kept, and how it should be disposed.

4. Notice. Consider providing clear notice to consumers or employees before capturing their fingerprints.

5. Consent. Consider obtaining opt-in consent before capturing or using fingerprints.

6. Sharing. Consider obtaining opt-in consent before sharing fingerprints or fingerprint geometry with any third parties.

## S. Passing Data Between Retailers To Facilitate Transactions

Online retailers often learn information about a consumer that may be used by them to help identify other products, services, or companies that may be of interest to the consumer. For example, if a person purchases an airplane ticket to Washington DC, the person may want information about hotels, popular restaurants, or amenities at the airport.

---

[71] FBI, Next Generation Identification (NGI) Monthly Fact Sheet (Sept. 2015) *available at* https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/next-generation-identification-monthly-fact-sheet (viewed Dec. 2015).

[72] https://support.apple.com/en-us/HT204587 (last viewed Dec. 2015).

[73] *See*, 740 ILCS 14/20 (1)-(4); Tex. Bus. & Com. Code § 503.001(d).

[74] Stipulation of Class Action Settlement, *Sekura v. L.A. Tan Enterprises, Inc.*, Case No. 15-CH-16694 (Cir. Ct. Cook County Ill. June 20, 2016).

Although online retailers often strive to provide recommendations quickly, and to make a consumer's transition to a third party retailer seamless, the Restore Online Shoppers' Confidence Act ("ROSCA") generally prohibits one online merchant from transferring payment information (*e.g.,* a credit card number) to a second online merchant. ROSCA also prohibits the second online merchant from charging a consumer's payment card or financial account, unless the second online merchant has clearly and conspicuously disclosed to the consumer all material terms of the transaction and received the consumer's express consent to the charge.

| $340.3 Billion | 6 | 100% |
|---|---|---|
| Amount spent per year by consumers online.[75] | Number of Federal Trade Commission enforcement actions initiated under ROSCA.[76] | Percentage of ROSCA cases that have been filed by the FTC in federal district court, as opposed to an administrative adjudication.[77] |

Questions to consider when evaluating the data privacy issues involved in passing information between online retailers:

1. Are consumers being presented with third party products or services when they visit a retailer's website?

2. Are consumers being presented with third party products or services immediately after they visit a retailer's website?

3. Are such items affirmatively selected by the consumer, or added automatically to the consumer's shopping cart?

4. If the consumer decides to purchase such third party products or services, would he or she likely think that your organization, or the third party, is processing the transaction?

5. Is the total cost of each third party product clearly and conspicuously disclosed?

6. If the consumer indicates that he or she wishes to buy a third party product or service, can the consumer easily change that decision?

7. Is contact information being transferred from one retailer to another?

8. Is payment information being transferred from one retailer to another?

9. Is the third party offering a free trial offer? If so will the consumer be charged any money to participate and does the consumer need to take an affirmative act to prevent a charge after the trial period?

10. Is the third party offering a continuity program or membership? If so are the terms of the program clearly and conspicuously disclosed?

---

[75] U.S. Census Bureau News, Quarterly retail E-Commerce Sales http://www2.census.gov/retail/releases/historical/ecomm/15q4.pdf. .

[76] Enforcement actions reviewed as of January 2017.

[77] *Id.*

## T. Privacy Due Diligence In A Merger Or Acquisition

The FTC can hold an acquirer responsible for the bad data privacy practices of a company that it acquires. Evaluating a target's data privacy practices, however, can be daunting and complicated by the fact that many "data" issues are first identified months, or years, after a transaction has closed. For example, although it is relatively easy to read a potential target's privacy policies it is far more difficult to verify that the policy is accurate or complete.

| $3 million |
| --- |
| Civil penalty imposed by the Federal Trade Commission upon acquirer for data privacy violation of acquisition that occurred prior to closing.[78] |

Due diligence questions to consider in a M&A transaction in order to evaluate data privacy related rsisk:

1. Has the target received a regulatory inquiry concerning its data privacy practices?

2. Has the target received litigation claims concerning its data privacy practices?

3. Has the target tracked data privacy complaints submitted to it by consumers?

4. Has the target tracked data privacy complaints submitted by consumers to government agencies, including the quantity and nature of data privacy complaints lodged with the Federal Trade Commission?

5. Is the target subject to a sector specific data privacy law?

6. Do the target's internal privacy policies and procedures comply with legal standards?

7. Do the target's external privacy policies and procedures comply with legal standards?

8. Has the target conducted a data map or a data inventory?

9. What are the target's data retention policies?

10. With whom does the target share data?

11. Does the target have a vendor management program in place?

12. Have the vendors used by the target provided appropriate contractual protections?

13. Did the target have an employee, such as a Chief Privacy Officer, who was focused on data privacy issues?

[78] United States (FTC) v. Playdom, Case No. 11-00724 (C.D. Cal. May 11, 2011).

14. If the target conducted operations internationally did it have a strategy in-place for handling the cross-border transfers of information?

## U. Vehicle Event Data Recorders

Event data recorders, also known as "black boxes" or "sensing diagnostic modules," capture information such as the speed of a vehicle and the use of a safety belt. In the event of a collision this information can be used to help understand how the vehicle's systems performed.

In December of 2012, the National Highway Traffic Administration proposed a rule that would require automakers to install event data recorders in all new light passenger vehicles. Although the proposed rule would have required manufacturers to install the devices beginning in 2014, the rule was never finalized. Nonetheless, some estimates indicate that most passenger cars are already equipped by manufacturers with event data recorders.

Since 2005 states have passed statutes designed to address the privacy implications of event data recorders. Although variability exists among the state statutes, most statutes require that a consumer be notified of the existence of the device prior to purchase, and restrict who may access the information on the device.

On December 4, 2015, the federal Driver Privacy Act of 2015 was enacted. The Act makes clear that data collected from an event data recorder belongs to the owner or lessee of the vehicle. The Act also provides that data recorded or transmitted by an event data recorder may not be accessed by a person other than the vehicle's owner or lessee, except in certain defined circumstances.

| 96% | 17 | 7 |
|---|---|---|
| Estimate of the number of new passenger cars equipped with event data recorders.[79] | The number of states that have passed legislation protecting the privacy of data on event data recorders.[80] | The number of exceptions included in some state statutes for who may access the data.[81] |

What to think about when utilizing event data recorders:

1. If your organization is placing event data recorders on vehicles, are you permitted by state statute to do so?

2. If your organization intends to use event data recorder information, which state statute governs your use?

---

79 Nat'l Highway Transp. Safety Admin., U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety, (December 7, 2012), http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety.

80 National Conference of State Legislatures, Privacy of data from Event Data Recorders: State Statutes, (June 1, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

81 *See*, *e.g.*, Ark. Code § 21-112-107 (2015).

3. If your organization is using event data recorder information, does the organization (or the use) fall under one of the exceptions set forth in the state statutes?

4. What are the penalties for failing to obtain appropriate consent?

5. If you have obtained consent, is your consent current and valid?

## V. Self-Driving Vehicles

Self-driving cars, or autonomous vehicles, may be the greatest disruptive innovation to travel that we have experienced in a century. A fully-automated, self-driving car is able to perceive its environment, determine the optimal route, and drive unaided by human intervention for the entire journey. Self-driving cars have the potential to drastically reduce accidents, travel time, and the environmental impact of road travel. However, obstacles remain for the full implementation of the technology including the need to reduce public fear, increase reliability, and create adequate regulations.

Of particular concern with regard to self-driving cars are data privacy and cyber security risks. To date, six states and the District of Columbia have enacted laws that address autonomous vehicles or autonomous technology, but none of these state regulations address key areas of data privacy and security, such as the collection, use, choice, and security of consumer data gathered from these autonomous vehicles or autonomous technology. As vehicles become more computerized and begin to generate huge amounts of data, the potential for unwanted third party access of that data and the risk of cyber threat increases. Hackers could access the personal data of a driver, such as the vehicle's location, the identity of others in the car, and whether the driver is home at any particular time. Additionally, cyberattacks could have potentially fatal consequences, not just for the driver and passengers inside the vehicle, but for anyone or anything physically surrounding the vehicle.

| 68% | 54 million | $87 billion | $759 million |
|---|---|---|---|
| Percentage of global automotive industry executives who expect self-driving cars to be on the market by 2025.[82] | The projected number of self-driving cars on the road globally by 2035.[83] | The market opportunity for car manufacturers, technology developers, and original equipment manufacturers by 2030.[84] | The market opportunity for automotive cybersecurity technology by 2023.[85] |

Questions to consider when evaluating the data privacy and security issues of self-driving cars:

---

82 Global Automotive Industry Expects Self-Driving Cars On Sale by 2025, Says just-auto.com Survey, Digital Journal (June 10, 2014), http://www.digitaljournal.com/pr/1975125.

83 IHS Automotive, Self-Driving Cars Moving into the Industry's Driver's Seat, (January 2, 2014), http://press.ihs.com/press-release/automotive/self-driving-cars-moving-industrys-drivers-seat.

84 Lux Research, Set Autopilot for Profits: Capitalizing on the $87 Billion Self-Driving Car Opportunity, (April 29, 2014), https://portal.luxresearchinc.com/research/report_excerpt/16874.

85 IHS Markit, Automotive Cybersecurity Market to Reach $759 Million in Revenue in 2023 (September 26, 2016), http://news.ihsmarkit.com/press-release/automotive-cybersecurity-market-reach-759-million-revenue-2023-ihs-markit-reports.

1. Do current regulations cover your self-driving car? If so, what aspect of your self-driving car do these regulations cover, and what do those regulations require?

2. What types of data does your driverless technology collect?

3. Do third parties have access to the data?

4. Do you have a duty to notify the driver of the self-driving car of the data you are either actively or passively collecting?

5. Do you have a duty to notify the driver if you lose the data or, based on the data, you are aware of conditions that could put the driver in danger?

6. What choices have you given, or are you required to give, the driver of the self-driving car?

7. Have you attained appropriate releases of liability permitted under current regulations?

8. Is your self-driving car or driverless technology susceptible to a cyberattack?

9. Have you tested and determined that your driverless technology is highly resilient to cyber threat?

10. Have you procured insurance in sufficient amounts to cover likely risks and threats?

## W. FTC Tracking Of Privacy Complaints

The FTC collects complaints about companies that allegedly violate the data privacy, data security, advertising, and marketing laws. The result is a massive database of consumer complaints known as "Consumer Sentinel" that is used by the FTC and other consumer protection regulators to identify and investigate enforcement targets.

Regulators can use Consumer Sentinel to search for complaints on any company. They can also request that the database alert them to new complaints about an organization, or connect them with other law enforcement agencies that might have an interest in investigating the same organization. In addition to these functionalities, the FTC also creates a "Top Violator" report and a "Surge" report that track those organizations that the FTC believes may have a suspicious pattern of consumer complaints.[86] The end result is that the vast majority of FTC enforcement actions target companies identified within the FTC's database.

[86] FTC Office of Inspector General, Evaluation of the Federal Trade Commission's Bureau of Consumer Protection Resources, OIG Evaluation Report No. 14-003, p. 4, 8 (Oct. 2, 2014), https://www.ftc.gov/system/files/documents/reports/evaluation-ftc-bureau-consumer-protection-resources/2015evaluationftcbcpreport.pdf.

| 28 million | 93.8% | 35 | 195 |
|---|---|---|---|
| Number of consumer complaints maintained in Consumer Sentinel.[87] | Percentage of FTC enforcement actions that target a company found in Consumer Sentinel.[88] | Number of government agencies that contribute complaints to the FTC's Consumer Sentinel.[89] | Number of distinct "law violations" tracked by the FTC.[90] |
| 394 – 2,795<br>Range of complaints filed per month against the top 50 organizations tracked.[91] | | | |

What to think about when considering the records that the FTC maintains about your organization:

1. Has your organization been identified as a potential enforcement target on the FTC's Top Violator or Surge reports?

2. Does your organization routinely track the quantity of complaints that the FTC maintains about it?

3. Is the volume of complaints filed about your organization above, or below, those of others in your industry?

4. If the FTC, or another regulator, searched for the complaints about your organization what potential compliance issues would they identify?

5. If your organization were investigated by the FTC, is the volume of complaints filed about it easily explained?

6. Is the volume of your complaints trending up, or trending down?

7. Have plaintiffs' law firms investigated your complaint volume?

## X. Companies Perceived By The FTC as Top Violators

As discussed in the previous section, the FTC collects complaints about organizations that allegedly violate the data privacy, data security, advertising, and marketing laws.

---

87 FTC, Consumer Sentinel Network Data Book for January – December 2015, p. 3 (February 2016) (12 million complaints from Consumer Sentinel and 16 million from do-not-call database).

88 FTC, Fiscal Year 2015 Performance Report and Annual Performance Plan for Fiscal Years 2016 and 2017, p. 51 https://www.ftc.gov/system/files/documents/reports/fy-2016-2017-performance-plan-fy-2015-performance-report/pprfy16-17_0.pdf.

89 FTC, Consumer Sentinel Network Data Contributors, https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors (last viewed Nov. 11, 2016).

90 Based upon Law Violation Codes used within the FTC's Consumer Sentinel database.

91 FTC, Top Companies Receiving Complaints in Consumer Sentinel (Aug. 1, 2016 – Aug. 31, 2016) (excludes complaints relating to scams connected to impersonating the government).

Each month the FTC creates a "Top Violators" report that ranks the fifty organizations with the greatest volume of consumer complaints. The report indicates whether each organization listed was included in the previous month's report, whether its rank has changed, and the number of complaints received by the FTC that month. For organizations that are new to the report, the FTC reviews their complaints and summarizes the issue, or issues, that have been raised by consumers.

| | |
|---|---|
| 78%<br><br>Percentage of the top 20 companies on the FTC's Top Violators Reports that have had a public FTC investigation concerning their advertising, marketing, data privacy, or data security practices.[92] | 93.8%<br><br>Percentage of FTC enforcement actions that target a company found in the FTC's complaint database.[93] |
| 394 – 2,795<br><br>Quantity of complaints filed per month against the top 50 companies tracked. [94] | |

Understanding the implications of the Top Violator Report to your organization:

1. Is your organization identified on the current Top Violators Report?
2. Has your organization ever been identified on a Top Violators Report?
3. If you are not listed on the Top Violator's Report, how close is your organization's complaint volume to those organizations that are on the list?
4. Are competitors in your industry identified on the Top Violators Report?
5. If so, if the FTC initiated an investigation of your competitor what impact would that have on your organization?
6. Are companies which provide service to your organization on the Top Violators Report?
7. If so, do the complaints filed against the competing organization suggest legal compliance issues which may put your organization at risk?
8. Are clients of your organization on the Top Violators Report?
9. If so, if a FTC investigation were to be initiated against your client, could it have a negative impact on your organization?

---

92 Based upon a review of the top 20 violators from complaints volume between 1/1/2009 – 12/12/2014, excluding companies not subject to FTC jurisdiction and complaints that do not relate to corporate behavior (e.g., imposter or spoofing).

93 FTC, Fiscal Year 2015 Performance Report and Annual Performance Plan for Fiscal Years 2015 and 2016, p. 51, https://www.ftc.gov/system/files/documents/reports/fy-2016-2017-performance-plan-fy-2015-performance-report/pprfy16-17_0.pdf

94 FTC, Top Companies Receiving Complaints in Consumer Sentinel (Aug. 1, 2016 – Aug. 31, 2016) (excludes complaints relating to scams connected to impersonating the government).

10. Do you have a system in place to quickly identify any pertinent changes to the Top Violator Report?

## Y. Companies Perceived By FTC As Emerging Threats

As discussed in the previous section, the FTC collects complaints about organizations that allegedly violate the data privacy, data security, advertising, and marketing laws.

Each month DPI creates a "Surge" report that identifies those organizations with the greatest increase in consumer complaint volume. For each organization listed the report indicates the quantity of complaints received in the past two months, the jurisdiction in which the organization is based, and a summary of the complaints filed.

| 12 | 93.8% |
|---|---|
| Number of organizations identified in Surge Report.[95] | Percentage of FTC enforcement actions that target an organization found in the FTC's complaint database.[96] |

Understanding the implications of the Surge Report to your organization:

1. What is the typical month-to-month variation in your organization's complaint volume?

2. Does your typical variation indicate a high likelihood of being identified on a Surge Report?

3. What is the typical month-to-month variation of your competitors?

4. What is the typical month-to-month variation of your key clients?

5. What is the typical month-to-month variation of your service providers?

## Z. Organizing Data Privacy Within A Company

Although organizations have dealt with privacy issues for years, only in the past decade have they begun to view the complexities of privacy as requiring formal organizational structure, dedicated employees, and/or dedicated resources. While in some organizations "privacy" falls within the ambit of the legal department; other organizations have created offices that are focused solely on privacy issues and that report to a Chief Privacy Officer ("CPO"). There is little commonality in how these offices are staffed, funded, or organized. For example, while some CPOs report directly to senior management, others report through a General Counsel or a Chief Compliance Officer.

---

[95] Statistic is based upon the last Surge Report released by the FTC. FTC, October 2014 Surge Report. Note that the FTC has refused to provide additional Surge Reports stating that to do so may interfere with its ongoing investigations.

[96] FTC, Fiscal Year 2015 Performance Report and Annual Performance Plan for Fiscal Years 2016 and 2017, p. 51 https://www.ftc.gov/system/files/documents/reports/fy-2016-2017-performance-plan-fy-2015-performance-report/pprfy16-17_0.pdf.

| | |
|---|---|
| 85%<br>Percentage of CPOs that spend at least 50% of their time on privacy-specific activities.[97] | 9<br>The average number of years of experience CPOs have in privacy related roles.[98] |
| 70%<br>Percentage of Privacy Offices that are housed within the Legal Department.[99] | 29%<br>Percentage of CPOs that report directly to the General Counsel.[100] |
| 3.3 – 25<br>The range of full time employees retained by Fortune 1000 companies to deal specifically with privacy-related issues.[101] | |

If you are creating a privacy office, or reviewing the scope of an existing office, consider the degree to which the office should be responsible for the following functions:

1. Drafting, reviewing, or revising privacy related policies and privacy related procedures *(e.g.,* BYOD policy, website privacy policies, employee privacy codes of conduct).

2. Following privacy related legal developments and trends.

3. Training employees (*e.g*., providing core privacy training to the majority of employees, as well as specialized privacy training for employees that have contact with personal information).

4. Responding to privacy related complaints or questions.

5. Assisting the organization in negotiating contracts in which the organization is providing privacy related representations, warranties, guarantees, or indemnification (*i.e.,* client-facing agreements).

6. Participating in the organization's incident response team.

7. Conducting privacy risk assessments or privacy impact assessments.

8. Assisting the organization when negotiating privacy provisions in contracts in which the organization is providing data to third parties (*e.g.,* reviewing privacy practices of vendors and negotiating appropriate contractual guarantees).

---

97 IAPP, Benchmarking Privacy Management and Investments of the Fortune 1000, p.13 (2014), https://iapp.org/resources/article/full-report-benchmarking-privacy-management-and-investments-of-the-fortune-1000/.

98 *Id.* at 11.

99 IAPP, IAPP-EY Annual Privacy Governance Report 2016, p.xii (2016), https://iapp.org/media/pdf/resource_center/IAPP%202016%20GOVERNANCE%20SURVEY-FINAL3.pdf.

100 *Id*. at .xviii.

101 IAPP, Benchmarking Privacy Management and Investments of the Fortune 1000, p. 17, 20 (2014), https://iapp.org/resources/article/full-report-benchmarking-privacy-management-and-investments-of-the-fortune-1000/. Survey found that on average companies in the Fortune 1000 with an "early stage" privacy program had 3.3 FTEs whereas companies with a "mature stage" privacy program had 25 FTEs.

9. Conducting a data inventory or a data map.

10. Monitoring or auditing the organization's privacy-related practices.

11. Reporting to senior management any significant privacy related risks or concerns.

12. Managing the cross-border transfer of information between jurisdictions with different privacy standards.

13. Working with developers, designers, or marketers to design privacy protections into new products, services, or promotions.

## AA. Responding To Government Subpoenas And Document Requests That Ask For Personal Information

Federal and state agencies traditionally obtain information for law enforcement purposes using a variety of methods including:

- court issued subpoenas,
- grand jury subpoenas,
- search warrants,
- litigation discovery requests, and
- administrative subpoenas. [102]

A request by a government agency for personal information about one, or more, consumers may conflict with consumers' expectations of privacy, and, in some instances, may arguably conflict with legal obligations imposed upon an organization not to produce information. For example, if an organization promises within its privacy policy that it will never share the information that it collects with a "third party" and does not include an exception for requests from law enforcement, or government agencies, a consumer could argue that by producing information pursuant to a government request, an organization has violated its privacy policy and committed an unfair or deceptive practice in violation of federal or state law.

| 335 |
| --- |
| Number of federal authorities that permit various federal agencies to issue administrative subpoenas.[103] |

[102] We use administrative subpoenas here to refer to "all powers, regardless of name, that Congress has granted to federal agencies to make an administrative or civil investigatory demand compelling document production or testimony" U.S. Department of Justice Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities Pursuant to Public Law 106-544, [hereinafter DoJ Report] available at http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4078&context=flr.

[103] *Id.*

If you receive a government request for personal information, consider the following steps and questions:

1. Does your organization maintain an internal procedure or protocol for how to respond to a government information request?

2. Has your organization made any representations to consumers that might be interpreted as indicating that information will not be provided to the government?

3. Was the information request actually issued by the agency that purported to issue it (*i.e.*, independently confirm with the issuing agency that the request is authentic)?

4. Confirm that the issuing agency does, in fact, want you to produce personal information.

5. Has the government agency provided notice to the people about whom the information relates of the request?

6. Does the request include a legal basis (e.g., an authorizing statute) for making the information request? If so, does the authorizing statute permit the agency to obtain the type of information requested?

7. Does the authorizing statute require the agency to comply with a specific procedural process prior to requesting the information? If so, has the agency complied?

8. Will complying with the information request pose an undue burden on your organization?

9. Has the request been issued, or reviewed, by a Court?

10. What opportunities does your organization have to negotiate with the agency to limit the quantity of personal information produced and/or to seek administrative or judicial review concerning the agency's need to obtain personal information?

## BB. Responding To National Security Letters That Ask For Personal Information.

National Security Letters ("NSLs") refer to a collection of statutes that authorize certain government agencies to obtain information and simultaneously impose a secrecy obligation upon the recipient of the letter.

Four statutes permit government agencies to issue NSLs: (1) the Electronic Communication Privacy Act,[104] (2) the Right to Financial Privacy Act,[105] (3) the National Security Act,[106] and the (4) Fair Credit Reporting Act.[107] Although differences exist between the NSLs

[104] 18 U.S. C. § 2709.

[105] 12 U.S.C. § 3414.

[106] 50 U.S.C. § 3162.

[107] 15 U.S.C. § 1681v; 15 U.S.C. § 1681u.

issued under each statute, in general, all of the NSLs permit a requesting agency to prevent an organization that receives the NSL from disclosing the fact that it received the request, or the type of information that was requested, if disclosure may result in a danger to national security, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. If the recipient of a NSL wishes to challenge a non-disclosure request accompanying a NSL, the recipient may file a petition with a U.S. district court in the district where the person does business,[108] or the recipient may request that the requesting agency obtain judicial review of the nondisclosure request.[109] In both instances, the requesting agency must file an application with the court setting forth the reasons for the nondisclosure request.

Notwithstanding any nondisclosure requests, NSL recipients may publicly report on a semiannual or annual basis certain information regarding aggregate NSL requests the entity receives.[110] The information that may be reported is limited to identifying in aggregate the rough quantity of NSL requests received (*e.g.*, 0-99 or 0-249) depending on the reporting format chosen.[111]

| 4 | 46,648 |
|---|---|
| Number of statutes that authorize federal agencies to issue NSLs. | Number of NSLs that a single federal agency (FBI) issued in a single year.[112] |

If you receive a NSL, consider the following steps and questions:

1. Does your organization maintain an internal procedure or protocol for how to respond to a government information request, and specifically to a NSL? If so, to the extent permitted under the NSL, follow the procedure to ensure internal awareness of the request.

2. Was the information request actually issued by the agency that purported to issue it? Consider independently confirming with the issuing agency that the request is authentic.

3. Confirm that the issuing agency does, in fact, want you to produce personal information. If so, attempt to negotiate with the issuing agency to reduce the type or volume of personal information requested.

4. Is the issuing agency permitted, under the statutes discussed above, to issue NSLs?

5. If so, does the statute upon which the agency relies apply to your organization?

6. If so, does the statute upon which the agency relies permit the agency to collect the type of information requested?

---

108 18 U.S.C. § 3511(b).

109 *Id.*

110 50 U.S.C. § 1874.

111 *Id.*

112 Semiannual Classified Congressional Reports concerning 2011.

7. Will complying with the NSL conflict with any contractual, statutory, or international privacy obligations? If so, consider raising this issue with the requesting agency to determine whether the NSL can be amended to avoid the conflict.

## CC. Responding To Third Party (Non-Government) Civil Subpoenas And Document Requests That Ask For Personal Information

Litigants in a civil dispute often use subpoenas, subpoenas *duces tecum*, and discovery requests to obtain personal information about individuals who may not be present in the litigation. A request for documents and information that include personal information about third parties may conflict with legal obligations imposed upon an organization not to produce information. For example, if an organization promises within its privacy policy that it will never share personal information with a "third party," and does not include an exception for requests made in civil litigation or through judicial process, a consumer could argue that by producing information pursuant to a subpoena or discovery request an organization has violated its privacy policy and committed an unfair or deceptive practice in violation of federal or state law.

In addition, some states have adopted specific statutes or procedural rules that are designed to protect the privacy interests of absent consumers. For example, California Civil Procedural Rule § 1985.3 prevents a party from issuing a subpoena for personal information from a variety of organizations including medical providers, banks, credit unions, lenders, brokerage firms, or insurance companies, unless the party issuing the subpoena provides a copy to the consumer whose records are sought, and informs them that they have a right to object to the organization furnishing information about them. The rule also requires that the party issuing the subpoena provide the consumer sufficient time to receive, and object, before production is anticipated.

| Nearly 100 Million | 361,689 |
|---|---|
| Number of Cases Opened in State Courts in 2013.[113] | Number of Cases filed in Federal District Courts in 2015.[114] |

If you receive a subpoena or document request asking for personal information about consumers consider the following steps and questions:

1. Does your organization maintain an internal procedure or protocol for how to respond to a subpoena or civil discovery request?

2. Has your organization made any representations to consumers that might be interpreted as indicating that information will not be provided to a requesting party, or that your organization will take certain steps (*e.g.,* informing them of the request) before producing such information?

[113] National Center for State Courts, Court Statistics Project, "Examining the Work of State Courts: An Overview of 2013 State Court Caseloads" p. 2 (Available at: http://www.courtstatistics.org/~/media/Microsites/Files/CSP/EWSC_CSP_2015.ashx).

[114] Administrative Office of the United States Courts, "Federal Judicial Caseload Statistics 2015 (Available at: http://www.uscourts.gov/statistics-reports/federal-judicial-caseload-statistics-2015).

3. Does a law within the state in which the consumer is resident restrict or prevent you from complying with the subpoena?

4. Does a law within the state from which the subpoena is issued restrict or prevent you from complying with the subpoena?

5. Is a protective order in place that would mitigate against privacy harms that might occur from disclosure?

6. If so, is the protective order sufficient to protect a consumer's privacy interest?

7. Has a court already evaluated the information request and weighed the privacy implications of production?

# II. DATA SECURITY

## A. Written Information Security Policies

Although federal law only requires that financial institutions and health care providers maintain a written information security policy or "WISP," approximately thirty four states have enacted legislation that requires organizations in other industries to take steps to keep certain forms of personal information safe. These statutes are broadly referred to as "safeguards" legislation. In some states safeguards legislation requires that organizations adopt certain security-oriented practices such as encrypting highly sensitive personal information or irrevocably destroying sensitive documents. In other states safeguards legislation requires the adoption of a comprehensive written information security policy.

| 5 | 4 | 8 |
|---|---|---|
| Number of states that require that some, or all, of the security program be memorialized in writing.[115] | Number of states that require that an employee be designated to maintain the security program.[116] | Number of states that require that a security provision be included in contracts with service providers.[117] |
| $100 - $500,000<br>Range of Sate Safeguard Law Penalties.[118] | | |

The following are the most popular types of personal information protected by state statutes:[119]

| | |
|---|---|
| 91% | Social Security Numbers |
| 74% | Financial Account Number |
| 72% | Driver's License Number |
| 31% | Health records |
| 15% | Federal, State, or Local Tax Returns |
| 12.5% | Biometric data |

Top 10 sections typically included in a WISP:

1. Designated employee responsible for overseeing security program.
2. Procedures for appropriately destroying documents with sensitive information.
3. Encryption standards for mobile devices.
4. Encryption standards for transmitting sensitive information.

---

115 Bryan Cave LLP, Survey of State Safeguards Laws, (2015).

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.*

5. Employee training.

6. Data breach incident response.

7. Vendor management.

8. Process for provisioning user access.

9. Process for de-provisioning user access.

10. Disciplinary measures for security violations.

## B. De-Identification, Anonymization, and Pseudonymization

De-identification of data refers to the process used to prevent personal identifiers from being connected with information. The FTC indicated in its 2012 report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* that the FTC's privacy framework only applies to data that is "reasonably linkable" to a consumer.[120] The report explains that "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[121] With respect to the first prong of the test, the FTC clarified that this "means that a company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[122] Thus, the FTC recognizes that while it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is a reasonable basis to believe that the remaining information in a particular record cannot be used to identify an individual. The FCC has adopted in its Broadband Privacy Order the FTC's three-part de-identification test.[123]

De-identification is not a single technique, but rather a collection of approaches, tools, and algorithms that can be applied to different kinds of data with differing levels of effectiveness. In 2010, the National Institute of Standards and Technology (NIST) published the *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* that provides a set of instructions and de-identification techniques for federal agencies, which can also be used by non-governmental organizations on a voluntary basis. The guide defines "de-identified information" as "records that have had enough PII removed or obscured, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual."[124]

---

120 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, (March 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

121 *Id*. at iv.

122 *Id*. at 21.

123 *Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 30 FCC Rcd ___ (2016), para. 106, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1103/FCC-16-148A1.pdf.

124 National Institute of Standards and Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), (April 2010), available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

| 18 | <.25% | 4 |
|---|---|---|
| The number of specific types of data that must be removed from a health record to qualify under the HIPAA "Safe Harbor" De-Identification Method.[125] | The re-identification risk found by two studies of health records that had been de-identified using field suppression methods.[126] /[127] | The number of randomly chosen observations of an individual that could be used to uniquely identify 95% of "mobility traces" (a record of locations and times that a person or vehicle visited over a year).[128] |
| Key Definition: "**Anonymization"** of data refers to a subcategory of de-identification whereby data can never be re-identified. This differs from de-identified data, which is data that may be linked to individuals using a code, algorithm, or pseudonym. | | |
| Key Definition: "**Pseudonymization**" of data refers to a procedure by which personal identifiers in a set of information are replaced with artificial identifiers, or pseudonyms. | | |
| Key Definition: "**Aggregation**" of data refers to the process by which information is compiled and expressed in summary form. | | |

NIST has identified the following five techniques that can be used to de-identify records of information:

1. Suppression: The personal identifiers can be suppressed, removed, or replaced with completely random values.

2. Averaging: The personal identifiers of a selected field of data can be replaced with the average value for the entire group of data.

3. Generalization: The personal identifiers can be reported as being within a given range or as a member of a set (i.e., names can be replaced with "PERSON NAME").

4. Perturbation: The personal identifiers can be exchanged with other information within a defined level of variation (i.e., DOB may be randomly adjusted -5 or +5 years).

5. Swapping: The personal identifiers can be replaced between records (i.e., swapping the ZIP codes of two unrelated records).

## C. Encryption

Encryption refers to the process of converting data into a form that is unreadable unless the recipient has a pre-designated algorithm, "key," and password to convert the information into

[125] 45 CFR 164.514.

[126] Kathleen Benitez and Bradley Malin, "Evaluating re-identification risks with respect to the HIPAA privacy rule," J. Am Med Inform Assoc. 2010; 17:169-177.

[127] Peter K. Kwok and Deborah Lafky, "Harder Than You Think: A Case Study of Re-identification Risk of HIPAA Compliant Records," Joint Statistical Meeting, August 2, 2011.

[128] Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility," Scientific Reports 3 (2013), Article 1376.

readable text. Most statutes, regulations, and agencies that require that companies utilize encryption to protect data do not mandate that a specific encryption standard be used. Some statutes do require, however, that companies use an encryption key that is at least 128-bits in length.

When examining whether a company's use of encryption is reasonable and appropriate for the type of data collected and the risks posed to that data, regulators often examine whether a company utilizes encryption "at rest" and/or "in transit." Encryption "at rest" refers to encryption applied to data while it is being stored. Encryption "in transit" refers to encryption applied to data while it is being transmitted across a network. Depending upon the type of software being used, and the architecture of a database, encryption at rest may significantly impair the ability of the data to be accessed and used efficiently.

| | | |
|---|---|---|
| 6<br>Number of states that require that sensitive information be encrypted when sent across public networks.[129] | 1<br>Number of states which explicitly require that sensitive information be encrypted when sent wirelessly.[130] | 1<br>Number of states which explicitly require that sensitive information be encrypted when stored on laptops or on portable devices.[131] |
| 51<br>Data breach notification statutes that contain a safe harbor for encrypted data.[132] | | |
| 87%<br>The number of locked devices in 2016 that the FBI claimed it could access despite widespread encryption technology.[133] | | |

What to think about when designing, or reviewing, an encryption policy:

1. What types of data does our organization encrypt?
2. Is the data encrypted at rest?
3. Is the data encrypted in transit?
4. Is the data encrypted when stored on personal storage devices?
5. What encryption standards are used at rest and/or in transit?
6. Are those encryption standards considered "strong" within the security community?

---

129 Bryan Cave Survey of State Safeguard Statutes (2015).

130 *Id.*

131 *Id.*

132 *Id*. Applies where the encryption key has not been acquired.

133 The FBI's Approach to the Cyber Threat, *remarks delivered by James Comey, Director of the Federal Bureau of Investigation* (August, 30, 2016), available at: https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat.

7. Does your state require a specific encryption standard?

8. Is there evidence that the encryption key could have been compromised?

9. Is there a process to review the sufficiency of the encryption standard periodically (*e.g.,* once per year)?

10. Has your organization contractually agreed to maintain a specific encryption standard?

## D. Document Retention Periods

Data minimization can be a powerful – and seemingly simple – data security measure. The term refers to retaining the least amount of personal information necessary in order for an organization to function. Less information means that there is less that the organization needs to protect, and less opportunity for information to be lost or stolen.

In practice data minimization requires organizations to fully understand where they collect information, why they collect information, and where it is stored. It also requires difficult decisions regarding what information the organization will likely need in the future from a business perspective, and what impact having limited consumer or employee records may have on potential legal disputes if they arise. For example, an organization that chooses to implement a 30 day or 60 day automatic "roll off" policy for employee email may not be able to identify email exchanges between an employee and a vendor that relate to a contract dispute that arises months later.

| | |
|---|---|
| > 8,000 emails<br>Average size of employee inbox.[134] | 6.5 million<br>Number of pages of Word data files that could be on a 100GB hard drive.[135] |
| 18 months[136]<br>Length of time search history is kept by Yahoo. | |
| "The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and hold onto personal information unnecessary to an identified purpose. Keeping data on the off-chance that it might prove useful is not consistent with privacy best practices."<br>- FTC Chairwoman Edith Ramirez[137] | |

What to think about when designing a retention policy:

[134] Dave Troy, The Truth About Email: What's A Normal Inbox? (April 5, 2013) https://pando.com/2013/04/05/the-truth-about-email-whats-a-normal-inbox/.

[135] *See*, netdocuments, File Sizes and Types, https://support.netdocuments.com/hc/en-us/articles/205219000-File-Sizes-and-Types.

[136] Yahoo, Data Storage and Anonymization FAQ, https://policies.yahoo.com/us/en/yahoo/privacy/topics/datastorage/index.htm;

[137] Edith Ramirez, The Privacy Challenges of Big Data: A View From the Lifeguard's Chair, Keynote Address Technology Policy Institute Aspen Forum, (August 19, 2013), https://www.ftc.gov/public-statements/2013/08/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair.

1. Do you systematically track all of the data fields that your organization collects from consumers and employees?

2. Do you systematically apply retention periods to each data field that you collect?

3. Do those retention periods reflect the current business needs, or estimates as to possible future business needs?

4. For a particular data field, what time period is typical in your industry and for the type of data at issue?

5. Should you attempt to anonymize (sometimes called de-identify) data after a certain amount of time?

6. If you do anonymize data, is your organization's process of anonymization legally sufficient?

7. What data and documents are you legally required to retain, and for how long must they be retained?

8. If you decide to retain other data and documents how does it increase, or decrease, your legal risk?

9. What additional data that, if collected, is your organization likely to need in the next 12 months?

10. What steps are taken to irrevocably destroy data that is no longer needed?

11. Are there any contractual requirements that require you to keep data for a certain duration?

12. Does the retention policy include an annual review process?

## E. Cyber Insurance

Most organizations know they need insurance to cover risks to the organization's property like fire or theft, or their risk of liability if someone is injured in the workplace. But, a substantial portion of organizations don't carry coverage for data breaches despite numerous high profile breaches. While many insurance companies offer cyber insurance, not all policies are created equal.

| 19% | 52% | 46% |
|---|---|---|
| Percentage of companies that had cyber-insurance in 2015.[138] | Percentage of companies that believed their exposure to cyber risk would increase in the next 24 months.[139] | Percentage of companies that did not plan to purchase cyber insurance in the next 24 months.[140] |

[138] Ponemon, 2015 Cyber Impact Report, (April 2015), http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf.

[139] *Id.*

Why is buying cyber insurance difficult?

1. There is little standardization among competing policies; as a result it is hard to comparison shop.

2. Policies' exclusions often swallow coverage; as a result, assessing the value of a policy is difficult unless you have extensive experience with the types of liabilities that arise following data breaches.

3. Policies often cover security but not privacy risks.

Items to review when shopping for cyber insurance:

1. Do the sub-limits on coverage match the corresponding risks?

2. Does the policy include sub-retentions (sub-deductibles) that are unlikely to be reached?

3. Does exclusion prevent payment for the largest risks, *e.g.*, charges that arise following a credit card breach, common theories alleged in class actions, etc.?

4. Is voluntary notification of affected consumers covered?

5. Will credit monitoring for affected consumers be covered?

6. Who does the insurer have on panel for legal representation, forensic investigations, and/or crisis management?

## F. Bounty or Bug Programs

Data security officers typically look for security risks by monitoring reports from automated security systems, listening to employees' reports of security issues, and/or auditing IT systems. There is a great deal of debate, however, about the merits of listening to the security concerns of people outside of an organization. On one end of the spectrum, some organizations refuse to discuss any aspect of their security with the public. On the other end of the spectrum, organizations proactively encourage the public to report security vulnerabilities by paying well-meaning hackers (usually called "white hat hackers" or "independent researchers") to report problems. While these organizations view "bounty" programs as commonsense crowdsourcing, others view the concept of paying someone who has hacked a company's system as extortion. As more companies move to establish bounty programs third parties have begun to offer platforms or frameworks to help organize the programs. Some frameworks provide a forum in which companies can communicate with hackers, a method to facilitate payments to hackers, and guidelines for hackers to follow when identifying vulnerabilities and reporting them to participating companies.

The following provides a snapshot of information on bounty programs as well as a checklist for organizations that are considering starting a program, or are evaluating the structure of their existing program.

---

[140] *Id.*

| 489 | 53% | $100k |
|---|---|---|
| The number of organizations that have established data security bounty programs (as of November 11, 2016).[141] | The percentage of bounty programs that pay a bounty.[142] | One of the largest maximum rewards offered through a bounty program (as of November 11, 2016).[143] |
| $100 to $25,000<br>Typical range of rewards offered for programs that pay monetary compensation. | | |

What to think about when considering a bounty program:

- If you do not enact a bounty program:

    1. What are the practical implications if the organization views any hack as "unauthorized?"

    2. What are the practical implications if a "white hat" hacker tries to breach your security with no guidelines on how they should act?

    3. Is there a risk that individuals who know of a security vulnerability may provide that information to bad actors instead of providing it, first, to you?

    4. Is there a risk that individuals who know of a security vulnerability may provide that information to the media or to regulators instead of providing it, first, to you?

    5. Would the organization view an unsolicited request for payment by a hacker as extortion?

- If you do enact a bounty program:

    1. Will you be encouraging more breaches to your system?

    2. Do you have confidence that you can track / monitor successful participants?

    3. Will all of your systems be "in scope" for the bounty program?

    4. Should certain forms of attack be prohibited (e.g. denial of service attaches)?

    5. Will employees be eligible to participate?

    6. Will the program be focused on weaknesses to the security of sensitive personal information, to the performance of IT infrastructure, or to both?

---

141 Statistics from Vulnerability Laboratory, Bug Bounties, Rewards, and Acknowledgements, http://vulnerability-lab.com/list-of-bug-bounty-programs.php.

142 Based upon review of data obtained from vulnerability labs, infra.

143 Microsoft has posted various $100,000 awards, *see* https://technet.microsoft.com/en-us/library/dn425036.aspx

7. Will you proactively disclose the level of compensation that a participant should expect?

8. What conditions of confidentiality will you impose on participants?

9. How can you avoid the unintentional access or acquisition of sensitive personal information?

10. How will you receive and document security vulnerabilities?

11. Will you utilize a third party that manages, hosts, or provides a framework for your program?

## G. Cyber-Extortion

Cyber extortion refers to a situation in which a third party threatens that if an organization does not pay money, or take a certain action, the third party will take an adverse action against the organization. Among other things, threats may include exploiting a security vulnerability identified by the extorter, reporting the organization's security vulnerability to the press, or reporting the organization's security vulnerability to regulators.

The following provides a snapshot of information concerning cyber-extortion as well as a checklist for organizations that are confronted by an extortion demand:

| $209 Million | 85% |
|---|---|
| The amount collected by cyber-extortion criminals in 2015.[144] | Estimate of the percentage of cyber-extortion cases that are not reported.[145] |
| $2,500 to $100,000 | |
| Range of unsolicited demands related to alleged security vulnerabilities made to Bryan Cave clients between 2014 and 2015. | |

What to think about when considering a cyber extortion demand:

1. Is the threat credible?

2. If the exploitation of a security vulnerability is threatened, can the organization identify the vulnerability without the aid of the extortionist?

3. If the disclosure of non-public information is threatened, is there any evidence that the information has not already been disclosed or shared with others?

4. If an extortion demand is paid what is the likelihood that your organization will receive similar demands in the near future?

[144] David Fitzpatrick and Drew Griffin, Cyber-Extortion Losses Skyrocket, http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/.

[145] NYA International, Cyber Extortion Risk Report (Oct. 2015) at 3.

5. If your organization were to pay the demand is it likely that the recipient of the funds may be associated with terrorism or located in a restricted country?

6. Is cyber-extortion covered under your cyber insurance policy?

## H. Ransomware

Some forms of cyber extortion are automated and not targeted at any specific victim. For example, "ransomware" refers to a type of malware that prevents users from accessing their systems unless, and until, a ransom is paid. Although variants of ransomware operate differently many encrypt the contents of a victim's hard drive using asymmetric encryption in which the decryption key is stored on the attacker's server and is available only after payment of the ransom. Victims typically discover the ransomware when they receive an on-screen message instructing them to transfer funds using an electronic currency, such as bitcoin, in order to receive the decryption key and access to their files. "CryptoLocker" is the most famous ransomware family and first appeared in 2013.

In November 2016, the FTC issued guidance for businesses on how to avoid and respond to ransomware attacks in its *How to defend against ransomware*[146] and *Ransomware – A closer look*.[147]

The following provides a snapshot of information concerning ransomware:

| | | |
|---|---|---|
| 1,402<br>The number of entities that reported being victimized by Ransomware over a six month period.[148] | $300<br>The average ransom amount associated with ransomware.[149] | 400%<br>Percentage increase in new ransomware attacks.[150] |
| $200 - $5,000<br>Typical range of ransomware demands.[151] | | |

What to think about if your organization is impacted by ransomware:

1. Is the ransomware designed to export data before encrypting it?

2. If so did the impacted data contain any personally identifiable information that might implicate a data breach notification statute?

---

146 FTC, How to defend against ransomware (November 10, 2015), https://www.consumer.ftc.gov/blog/how-defend-against-ransomware?utm_source=govdelivery.

147 FTC, Ransomware – A closer look, (November 10, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look?utm_source=govdelivery.

148 FBI, 2014 Internet Crime Report at 47 *available at* IC3.gov (last viewed Nov. 22, 2015).

149 Symantec, Security Response: The Evolution of Ransomware (Aug. 6, 2015) at 5.

150 Beazley, Beazley Breach Insights (October 2016) at 1, available at: https://www.beazley.com/documents/Insights/201610-ransomware-attacks-set-to-quadruple-in-2016.pdf.

151 FBI, Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Treat (Jan. 20, 2015).

3. Is it possible for your organization to recover the impacted files using backup systems?

4. Is the variant of ransomware involved associated with a known criminal enterprise?

5. Should your organization contact law enforcement?

6. Should your organization make the attack publicly known?

7. If your organization were to pay the ransom demand, is it likely that the recipient of the funds may be associated with terrorism or located in a restricted country?

8. Is cyber-extortion and/or ransomware covered under your cyber insurance policy?

9. What systems within your organization are at the greatest risk of a ransomware attack, and are they protected?

10. Have you prepared sufficient backups of critical systems and data?

## I. FDIC Cybersecurity Examinations

FDIC bank examinations generally include a focus on the IT systems of banks with a particular focus on information security. The federal banking agencies issued *Interagency Guidelines Establishing Information Security Standards* ("Interagency Guidelines") in 2001. In 2005, the FDIC developed the Information Technology—Risk Management Program (IT-RMP), based largely on the Interagency Guidelines, as a risk-based approach for conducting IT examinations at FDIC-supervised banks. The FDIC also uses work programs developed by the Federal Financial Institutions Examination Council ("FFIEC") to conduct IT examinations of service providers.

The examination process relies on bank management attestations regarding the extent to which IT risks are being managed and controlled. Examiners focus their efforts on management-identified weaknesses and may confirm selected safeguards described by management as adequate. Nonetheless, reports by the Office of the Inspector General within the FDIC indicate that examiners may not be consistent in their review of bank compliance with the Interagency Guidelines and do not regularly provide a clear statement of adequacy on intrusion detection programs and incident response plans.

| 2,323 | 8-10 days | 15- 20 days | 20% |
|---|---|---|---|
| Number of IT examinations at financial institutions and technology service providers conducted by FDIC in a year.[152] | Time spent by FDIC to perform an IT examination at a financial institution found to have adequate security.[153] | Time spent by FDIC to perform an IT examination at a financial institution found to have some degree of supervisory concern.[154] | Percentage of Consent Orders issued in 2015 specifically citing deficiencies in IT as a basis for the Order. Over 50% involve either IT deficiencies or BSA and Compliance issues. |

What bank directors should be thinking about when preparing for an examination:

1. Is the Board comfortable that the Bank has management qualified to oversee all aspects of the Bank's IT operations, including compliance with all applicable data security laws and regulations?

2. Is there a designated Vendor Management Coordinator in the Bank with an appropriate level of due diligence and vendor risk modeling experience for the type and quality of the Bank's IT services?

3. Do the directors understand what IT services are being outsourced and whether the Bank's Vendor Management Program meets the requirements and guidance of the FFIEC IT Examination Handbook, Outsourcing Technology Services?

4. Does the Bank's Business Continuity Planning/Disaster Recovery Plan ("BCP/DR" Plan) adequately address the sudden loss of IT services?

5. When did senior management last review the organization's incident response portion of the BCP/DR Plan?

6. Has the incident response plan been strategically tested (e.g., a breach tabletop simulation)?

7. Has the incident response plan been operationally tested (e.g., a breach simulation)?

8. Does the organization have a plan for how it would communicate a breach to bank customers, regulators and law enforcement?

9. Has the organization retained cyber insurance coverage? Does management understand what is, and what is not, covered under the policy?

[152] FDIC Office of Inspector General, Report No. EVAL-15.003 (Mar. 2015).

[153] *Id.*

[154] *Id.*

10. Does the organization have external resources already identified, and under contract, to provide assistance in the event of a security incident?

## J. Wire Transfer Fraud

Businesses are increasingly falling victim to wire fraud scams – sometimes referred to as "man-in-the-email" or "business email compromise" scams. Although there are multiple variants, a common situation involves an attacker gaining access to the email system of a company, or the company's vendor, and monitoring email traffic about an upcoming transaction. When it comes time to submit an invoice or a payment, the attacker impersonates one of the parties and sends wire instructions asking that payment be sent to the attacker's bank account.

Wire fraud scams often victimize two businesses – the business that expected to receive payment, and the business that thought that they had made payment. The scam can cause significant contractual disputes between the victims as to who should bear the loss.

| 7,066 | $747 million | 270% |
|---|---|---|
| The number of businesses victimized by wire transfer fraud.[155] | The amount of money lost in the US due to wire transfer fraud.[156] | Increase in identified victims and exposed loss from January 2015 to April 2016.[157] |

Steps to help avoid wire fraud scams:

1. Avoid free web-based email systems to transact business.

2. Enable multi-factor authentication to log into all email systems.

3. Require employees to select unique and strong passwords or pass phrases.

4. Require employees to change email passwords frequently.

5. Require multi-factor authentication (e.g., email and telephone call) when receiving initial payment information.

6. Require multi-factor authentication when receiving a request to change payment information.

7. Send a confirmatory letter or email (not using the "reply" feature in email) concerning any request to change payment information.

8. Delay payment in connection with any request to change payment accounts or a request to make payment to a foreign bank account.

---

155 Federal Bureau of Investigation, Alert No. I-082715a-PSA (August 27, 2015), http://www.ic3.gov/media/2015/150827-1.aspx#fn2 (time period for reporting 10/1/2013 – 8/1/2015).

156 *Id.*

157 Federal Bureau of Investigation, FBI Warns of Dramatic Increase in Business E-Mail Scams (April 2016), https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams.

9. Review any request received by email to change payment accounts for signs that the email may be from a third party.

10. Provide clear instructions to business partners concerning how payment information should be communicated.

If you are victimized by wire fraud, consider:

1. Notifying the receiving bank and request that a freeze be placed on any remaining funds.

2. Notifying law enforcement.

3. Investigating whether your email system may have been compromised.

4. Asking business partners to investigate whether their email systems may have been compromised.

## K. Tax Filing Fraud

Tax returns and W-2s are information rich documents that contain the name and Social Security Number of an employee, as well as information concerning their salary and address, and personal behavior and characteristics (*e.g.,* the charities that they support, their sources of income, their investments, and their relationships with financial institutions). Each year cyber-attackers target these documents. If successful, an attacker may attempt to sell sensitive information contained in the file. Other attackers may attempt to use tax-related documents (e.g., an employee's W-2) to submit a fraudulent income tax return in the hope of obtaining any refund owed to an employee.

There are many methods by which an attacker may attempt to obtain tax related information. The most visible have been large hacking attempts against the Internal Revenue Service itself. Other attackers attempt to obtain tax documents from employers. For example, in 2016 IRS Commissioner Kohn Koskinen highlighted spear phishing attempts against human resource departments: "This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees." The following provides a snapshot of information regarding tax filing fraud.

| 1,026 | 403% |
|---|---|
| The number of phishing scams for W2's reported to the IRS in January of 2016.[158] | The percentage increase in reported phishing attempts between January 2015 and January 2016.[159] |

[158] https://www.irs.gov/uac/Newsroom/Consumers-Warned-of-New-Surge-in-IRS-Email-Schemes-during-2016-Tax-Season-Tax-Industry-Also-Targeted .

[159] *Id.*

Employers should consider taking the following steps to help prevent a data breach of your employee tax records:

1) If you receive a request from an executive to email large quantities of employee information, verify that request by telephone before responding.

2) If the request appears legitimate, consider transmitting the data using a secure connection and not by email.

3) If you need to transmit tax information by email, encrypt the document before sending it.

4) Never use a formulaic or easy-to-guess password for an encrypted file (e.g. employee's last name).

5) Do not publicly post any information that your employees may need to access their tax related information online.

6) Track the rate of tax related fraud reported to your Human Resource department each year. If the quantity of tax reported fraud is significantly greater this year than it was in previous years, consider investigating whether data may have been breached.

7) If you have fallen victim to email phishing, talk to your outside counsel about notification requirements and whether it makes sense to provide employees with credit monitoring services.

## L. Incident Response Plans

The best way to handle any emergency is to be prepared. When it comes to data breaches incident response plans are the first step organizations take to prepare. Furthermore, many organizations are required to maintain one. For example, any organization that accepts payment cards is most likely contractually required to adopt an incident response plan.

A good incident response plan does not attempt to predict every type of breach that may occur. Rather the fundamental components of an incident response plan is that it establishes the framework for who within an organization is responsible for investigating a security incident, what resources that person has at their disposal (inside and outside of the organization), and when a situation should be elevated to others within the organization. They can also provide a reference guide for the type of actions common to most security investigations.

| $17 / record. | 22% | 78% | 17% |
|---|---|---|---|
| The amount one study suggests having a written incident response plan lowers the cost of a data breach.[160] | Percentage of companies that have no incident response plan.[161] | Percentage of companies with a plan that have no scheduled review or have never reviewed the plan.[162] | Percentage of companies that are not sure if their plan is effective.[163] |

What are organization's top concerns when it comes to incident response plans?

1. The plan has little relationship to how the organization actually handles security incidents.

2. The plan has never been tested.

3. The plan does not cover all of the issues that arise in a data security incident.

Checklist for drafting an effective incident response plan:

1. The plan assigns a specific person or group to lead an investigation.

2. The plan provides a clear plan for escalating information about an incident.

3. The plan discusses the need for preserving evidence.

4. The plan incorporates legal where appropriate to preserve attorney-client privilege.

5. The plan discusses how the organization will communicate externally concerning an incident.

6. The plan includes contact information for internal resources.

7. The plan includes contact information for pre-approved external resources.

8. The plan is reviewed annually.

9. The plan is tested.

## M. Forensic Investigators

Many competent IT departments lack the expertise, hardware, or software to preserve evidence in a forensically sound manner and to thoroughly investigate a security incident. In-

[160] Ponemon Institute, Is Your Company ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness, p. 1 (September 2014), http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

[161] *Id.*

[162] *Id.* at 21.

[163] *Id.* at 4.

house counsel needs to be able to recognize such a deficiency quickly – and before evidence is lost or inadvertently destroyed – and retain external resources to help collect and preserve electronic evidence and investigate the incident.

Although in the midst of an emergency you may feel that you have relatively little leverage to negotiate preferable terms in a service agreement with a forensic investigator, given the sensitivity of the information to which the investigator will have access it is essential to make sure that your service agreement protects your organization.

| | | |
|---|---|---|
| $4.9 million<br><br>Highest amount spent on a forensic investigation.[164] | $261,597<br><br>Average amount spent on a forensic investigation.[165] | $41,747<br><br>Median amount spent on a forensic investigation.[166] |
| $1,250 - $4.9 million<br>Range of forensic investigation costs.[167] | | |

What to consider when retaining a forensic investigator:

1. Does the forensic investigator have sufficient expertise to conduct the investigation?

2. Does the forensic investigator have sufficient capacity to immediately deploy resources to timely investigate the incident?

3. Is there a master service agreement already in place?

4. Does the agreement contain data security provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?

5. Does the agreement contain data privacy provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?

6. Is the agreement structured to protect attorney-client privilege?

7. Does the forensic investigator understand what you expect of them to maintain attorney-client privilege?

8. Does the agreement include sufficient protections in the event that the forensic investigator is itself breached?

9. If the organization has cyber-insurance, is the forensic investigator a preferred provider and/or approved by the insurer?

---

164 Statistics based upon cyber liability insurance claims. Net Diligence, Cyber Claims Study 2015, p. 9 (2015), http://www.netdiligence.com/NetDiligence_2015CyberClaimsStudy.pdf.

165 *Id.* at 13.

166 *Id.*

167 *Id.* at 12.

10. Does the forensic investigator represent a business partner that may have an interest in the incident? If so, is there a potential conflict of interest?

## N. Credit Monitoring Services

Organizations are not, generally, required to offer services to consumers whose information was involved in a breach.[168] Nonetheless, many organizations choose to offer credit reports (*i.e.,* a list of the open credit accounts associated with a consumer), credit monitoring (*i.e.,* monitoring a consumer's credit report for suspicious activity), identity restoration services (*i.e.,* helping a consumer restore their credit or close fraudulently opened accounts), and/or identity theft insurance (*i.e.,* defending a consumer if a creditor attempts to collect upon a fraudulently opened account and reimbursing a consumer for any lost funds). In addition, if you do offer one of these services a 2014 California statute and a 2015 Connecticut law prohibits you from charging the consumer for them.

Although many consumers believe that credit-related services should be offered following a breach, many (if not most) data breaches do not involve information that could be used to open a credit account. As a result credit-related services often do not protect consumers from any harm that might result from the breach that triggered the offering. In addition, some courts have viewed offers of credit-related services that an organization makes as a gesture of goodwill as an admission by the organization that consumers' credit is, in fact, at risk.[169]

| | | | |
|---|---|---|---|
| 58%<br><br>Percentage of consumers that believe an organization should provide credit monitoring following a breach.[170] | 25%<br><br>Percentage of companies that offer some form of credit-related service in their breach notification letters.[171] | 6x<br><br>The odds of being sued are 6 times lower when an organization offers free credit monitoring.[172] | 4<br><br>The number of credit monitoring services that have been investigated by the FTC for unfair or deceptive practices. |
| \$0.25 - \$2.00<br>Approximate cost of one year of credit-related services per consumer depending upon the number of impacted individuals, the type of information breached, and the services offered. | | | |

What to think about when evaluating a credit-related service:

1. Will the credit monitoring company attempt to upsell enrollees? If so, will recipients of the free service perceive that it is not, in fact, free?

---

168 Connecticut is the first state to require a company to offer an affected individual credit monitoring if the affected individual's name and Social Security Number are involved in a breach.

169 *See*, Remijas v. Neiman Marcus Group, LLC, No. 14-3122 (7th Cir. July 20, 2015).

170 Ponemon Institute, The Aftermath of a Mega Data Breach: Consumer Sentiment, (April 2014), http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.

171 *Id.*

172 Romanosky, et al, Empirical Analysis of Data Breach Litigation, 11(1) Journal of Empirical Legal Studies June 1, 2012), http://www.econinfosec.org/archive/weis2012/papers/Romanosky_WEIS2012.pdf.

2. Will the credit monitoring company market additional products or services to enrollees? If so, will recipients of the service perceive that their privacy has been violated?

3. Will the credit monitoring company allow other companies to cross-market products to enrollees?

4. Is the credit monitoring service permitted to retain information about enrollees after they stop providing service?

5. Has the credit monitoring company provided the organization with adequate assurance (and indemnifications) if the information that you provide to them (e.g., customer lists, lists of impacted consumers, or lists of impacted employees) itself becomes breached?

6. Are you indemnified if the credit monitoring company's products are alleged to be unfair or deceptive?

7. Are you indemnified if the credit monitoring company is negligent in providing monitoring services?

8. Have you been given a copy of all materials, including marketing materials, enrollment terms, insurance contracts, etc., that relate to the service being offered so that you know what your customers/employees are being provided?

9. What service level guarantees are provided for how quickly enrollees will be able to reach the credit monitoring company?

10. Has the credit monitoring company received any complaints, either from regulators or consumers, about its product offering or service?

## O. Reputation Management

The reputational injury following a data breach can be severe. Indeed, reputational injury – including lost customers – often surpasses legal liability.

Effective management of the reputational impact of a data security incident requires a proactive and reactive strategy. The proactive strategy assumes that the organization will control when, and what, information will be conveyed to the public, media, and impacted consumers. For many organizations the proactive strategy that they choose is to wait until their investigation of an incident is complete so that they can provide the public with the most accurate and meaningful information.

The reactive strategy anticipates that the public may be alerted to a possible security incident at a time when the organization may not have full or complete information. The reactive strategy must carefully balance responding to requests from the public for details that may not be known to the organization. While the pressure to provide information can be significant, providing inaccurate, incomplete, or preliminary information can confuse consumers, increase the likelihood of legal liability, and, in the long run, lead to worse reputational injury. Due to the complexities involved, many companies retain third party communications, public relations, or reputational consultants to help manage reputational impact.

| 72% | 45% | 12% |
|---|---|---|
| Percentage of people that reported that they "trusted" family owned businesses.[173] | Percentage of people that reported that they "trusted" big business.[174] | Percentage of customers that boycott a retailer if a data breach has been reported.[175] |
| \$3,964 - \$240,000<br>Range of money spent on a crisis management or public relations firm following a data breach.[176] | | |

What to think about when retaining a consultant to help manage the reputational impact of a security incident:

1. Has the consultant dealt with data breaches in the past? If so, was the strategy advocated by the consultant effective in controlling the reputational impact and quantity of media exposure?

2. Has the consultant dealt with data breaches in the industry in which you operate?

3. What was the most publicized breach that they handled? (Remember that high publicity does not necessarily signify an effective reputation-management strategy).

4. What other breach-related services do they provide? If reputation-management is not the main focus of the consultant, is their practice sufficiently specialized in that area?

5. What is the consultant's general approach to responding to media inquiries about a security incident when a forensic investigation is not complete?

## P. Data Breach Notification Laws

Although Congress has attempted to agree on federal data breach notification legislation, there is no national data breach notification law that applies to most companies. Instead, 47 states, plus the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, have each enacted their own statutes addressing an organization's notification obligations in the wake of a data breach involving personal information. The only states without such laws are Alabama, New Mexico, and South Dakota, although their citizens may be covered in some situations by the data breach laws of other states.

---

173 2015 Edelman Trust Barometer, 7, http://www.edelman.com/insights/intellectual-property/2015-edelman-trust-barometer/trust-and-innovation-edelman-trust-barometer/executive-summary/.

174 *Id.*

175 Interactions Marketing, Retail's Reality: Shopping Behavior After Security Breaches, Retail Perceptions (July 2014), http://www.interactionsmarketing.com/retailperceptions/pdf/Retail_Perceptions_Report_2014_06.pdf.

176 Net Diligence, Cyber Claims Study 2015, (2015), https://netdiligence.com/wp-content/uploads/2016/05/NetDiligence_2015_Cyber_Claims_Study_093015.pdf

While state data breach laws are similar, they are not uniform. The following summarizes some of the key provisions of state data breach notification laws and highlights areas in which state laws diverge. In the event of a breach involving records of consumers who live in multiple states, the laws of each of those states should be reviewed to ensure that the organization is complying with all notification requirements.

| | |
|---|---|
| 51<br><br>Number of states and territories with a breach notification law. | 3<br><br>Number of states that do not have a breach notification law. |
| 40%<br><br>Percentage of state laws that require notifying regulators after some breaches. | 20%<br><br>Percentage of state laws that expressly confer a private right of action to consumers if the statutes is violated. |

What to consider when evaluating state data breach laws:

1. In which jurisdiction do the data subjects reside? Do the laws of those jurisdictions purport to be extraterritorial?

2. Is your organization exempt from the applicable state data breach laws?

3. What types of personal information are covered by the applicable statutes?

4. Do the applicable statutes only require notification if the breach is "material?" If so, what language does the statute use to determine whether a breach is material?

5. If notification to consumers is required, how much time does the statute give you to provide notice?

6. Do the applicable statutes require that you notify state regulators?

7. Do the applicable statutes require that notification letters contain specific types of information?

8. Do the applicable statutes prohibit you from including some types of information in a notification letter?

9. What form should the notification take? A letter? An email? A telephone call?

10. Do the applicable statutes require your organization to notify any third parties?

## Q. Cybersecurity Disclosures

In October of 2011, the U.S. Securities and Exchange Commission ("SEC") issued guidance regarding a public company's obligations to disclose cybersecurity risks and cyber

incidents (the "Cybersecurity Disclosure Guidance").[177] The Cybersecurity Disclosure Guidance applies to all SEC registrants and relates to disclosures under the Securities Act of 1933 and the Securities Exchange Act of 1934.

The SEC staff acknowledged in the Cybersecurity Disclosure Guidance that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, but has made clear that there are a number of disclosure requirements that might impose an obligation on an issuer to disclose such risks and incidents. The Cybersecurity Disclosure Guidance specifically discusses disclosures required when discussing a company's risk factors, MD&A, business descriptions, legal proceedings, financial statements and disclosure controls and procedures. The staff stated that as with other operational and financial matters, issuers "should review, on an ongoing basis, the adequacy of their disclosures relating to cybersecurity risks and cyber incidents," with a view to ensuring timely, comprehensive and accurate information that a reasonable investor would consider material. The staff also made clear that if a cyber incident occurs, such as a data breach, registrants should be certain to disclose any material impact of the incident on their business operations and explain how they have taken steps to mitigate damage.

Since the original publication of the Cybersecurity Disclosure Guidance, the SEC has remained focused on the implications of cybersecurity on public companies and regulated financial service firms. In 2014 the SEC's Office of Compliance Inspections and Examinations issued a national exam program alert providing a framework for assessing cyber risk and announcing a plan to examine a sampling of registered broker-dealers and investment advisors to review their cybersecurity preparedness. All public companies should evaluate their current disclosures to ensure that they are consistent with the Cybersecurity Disclosure Guidance and should consider implementing a readiness plan to ensure appropriate and timely disclosures in the event of a cyber incident.

| 85% | 46% | 53% |
|---|---|---|
| The percentage of Fortune 500 companies that identified cybersecurity risk in a SEC filing in 2012 (the year after the SEC issued the Cyber Disclosure Guide).[178] | The percentage of Fortune 500 companies in 2012 that described the extent of cybersecurity risk as "critical," "significant," "materially harmful," or "seriously harmful" to their business operations.[179] | The percentage of global company executives that described insufficient preparation to manage cyber threats as a risk that could have a "significant impact" on their organizations in 2015.[180] |

What every public company should do about cybersecurity disclosures:

[177] Securities and Exchange Commission, CF Disclosure Guidance Topic No. 2: Cybersecurity, Oct. 13, 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[178] Willis, Fortune 500 Cyber Disclosure Report, 2013, http://www.willis.com/documents/publications/Services/Executive_Risks/2013/FinexNA_Cyber_Update_v2.pdf.

[179] *Id.*

[180] Protiviti, Executive Prospectives on Top Risks for 2015, 2015, http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2015.pdf.

1. Evaluate the company's procedures for assessing the materiality of cybersecurity matters and implement a regular schedule of ongoing review, perhaps in connection with the company's regular quarterly reporting processes.

2. Determine what disclosure should be made in the company's SEC filings based on the company's exposure to a cybersecurity incident and the materiality of actions being taken proactively by the company to mitigate risk.

3. Review the company's current disclosures and compare those disclosures to peer companies with similar cybersecurity risks and issues.

4. Consider establishing a disclosure readiness plan in the event of a cyber incident. Review the implications for such a plan of active shelf registration statements, share buyback programs and other ongoing securities market activities.

5. Ensure involvement by the board of directors or the risk management committee of the board in the cybersecurity risk assessment and disclosure planning.

## R. Class Action Litigation Trends

There is a great deal of misunderstanding concerning data security breach-related class actions. In large part the media and the legal media have exaggerated the quantity (and success) of class action litigation.

The following provides an overview of the risks associated with lawsuits following data security breaches.[181]

| | | |
|---|---|---|
| 4%<br>The percentage of data breaches that lead to lawsuits.[182] | 3x<br>The increased odds of being sued if the breach was caused by a company's unauthorized disclosure or disposal of data.[183] | 6x<br>The decreased odds of being sued if a company provides free credit monitoring following a breach.[184] |
| 52%<br>Settlement rate for data breach lawsuits.[185] | +30%<br>Increase in likelihood of settlement post class-certification.[186] | 10x<br>The increased odds of settlement where the cause of the breach is a cyber-attack.[187] |

[181] Romanosky, et al, Empirical Analysis of Data Breach Litigation, 11(1) Journal of Empirical Legal Studies June 1, 2012), http://www.econinfosec.org/archive/weis2012/papers/Romanosky_WEIS2012.pdf.

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

| -25% | -16% | 20 |
|---|---|---|
| Decline in the quantity of data breach class action filings.[188] | Decline in unique defendants of class action filings.[189] | Number of different legal theories alleged by plaintiffs.[190] |

Factors to look at when considering the likelihood of receiving a class action complaint following a data breach:

1. Is a plaintiff's firm looking at government records for information relating to your organization's data security practices? For example, have they submitted requests to the FTC under the Freedom of Information Act?

2. Was the quantity of records lost lower, or greater, than the average number of records involved in recent class action lawsuits?

3. Did consumers suffer any direct monetary harm?

4. Could the data fields involved lead to identity theft?

5. Has there been any evidence of actual identity theft?

6. Did you offer credit monitoring, identity theft insurance, and/or credit repair services?

7. If so, what percentage of impacted consumers availed themselves of your offer?

8. Has the jurisdiction in which you are most likely to receive a lawsuit (e.g., where you are incorporated or primarily operate your business) permitted other data security class action complaints to proceed past the pleadings stage?

9. Has the media widely reported on your data breach?

10. If so, did the media report your data breach before, or after, the company notified impacted consumers?

## S. Credit Cards and the Payment Card Industry Data Security Standard

For most retailers the primary source of revenue comes from credit card transactions. In order to accept credit cards, a retailer must enter into a contractual agreement with a payment processor and a merchant bank. As discussed above, those agreements typically required that the retailer represent and warrant its compliance with the Payment Card Industry Data Security Standard ("PCI DSS"). Alternatively, they require a representation and warranty that the retailer complies with the rules of the payment card brands (*i.e.,* American Express, Discover,

188 Bryan Cave LLP, Snapshot of Bryan Cave's 2016 Data Breach Litigation Report, https://d11m3yrngt251b.cloudfront.net/images/content/8/3/v2/83697/Data-Privacy-Infographic.pdf

189 *Id.*

190 Bryan Cave LLP, 2016 Data Breach Litigaiton Report, at 9, available at https://d11m3yrngt251b.cloudfront.net/images/content/8/2/v2/82494/DataBreachLitigationReport.pdf.

MasterCard, and Visa), and some of the payment brand rules could be interpreted as requiring that a retailer be compliant with the PCI DSS.

The PCI DSS is a standard that originally was established by the payment brands, and later transferred to the Payment Card Industry Security Standards Council ("PCI SSC") for management and further development. The standard sets forth what the payment brands contend is a baseline of technical and operational requirements designed to protect cardholder data. Put differently, many consider the PCI DSS as the minimum requirements that a company must meet in order to accept and process credit cards.

The current version of the PCI DSS was published in April of 2016 and represents the sixth incarnation of the standard.

| 240+ | 12 Months |
|---|---|
| Number of security controls required under the current version of the PCI DSS.[191] | The frequency with which large retailers must audit and certify their compliance with the PCI DSS.[192] |

Factors retailers should consider when evaluating your compliance with the 12 requirements of PCI DSS:

1. Are there any deficiencies identified in your organization's latest "Report on Compliance," and are you remediating those issues?

2. Are there any concerns about the scope of your organization's latest "Report on Compliance?"

3. If PCI non-compliance is identified, does this trigger contractual notification or remediation requirements?

4. With new technologies, is your vendor contractually required to meet PCI standards?

5. Do your device vendors and manufacturers meet requirements, such as PIN Transaction Security (PTS) standards?

6. Is your Payment Application PA-DSS validated?

7. Are you using a Point to Point Encryption ("P2PE") Isolution?

8. Does your Point-to-Point Encryption solution meet the PCI P2PE standard?

9. Have the vendors that access, transmit or store you credit or debit card data provided you with appropriate indemnification in the event of a breach caused by the vendor or their equipment?

---

191 Payment Card Industry, Data Security Standard v 3.2, https://www.pcisecuritystandards.org/security_standards/documents.php ("PCI DSS 3.2").

192 *See, e.g.,* American Express Merchant Operating Guide (Oct. 2016).

## T. Selecting a Qualified Security Assessor ("QSA")

Retailers that accept credit cards are typically required by the payment card brands to show that they are in compliance with the Payment Card Industry Data Security Standards or "PCI DSS" at least once a year. How a retailer is permitted to show compliance depends in part on whether the retailer has a history of data security issues (*e.g.,* have they suffered a breach) and the quantity of credit cards that the retailer transacts each year. Typically retailers that have either had a data security breach, or transact large quantities of credit cards, are required to retain a Qualified Security Assessor or "QSA" to conduct an audit and to provide an independent report showing whether the retailer is, or is not, in compliance with the PCI DSS. Retailers that have not experienced a data breach and transact relatively few cards are often permitted to self-certify their compliance with the PCI DSS.

A QSA is a company that has been certified by the PCI Security Standards Council ("PCI SSC") to validate compliance with the PCI DSS. The independence, effectiveness, and consistency of QSAs has recently been called into question. Among other things, the Federal Trade Commission ("FTC") has initiated an investigation of the QSA-industry.[193]

By understanding what the FTC is looking at when evaluating QSAs, retailers can perform their own due diligence to try to avoid allegations by the FTC, or others, that a QSA's examination is insufficient. The FTC's investigation is focused on the following issues that may impact a QSA's judgment in terms of a retailer's PCI DSS compliance:

1. The percentage of the QSA's revenue that comes from providing QSA services.

2. How often the QSA determines that retailers are not in compliance with the PCI DSS.

3. How QSAs bid, negotiate, price, and scope the audits that they perform.

4. The extent to which QSAs rely upon representations made by a retailer's employees.

5. The extent to which QSAs utilize sampling as part of their assessments.

6. The extent to which QSAs are willing to share "draft" reports with retailers that flag areas of non-compliance, but generate final reports that show full compliance if the retailer remediates areas of concern.

7. The extent to which QSAs are willing to issue final reports that show compliance based on assurances that a retailer will remedy a deficiency in the future.

8. The rate at which the retailers that a QSA certifies as compliant experience data breaches.

9. Whether QSAs have policies and procedures to prevent potential conflicts of interest.

[193] Commission Orders to File Special Reports to Collect Information Regarding Data Security Auditors (file No. P155402).

10. How QSAs assess whether the risk of a PCI DSS deficiency has been appropriately mitigated by a "compensating control."

The following provides a snapshot of information when evaluating a QSA:

| | | |
|---|---|---|
| 166<br><br>The number of companies certified as QSAs in the United States.[194] | 9<br><br>The number of QSAs that have been ordered to provide information to the FTC concerning their methods for conducting assessments.[195] | 3<br><br>The number of QSAs that have been implicated in public lawsuits following data security breaches.[196] |

## U. Negotiating Payment Processing Agreements

Credit cards are the primary form of payment received by most retailers. In order to process a credit card a retailer must enter into an agreement with a bank and a payment processor. Payment processing agreements often have significant impacts on a retailer's financial liability in the event of a data breach. In many cases, the contractual liabilities that flow from a payment processing agreement surpass all other financial liabilities that arise from a data breach including the cost to investigate an incident, defend litigation, and defend a regulatory investigation.

| | | |
|---|---|---|
| 244<br><br>The number of companies that offer payment processing services for in-store (point of sale) transactions in the United States.[197] | $67 million<br><br>The amount of Target's contractual liabilities to its payment processor in connection with just one of the four major payment brands.[198] | 25,000<br><br>The word count of a typical payment processing agreement. |

The following checklist describes common data security related provisions to look for within most payment processing agreements:

1. Incorporation of Payment Brand Rules. Most payment processing agreements incorporate by reference the rules, regulations, and guidelines of the payment brands (*e.g.,* American Express, Discovery, MasterCard, and/or Visa). When negotiating a payment processing agreement it is important to determine whether

194 PCI SSC website https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors (last viewed March 9, 2016).

195 FTC to Study Credit Card Industry Data Security Auditing, Commission Issues Orders to Nine Companies that Conduct Payment Card Industry Screening (Mar. 7, 2016) *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing.

196 QSAs responsible for certifications in the CardSystems, Target, and Heartland breaches appear to have been involved in the resulting litigation as possible defendants.

197 Visa, Global Registry of Service Providers, http:www.visa.com/splisting/searchGrsp.do (search conducted of "payment processing POS / Card present" and "United States" region of operation). Search was last conducted November 11, 2016.

198 Robin Sidel, Target to Settle Claims Over Data Breach: Retailer to pay Visa issuers up to $67 million, Wall Street Journal, (August 18, 2015), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013.

the obligation to abide by the payment brand rules is unilateral (*i.e.,* is imposed only upon the merchant) or reciprocal (*i.e.*, is imposed upon the merchant, the acquiring bank, and the payment processor).

2. Incorporation of the Payment Card Industry Data Security Standard. Many payment processing agreements reference the PCI DSS and require that a merchant be, and remain, in full compliance with the requirements of the PCI DSS. When negotiating a payment processing agreement it is important to determine whether you are, or are not, currently in compliance with the PCI DSS, and whether the obligation to comply with the PCI DSS is unilateral or reciprocal. Put differently, does the agreement require just the merchant to comply with the PCI DSS or does it require all parties to comply with applicable portions of the standard? Note that even if a payment processing agreement does not expressly incorporate the PCI DSS, if the payment processing agreement incorporates the Payment Brand Rules, the Payment Brand Rules may themselves incorporate the PCI DSS by reference.

3. Incorporation of Other Rules, Guidelines, or Procedures. Some merchant banks and payment processors maintain their own procedures, protocols, or "operating guidelines," and attempt to incorporate those documents by reference into a payment processing agreement. If you are negotiating an agreement that incorporates bank or processor specific rules, be sure to ask for a copy of those documents. Note that many banks do not make such documents public (*e.g.,* they are not available online); a contracting party must specifically ask for a copy or request access to a password restricted repository.

4. Indemnification. Most merchant banks and payment processors attempt to require that a merchant indemnify them for any fine, penalty, assessment, or other contractual liability, imposed by the payment brands upon the merchant bank or the payment processor as a result of a data security incident that occurs at the merchant. In many situations these "assessments" form the greatest financial liability imposed upon the merchant after a data breach.

5. Assignment of Rights. If a merchant is required to indemnify a merchant bank and/or payment processor for fines, penalties, assessments, or other contractual liabilities imposed by the payment brands, the merchant has a strong interest in being able to appeal, or contest, those liabilities before they are incurred. Some merchant banks and payment processors have assigned, or subrogated, their rights vis-à-vis the payment brands to the merchants. Doing so ensures that the merchant is able to "stand in the shoes" of the bank and the payment processor to ensure that the assessments that are issued (and which the merchant must pay under an indemnification obligations) are reasonable and appropriate.

6. EMV Compliance. In October of 2015, the payment brands instituted new rules intended on encouraging merchants, banks, and payment processors to adopt the EMV standard (*e.g.,* chip and pin). When negotiating a payment processing contract it is important to understand what, if any, requirements are imposed upon the parties to be compliant with the EMV standard.

7. Applicable Law: Payment processing agreements typically contain a broad mandate that the merchant comply with applicable laws and regulations. Often

such agreements will specifically reference data privacy and security laws. As with other sections in the agreement, it is important to note whether obligations to comply with privacy and security laws are unilateral or reciprocal.

8. Subcontractors: Does the payment processing agreement attempt to hold the merchant responsible for the acts and omissions of its third party service providers? Some payment processing agreements also require that a merchant disclose its use of third party subcontractors that accesses/stores/transmits PCI data to its bank and/or payment processor.

9. Exclusivity: Does the payment processing agreement impose any restrictions on a merchant's ability to hire third parties? Does it impose any restrictions on a merchant's ability to use other payment processors or merchant banks?

10. Confidentiality / Data Security: Consider whether the payment processing agreement contains the following specific confidentiality and data security terms:

    a. Is the merchant bank or payment processor subject to confidentiality obligations at least as protective as those to which the merchant is subject?

    b. Is the bank or payment processor permitted to store / transfer payment card information outside the United States?

11. Data Security Incidents: Payment processing agreements typically require that a merchant notify a bank or a payment processor of a data breach. Consider whether the agreement contains a time period that may be difficult to comply with (*e.g.,* immediate notification) or one that may be commercially practical *(e.g.,* notification within 72 hours of discovery of an incident)? As with other provisions in the payment processing agreement, is the breach notification obligation unilateral or reciprocal?

12. Reserve: Many payment processing agreements permit a merchant bank or payment processor to establish a reserve in the event of a data security incident. Often a bank or a payment processor will attempt to negotiate a provision which permits them to fund the reserve using the proceeds from any credit card transaction. If a reserve provision is proposed consider whether there are sufficient terms to protect the merchant such as:

    - A cap on the total reserve amount.
    - A daily cap on the percentage of sales Vendor may withhold when establishing a reserve.
    - Is the reserve amount tied to a calculation based on objective risk criteria.
    - Is there a termination of the reserve and payment of funds.
    - Is the reserve comingled with other merchant's funds.

13. Vendor Liability: As discussed above, "reciprocity" is a constant theme when evaluating a payment processing agreement. In the context of liability, consider whether your payment processing agreement holds your bank and payment processor liable for breaches that occur within their systems, whether they are required to indemnify you for damages that would relate to such a breach, and

whether any cap that applies to their damages is similar to any cap that applies to the merchant's damages.

## V. Credit Card Breaches

For most retailers credit cards are the primary form of the payments that they receive. Accepting credit cards, however, carries significant data security risks and potential legal liability. In addition to the normal repercussions of a data security breach – *e.g.*, reputation damage, the risk of class action litigation, and the risk of a regulatory investigation – if a retailer's credit card system is compromised the retailer may be contractually liable to its payment processor, its merchant bank, and ultimately the payment card brands (*e.g.*, VISA, MasterCard, Discover, and American Express). In many cases that contractual liability surpasses any other financial obligation that arises from the breach.

| 26 | 130 million | 23% |
|---|---|---|
| The number of separate contractual penalties, fines, adjustments, fees and charges that the credit card brands may assess upon a retailer.[199] | Largest number of credit card numbers impacted by a breach.[200] | Percentage of data breach class actions that involved credit card data.[201] |

Factors retailers should consider when preparing to respond to a credit card data breach:

1. Does your payment processing agreement cap or limit your contractual liability in the event of a data breach?

2. Does your payment processing agreement cap or limit your processor's liability in the event that they suffer a data breach?

3. Do you have a contractual obligation to notify your payment processor or merchant bank in the event of a possible security breach?

4. Have the vendors of your point of sale equipment provided you with indemnification in the event of a breach caused by their equipment?

5. Is a reporting structure, and contact information, included in your incident response plan?

6. Are there any deficiencies identified in your organization's latest "Report on Compliance."

---

199 American Express Merchant Regulations (April 2014); Discover Merchant Operating Regulations (April 2014); MasterCard Security Rules and Procedures (Feb. 2015); Visa Service Rules (April 2015).

200 Privacy Rights Clearinghouse, http://www.privacyrights.org/ (last searched Nov. 11, 2016).

201 Bryan Cave LLP, Bryan Cave 2016 Data Breach Litigation Report, https://d11m3yrngt251b.cloudfront.net/images/content/8/2/v2/82494/DataBreachLitigationReport.pdf (last viewed Nov. 11, 2016).

7. If you have cyber-insurance are there any exclusions that would impact its coverage for credit card related breach costs?

8. If you have cyber-insurance is there a sub-limit for Payment Card Industry ("PCI") related liabilities?

9. Do you have a contractual relationship in place with a forensic investigator that is certified by the Payment Card Industry (a "PFI")?

10. Do you have a contractual relationship in place with a forensic investigator that is independent of the Payment Card Industry?

## W. Causes of Healthcare Data Breaches

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), covered entities (e.g. healthcare providers and health plans) must notify the Department of Health and Human Services ("HHS") of breaches of unsecured protected health information ("PHI").[202] The information provided to HHS provides companies with a high level of insight concerning the types of breaches that occur in the health care industry.

The data collected by HHS concerning breaches affecting 500 or more individuals in as of November 11, 2016 shows, for a second year in a row, unauthorized access or disclosure, such as misdirected mailings, break-ins of physical premises, and employees accessing PHI that is not necessary for their duties, are the most common forms of data breach in the health sector.

| | |
|---|---|
| 41%<br>The percentage of reported breaches caused by unauthorized access or disclosure.[203] | 36%<br>The percentage of unauthorized access or disclosure caused by paper records.[204] |
| 18%<br>The percentage of reported breaches caused by theft of hardware of all types.[205] | 31%<br>The percentage of reported breaches caused by hacking/IT incidents.[206] |

Things to consider when reviewing your information security program in light of HHS data:

1. Implement different access levels for employees' access to PHI based on their job duties;

2. Immediately stop access to PHI by terminated employees and escort them if necessary;

---

202 45 C.F.R. §164.408(a)-(b).

203 U.S. Dep't of Health and Human Servs. Office for Civ. Rights, Breaches Affecting 500 or More Individuals, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (November 11, 2016).

204 *Id.*

205 *Id.*

206 *Id.*

3. Require a two-step verification process to ensure that mail and email recipients' information is correct before sending invoices or appointment reminders;

4. Transition from paper records to secure, encrypted computer databases;

5. Shred paper records when no longer needed;

6. Prevent break-ins by implementing physical safeguards such as security alarms, security guards, and locks on windows and doors.

## X. Healthcare Data Breach Litigation Trends

Companies that have a breach involving PHI worry not only about fines and penalties imposed by HHS, but about class action lawsuits. The risk that a class action lawsuit will lead to financial liability, however, is often misunderstood.

In many, if not most, class action lawsuits that involve the loss of PHI, plaintiffs have been unable to prove that they have standing to seek recovery. Specifically, unless a plaintiff has been the victim of identity theft or has suffered some other type of concrete injury, most courts have refused to let them proceed based solely on the allegation that they are subject to a theoretical increased risk of harm as a result of the breach. The following summarizes the types of allegations where courts have, and have not, found standing.

| Allegations Found To Be Insufficient | Allegations Found By Some Courts To Be Sufficient |
|---|---|
| • Alleged violation of HIPAA<br>• Data loss, but no evidence of access or misuse<br>• Data loss, but no evidence of identity theft<br>• Loss of value of PHI because the PHI can be sold on the cyber black market<br>• Patients' right to truthful information about the security of their PHI after the breach<br>• Plaintiffs' receipt of unsolicited phone calls from telemarketers and scam artists, without evidence that such calls resulted from the breach<br>• Costs incurred to travel to a different hospital with allegedly better security | • Plaintiffs lost data has been actually accessed or misused<br>• Plaintiffs with no prior history of identity theft became identity theft victims shortly after breach<br>• Plaintiffs' personal information had not previously been the subject of another unrelated breach<br>• Plaintiffs receive unsolicited phone calls marketing products related to information that has been breached (*e.g.* the products are for a specific medical condition listed in the breached PHI), but have never received such phone calls in the past |

What factors should you look at when considering the risk that litigation poses following a breach:

1. Was the quantity of records lost lower, or greater, than the average number of records involved in recent class action lawsuits?

2. Were the records lost encrypted, obscured, or de-identified?

3. Could the type of information lost be used to commit identity theft?

4. Did patients suffer any direct monetary harm?

5. Has there been any evidence of actual identity theft?

6. Could the data loss hurt the reputation of a patient or cause emotional distress?

7. Did you offer credit monitoring, identity theft insurance, and/or credit repair services?

8. If so, what percentage of impacted consumers availed themselves of your offer?

9. If filed as a class action, is the class representative's claim of identity theft premised on unique facts?

## Y. Healthcare Data Breach Enforcements and Fines

The Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Enforcement of the Privacy Rule began on April 14, 2003, while enforcement of the Security Rule began on April 20, 2005. Furthermore, covered entities and business associates were required to comply with the HIPAA Breach Notification Rule beginning on September 23, 2009.[207]

The OCR relies on complaints filed by third parties, self-reports of data breaches, and media reports to identify targets for compliance reviews. If a covered entity or business associate is found to have committed serious violations during a compliance review, HHS may require the entity to enter into a "Resolution Agreement" ("RA") that may include a fine and a corrective action plan.

| | |
|---|---|
| 141,754<br><br>Number of HIPAA complaints received by OCR since 2003.[208] | 1,105<br><br>Number of compliance reviews initiated by OCR since 2003.[209] |
| 33<br><br>Number of RAs since 2008.[210] | $41 million<br><br>Total fines collected for HIPAA violations.[211] |
| $5.55 million<br><br>Largest fine assessed by OCR to date.[212] | |

[207] The HIPAA Breach Notification Rule requires covered entities and their business associates to notify the HHS Secretary, individuals, and in some cases, provide notice in media, regarding breaches of unsecured protected health information.

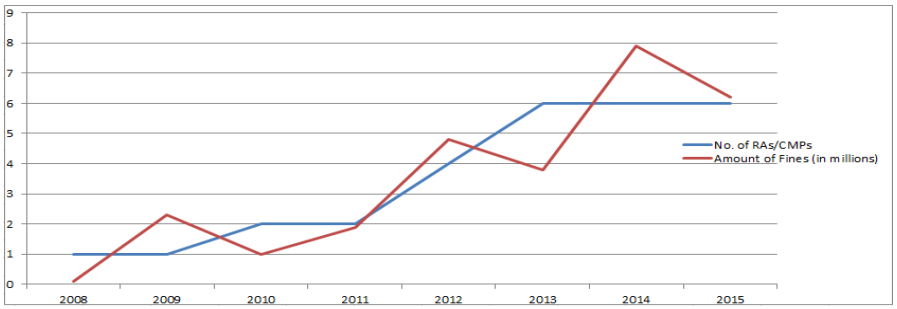
[208] U.S. Dep't of Health and Human Servs., Enforcement Highlights, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (November 11, 2016).

[209] *Id.*

[210] U.S. Dep't of Health and Human Servs., Resolution Agreements, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (November 11, 2016).

[211] *Id.*

Trends in Enforcement Activities and Fines[207]




What to consider when assessing the impact of an OCR investigation:

1. While enforcement activities and fines are projecting upward, they appear stable between 2014-2015.

2. Only a minority of investigations lead to fines and penalties.

3. Cooperation in government-initiated compliance reviews is key to reducing the risk of a penalty.

4. Having multiple incidents, even if minor on their own, tends to trigger an investigation and lead to fines and RAs.

## Z. Healthcare Business Associates

The Health Information Technology for Economic and Clinical Health ("HITECH") Act modified the Health Insurance Portability and Accountability Act ("HIPAA") by expanding the definition of Business Associates ("BA") and their responsibilities and liabilities. A BA includes:

1. Health Information Organizations

2. E-Prescribing Gateways

3. Persons/entities that for, or on behalf of, a Covered Entity:

- Create or received PHI
- Maintain or store PHI even if they do not or can not access the PHI
- Offer personal health records
- Provide data transmission services if they routinely access the PHI

The Federal Office for Civil Rights ("OCR"), which enforces HIPAA and HITECH, has identified BAs as one of its top enforcement priorities. Under HIPAA and HITECH, BAs are directly liable for compliance and subject to the following monetary penalties:

---

212 Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html (November 11, 2016).

| Violation Category | Each Violation | Maximum Penalty per Identical Provision Violated in Calendar Year |
|---|---|---|
| Did Not Know | $100 - $50,000 | $1,500,000 |
| Reasonable Cause | $1000 - $50,000 | $1,500,000 |
| Willful Neglect – Corrected | $10,000 - $50,000 | $1,500,000 |
| Willful Neglect – Not Corrected | $50,000 | $1,500,000 |

Companies that are considered BAs, or companies that are contracting with a BA, should consider the following checklist when evaluating their compliance with HIPAA and HITECH:

1. Designate a security officer.
2. Perform a Security Risk Assessment.
3. Implement administrative, physical, and technical safeguards to protect PHI.
4. Identify and report breaches of security.
5. Develop policies for HIPAA / HITECH compliance.
6. Impose disciplinary actions where employees or vendors violate HIPAA / HITECH obligations.
7. Verify that a Business Associate Agreement is in-place with all service providers that handle PHI.
8. Maintain HIPAA and HITECH relevant documentation for such periods as required by law.

## AA. Ransomware May Be a Reportable HIPAA Breach

In 2016, more than 4,000 ransomware or other malware attacks occurred daily, a 300% increase since 2015. There have been reports of six hospitals that have been victims of ransomware in 2016. Ransomware is a type of malicious software used by cyber actors to deny access to an entity's systems and/or data. Ransomware may spread to shared storage drives and other systems. The systems and data are held hostage until a ransom is paid.

Ransomware is more disruptive and debilitating than other criminal cyber threats because it can:

- Disrupt the ability to provide health services and daily operations
- Inflict significant financial losses
- Damage electronic protected health information (EPHI) and other sensitive data beyond recovery

- Expose EPHI to a breach
- Harm the reputation of the company

Cyber attackers enter the organization's system by tricking a user to disclose a password or to click on a virus-laden email attachment. They also are seeding legitimate websites with malicious codes, taking advantage of unpatched software on an organization's computers.

The presence of ransomware on a computer of a covered entity or business associate is a security incident under the HIPAA Security Rule, and appropriate measures must be taken to respond. A risk assessment must be performed to determine whether there was a reportable breach of EPHI as a result of the ransomware attack. If EPHI is encrypted as a result of the ransomware attack, the Office for Civil Rights (OCR) considers this to be a breach because the attackers have taken control of the EPHI. If the EPHI was encrypted by the covered entity/business associate in a manner consistent with the *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*[213], then most likely a breach did not occur unless there was a failure of the encryption solution based on a factual analysis of the event.

A new fact sheet, "Ransomware and HIPAA[214]" released by the OCR emphasizes that covered entities/business associates are required to implement appropriate security measures to reduce the risks to EPHI by the introduction of malware, including ransomware. As part of the required HIPAA Security Rule Risk Assessment, covered entities/business associates must identify the potential risks to their EPHI and what measures will be implemented to address the vulnerabilities. As an example, although there is not a HIPAA regulation that specifically requires covered entities/business associates to update the firmware of network devices, entities should identify and address the risks to EPHI of using network devices running on obsolete firmware, especially when firmware updates are available to remediate known security vulnerabilities.

Because prevention and early detection are the best defenses against ransomware, as part of the required security awareness training, include information specifically focused on ransomware such as:

- Never click unsolicited links or open unsolicited attachments
- Indicators of ransomware:
  - link clicked on/attachment opened that appears malicious
  - increased activity in computer central processing unit
  - inability to access files
  - Require immediate reporting of suspicion 24/7 to designated person

## BB. How to Develop a HIPAA Incident Response Team

Covered entities and business associates are required to identify and report breaches of unsecured protected health information ("PHI") and security incidents. "Breach" is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Laws which compromises the security or privacy of the PHI, and is not one of the breach

[213] Available at http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

[214] Available at www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

exclusions.[215] Breach applies to both paper and electronic PHI. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of electronic PHI ("EPHI") or interference with the entity's system operations in its information system.[216] The Federal Office for Civil Rights ("OCR") has recommended that covered entities and business associates have incident response teams capable of identifying and handling breaches and security incidents.[217] Incident response plans and policies should be developed, reviewed annually, and approved by management.

Being capable of responding quickly and appropriately to breaches and security incidents must be a high priority for covered entities and business associates. The potential effects of these events can be devastating, both financially and legally, as well as create significant consequences from a public relations perspective.

| | |
|---|---|
| Average total cost of security incident in 2016 is $4 million, or $355 per record for healthcare entities.[218] | Fines imposed by the OCR for breaches and security incidents in the past 12 months total $23,194,000. |

Having an incident response team can decrease the cost of a security incident by $16 per record.[219] In 2015, hacking was the leading cause for the largest security incidents.

An incident response team ("IRT") must be specific to the covered entity/business associate and should be structured based on the mission, size, structure, and function of the entity. The purposes of the IRT should include both proactive and reactive functions: incident preparation and prevention; incident reporting; analysis of incidents; responding to incidents; and post-incident activities.

In developing the incident response plan, policy, and procedures, the following are some of the considerations:

1. Who should be on the IRT?
2. Who should lead the IRT?
3. Why is an IRT needed?
4. Define the goals and functions of the IRT.
5. Should the IRT be ad hoc or a major job function?
6. Should any responsibilities be outsourced?

---

215 45 CFR §164.402.

216 45 CFR §164.304.

217 "Is Your Covered Entity or Business Associate Capable of Responding to a Cyber Security Incident?" OCR, July 2016 (available at www.hhs.gov/sites/default/files/HIPAA-cyber-awareness-monthly-issue-6.pdf).

218 "2016 Cost of Data Breach Study: Global Analysis," Ponemon Institute LLC, June 2016 (available at www-03.ibm.com/security/data-breach/).

219 *Id*, at p. 14.

7. How will the IRT be implemented?

## CC. Third Party Vendor Management Programs

Third-party service providers present difficult and unique privacy and cybersecurity challenges. Vendor management is important throughout the life of a relationship with your service provider. Vendor diligence starts during the vendor selection process, continues through contract negotiation, and ends when the parties terminate their relationship. The goal is to effectively improve the service your vendors provide and mitigate the risk inherent in the vendor relationship.

| | | | |
|---|---|---|---|
| $78 billion => $235 billion<br><br>The amount companies spent on cloud services in 2011, compared to the projected amount that companies are estimated to spend by 2017.[220] | 62%<br><br>The percentage of companies that evaluate the security risks of their third-party vendors.[221] | 32%<br><br>The percentage of companies that require their partners and vendors to comply with their security practices.[222] | 28%<br><br>The percentage of breaches attributable to a partner or vendor.[223] |

What to consider when evaluating a vendor agreement:

1. What data and information will you be sharing with your vendor?

2. Does your vendor agreement require that the vendor use your data only to provide services to your company?

3. Under what terms is your vendor required to keep your data confidential?

4. Is your vendor required to comply with government requests to produce your data?

5. Is your vendor required to keep your data in a logically distinct manner?

6. What are the laws and industry regulations that apply to your company with which your vendor will be required to comply?

7. Under what terms is your vendor required to notify you if your vendor is breached?

---

220 IHS Markit, The Cloud: Redefining the Information, Communication and Technology Industry, (February 2014), http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017.

221 PricewaterhouseCoopers, US cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey, (July 2015), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

222 PricewaterhouseCoopers, PwC Viewpoint on Third Party Risk Management, (November 2013), https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-viewpoint-vendor-risk-management.pdf.

223 *Id*.

8. Is your vendor subject to your privacy, cybersecurity, and data retention policies?

9. Does your privacy policy allow your company to share your data with a vendor?

10. After the termination or expiration of the vendor agreement, under what terms is your vendor required to return your data?

11. What right does your vendor have to withhold access to your data or terminate your service?

12. What rights do you have to audit your vendor's operational practices?

13. Is your vendor required to self-audit?

14. Have your vendor's past audits exposed any vulnerabilities, or has your vendor been breached in the past?

15. Will your vendor be required to maintain certain levels of insurance during the term of the vendor agreement?

## DD. Cloud Computing

Most companies today use some form of cloud computing whether through software-as-a-service, platform-as-a-service, or infrastructure-as-a-service. Cloud computing's cost-effective scalability can offer significant advantages to an organization, but it can also raise significant security concerns. Although many cloud providers offer assurances that their systems are secure, many are also unwilling to contractually guarantee the security of data placed in the cloud and are unwilling to fully indemnify a company in the event that the cloud provider's system is breached.[224]

| 95% | 64% | 71% |
|---|---|---|
| Percentage of those enterprises that used a cloud service in 2016.[225] | Percentage of eCommerce sites that relied on cloud computing in 2014.[226] | Percentage of companies that view data security as a concern in moving services to the cloud.[227] |

To minimize data security risks companies should evaluate the following as they consider cloud service providers:

[224] *See*, Steve Norton, Dropbox Confronts Cloud Security Skeptics, Wall Street Journal Online, (May 1, 2015), http://blogs.wsj.com/cio/2015/05/01/dropbox-is-not-part-of-security-problem-says-new-security-chief/?KEYWORDS=cloud+computing.

[225] RightScale, RightScale 2016 State of the Cloud Report, http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf.

[226] Claranet, Claranet Research Report: Adoption Trends in Cloud Computing 2011-2014, http://cloudindustryforum.org/images/PDF/CL0072-Claranet-Research-Report-Adoption-Trends-in-Cloud-Computing-2011-2014.pdf.

[227] *Id.*

1. Does data need to be stored in a specific jurisdiction? Some jurisdictions require that data remain within their borders and by utilizing an open cloud environment, where data is transferred freely across borders, a company could inadvertently violate prohibitions concerning the cross-border transfer of data.

2. Does the cloud service provider agreement set forth whether the vendor is dedicating hardware to the customer? Absent express language, the vendor is likely providing shared hardware to the customer.

3. Does the agreement clearly explain who has rights to the data stored using the cloud service? Depending on the underlying service, some agreements grant the vendor limited rights.

4. To what extent is cryptography used? Is each separate record in the cloud encrypted, or does all data use the same encryption key? The value of these approaches vary based on the sensitivity of the data and the processing costs.

5. Who is responsible for backing up data and at what frequency?

6. Does the agreement set forth standards for how the customer can export its data from the vendor? A customer may want to switch from one cloud vendor to another or may simply want to proceed in a different technological direction.

7. Are the appropriate licenses in place to execute software in a cloud computing environment? For example, some software is priced based on the type of server on which it will be run. Meanwhile, the execution of the software in a cloud (or networked) environment may trigger additional considerations.

8. Does the agreement give the customer sufficient flexibility to expand or contract the extent to which it uses the cloud services? One of the advantages of cloud computing is the idea that use can be scaled to match a customer's needs.

9. Are the agreement's terms sufficiently defined to avoid ambiguities over what the vendor has contracted to provide the customer? Trending technology terms often must be defined to ensure all parties perceive them the same way.

10. Does the agreement guarantee to maintain any current APIs or features, or does it promise to evolve to provide future functionality? Depending on the circumstances, schedules can be a useful way to ensure certain necessary functionality remains in the service or developed in the future (i.e., provision of advanced AI functionality).

11. Will the network connections between the vendor and the customer provide sufficient resources, and if not, what contractual recourse does the customer have? Although cloud computing is seen as ubiquitous, engineering realities may curb its availability. Customers should consider that risk when contracting and request adequate service level compensation.

12. Does the agreement require that the vendor maintain any customer industry-specific needs or regulations? Depending on the sensitivity of the data, the

customer may be required to certify that the cloud vendor adheres to certain data security standards.

13. Does the agreement give the customer the ability to delete data stored by the vendor and confidence that such deletion can be achieved? For some categories of data, customers must ensure that data is completely removed from the servers.

14. Does the agreement clearly set forth how the parties should communicate in the event of a data breach or service outage? Similarly, does the agreement contain adequate representations about the vendor's steps to prevent either event and whether the vendor will indemnify the customer against any damages should either event occur?

15. Does the cloud vendor have adequate liability coverage? Does the agreement contain carve outs to the limitation of liability for a breach of the data security obligations? Although no one wants the agreement to reach that point, it is important to understand the extent to which the cloud provider is willing to absorb a loss that might impact many (or all) of its customers simultaneously.

## EE. Sharing Threat Indicators With The Government

After a security incident is identified organizations often consider whether to share information concerning the incident with government agencies. If the incident involved criminal conduct, federal law enforcement agencies – such as the Federal Bureau of Investigation or the United States Secret Service – may be interested in investigating and attempting to prosecute those responsible. It's also possible that law enforcement already may be investigating similar incidents and can share information that may help in your investigation. For example, they may be able to identify IP addresses associated with bad actors, security vulnerabilities that are being exploited within other organizations, or evidence that might suggest that criminals successfully obtained information from your organization.

The "Cybersecurity Act of 2015" is designed to promote the ability of organizations to identify data security incidents, and to share that information with law enforcement. The Cybersecurity Act has three main provisions. First, it provides a safe harbor from liability for organizations that monitor information systems for cyber threats. Under the safe harbor an organization cannot be sued for engaging in monitoring that complies with the Act. Second, if a threat is identified it provides a safe harbor for the organization to share that information with federal agencies. Third, if an organization chooses to share a cyber threat indicator or a defensive measure with the Federal government, any privilege that might have attached to the information shared (*e.g.,* attorney client privilege) is not waived.

What to consider when deciding whether to share information with the government:

1. Most organizations are <u>not</u> required to share information with the federal government concerning cyber threats or data security incidents. The Cybersecurity Act of 2015 does not compel sharing, it is designed to protect organizations that voluntarily choose to share information.

2. The Cybersecurity Act of 2015 only protects information shared with the *federal* government. If you are considering sharing information with state or local

government agencies you should consider whether doing so may result in liability or privilege waiver.

3. The safe harbors in the Cybersecurity Act of 2015 require that a company follow guidelines for what information can be shared, and how that information must be shared. You should carefully review the requirements before disclosing information to the government to make sure that you can utilize the protections under the Act.

4. To the extent that you have contractual or other statutory obligations not to share information with the government, it is uncertain whether courts will interpret the Cybersecurity Act of 2015 as immunizing your organization from liability if you choose to voluntarily share information.

The following provides a snapshot of information regarding threat monitoring and information sharing with the government:

| 43,000 | 70% |
|---|---|
| Number of members in Infragard – a forum created by the FBI for the private and public sector to share threat indicators.[228] | Percentage of Fortune 500 companies that participate in Infragard – an organization created by the FBI to facilitate the sharing of cyber threat information.[229] |

## FF. Security Due Diligence In A Merger Or Acquisition

The FTC can hold an acquirer responsible for the bad data security practices of a company that it acquires. Evaluating a potential target's data security practices, however, can be daunting and complicated by the fact that many "data" issues arise months, or years, after a transaction has closed. For example, the FTC has investigated data security breaches and unlawful data collection practices that occurred years *before* the company was acquired, but were discovered months *after* a transaction closed.

| 21 months | 9 months |
|---|---|
| Number of months hackers penetrated a target's systems *before* the target was acquired and investigated by the FTC.[230] | Number of months hackers continued to penetrate a target's systems *after* the target was acquired and investigated by the FTC.[231] |

Due diligence questions relating to data security to consider in a M&A transaction:

1. Is the target subject to a sector specific data security law?

---

228 http://www.infragardmembers.org/ (last viewed Nov. 2016).

229 According to InfraGard website 350 out of 500 companies on the Fortune 500 have a representative in InfraGard. http://www.infragard.org (last viewed Nov. 2016).

230 *See*, In the Matter of Reed Elsevier and Seisint, FTC Docket No. C-4226 (July 29, 2008), https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter.

231 *Id.*

2. Has the target received a regulatory inquiry concerning its data security practices in the past two years?

3. Has the target received litigation claims concerning its data security practices?

4. How many data security incidents has the target experienced? Is the quantity reported commensurate with what would be expected given the industry, type of data held by the target, and quantity of data held by the target?

5. What data breaches has the target experienced? Is the quantity reported commensurate with what would be expected given the industry, type of data held by the target, and quantity of data held by the target?

6. Does the target have a Written Information Security Program ("WISP")? If so, is it appropriate given the type and quantity of data held by the target?

7. Does the target have an Incident Response Plan ("IRP"). If so, is the IRP appropriate and effective?

8. How has the target dealt with prior security incidents and security breaches?

9. Has the target conducted and documented internal security assessments?

10. Has the target conducted and documented external security assessments (e.g., penetration tests, vulnerability scans, data security audits)?

11. If the target accepts payment cards, are any areas of non-compliance with the Payment Card Industry Data Security Standard ("PCI DSS") identified in their most recent Report on Compliance ("ROC")? Does the ROC appear to accurately describe the target's network and payment card infrastructure?

12. Has the target conducted a data map or a data inventory?

13. What are the target's data retention policies?

14. Does the target have a vendor management program in place? If so, how has the target evaluated the security practices of its vendors and subcontractors?

15. Did the target have dedicated employees focused on data security issues (*e.g.,* a Chief Information Security Officer)?

# III. DATA TRANSFERS FROM OTHER COUNTRIES

## A. EU-US Data Transfers

The EU Data Protection Directive 95/46/EC (the "Directive") creates the legal framework that underpins the national data protection laws in each of the EU member states. The Directive provides that personal data may only be transferred to countries outside the EU when an adequate level of protection is guaranteed by the party that desires to make the transfer. Few exemptions apply, and the laws of the United States are not considered by the European Union as providing, all other things being equal, an adequate level of data protection. As a result,

when most companies transferred personal information from the EU into the United States they needed to take one of the following steps to achieve the "adequacy" status required by the Directive:

- Safe Harbor Certification
- EU Model Contracts for Data Transfer
- Binding Corporate Rules

The EU-US Safe Harbor Framework (the "Safe Harbor") was developed by the United States Department of Commerce and operated by participating companies pledging to adhere to seven privacy principles and agreeing that the FTC could investigate and enforce that adherence. In 2000 the EU Commission reviewed the seven principles, and the FTC enforcement mechanism, and determined that companies which certified their adherence to the framework met the Directive's adequacy requirement. In October of 2015, however, the European Court of Justice held that the Safe Harbor was invalid as it failed to offer sufficient levels of data protection. Following that decision companies that were on the Safe Harbor could no longer rely upon it as a basis of adequacy.

In 2016, the United States and the European Union finalized a new framework called Privacy Shield. Privacy Shield was intended to replace the now-defunct Safe Harbor.

## B. Privacy Shield

In February of 2016, the European Commission ("EU Commission") released the draft text of the EU-U.S. Privacy Shield Framework ("Privacy Shield"). Privacy Shield was designed to replace the invalidated Safe Harbor as a new adequacy measure to govern the transfer of personal data between the EU and U.S. On June 29, the EU Commission sent an updated text version of the Privacy Shield to the Article 31 Committee — which includes representatives of the 28 Member States and the EU Commission — based on changes recommended by the Article 29 Working Party – an advisory body on data protection and privacy. The EU Commission announced on July 8, 2016, that the Article 31 Committee approved the final version of the Privacy Shield, and the Privacy Shield was formally approved by the EU Commission on Tuesday, July 12, 2016. The U.S. Department of Commerce began accepting certifications from companies that sought to enter the protections of the framework on August 1, 2016.

| 1,506 | 9 |
|---|---|
| Number of companies that have joined Privacy Shield.[232] | Number of options that companies have among private independent dispute resolution organizations to satisfy Privacy Shield's requirement that companies offer ADR.[233] |

[232] https://www.privacyshield.gov/list (last viewed Jan. 23, 2017).

[233] *Id.*

To join Privacy Shield, companies must annually self-certify to the U.S. Department of Commerce that they comply with the following Privacy Shield principles ("Privacy Shield Principles"):

1. Notice – Inform individuals as to the company's adherence to the Privacy Shield Principles.

2. Choice – Provide individuals with the right to opt out of the disclosure of their personal data to third parties, or, in the case of sensitive data to opt in.

3. Accountability for Onward Transfer – Assume responsibility for disclosures of personal information to third parties, contractually require such third party's compliance with the Privacy Shield Principles, and require the third party to notify the company if such third party determines it will be unable to comply.

4. Security – Implement reasonable and appropriate data security measures.

5. Data Integrity and Purpose Limitation – Limit the collection and retention of personal data to the disclosed purpose for collection and use of such personal data, and limit the length of time such data may be retained.

6. Access – Provide individuals with the right to access, correct, or delete their personal data.

7. Recourse, Enforcement, and Liability – Provide enforcement and recourse mechanisms for individuals affected by non-compliance with the Privacy Shield Principles.

Once a self-certification is complete, a company is placed on the U.S. Department of Commerce's publicly available list of Privacy Shield participants ("Privacy Shield List"). Unlike companies using the Privacy Shield to transfer other types of data (*e.g.,* consumer data), companies that seek to transfer employee data must also indicate their willingness to cooperate with the relevant EU data protection authorities and to provide the U.S. Department of Commerce with a copy of their human resources privacy policy.

## C. EU Model Clauses

The EU Commission has held that companies can provide sufficient protection for personal data transferred outside of the EU by requiring the data recipient to sign a contract which incorporates many of the protections that are enshrined in the EU Directive. In order to facilitate transfers that rely upon contractual guarantees, the EU Commission approved three forms of template agreements, or "model contracts," that can be used by companies.

Two of the template agreements can be used only for the transfer of information from a data controller within the EU to another data controller that is located outside the EU. The remaining template agreement is designed to be used for a transfer from a data controller that is located within the EU to a data processor that is located outside the EU. If a company decides to use the model clauses in order to achieve a level of protection considered adequate under the Directive functionally three steps must be followed. The following provides a high level overview of how to implement the model contracts:

Step 1 – National law compliance.

A model contract can help a company in the EU that intends on sending data to a company outside of the EU (e.g., one located in the United States) satisfy itself that the data, once received, will be safeguarded appropriately. The model contract does not, however, ensure that the company which intends to send the data has a right to collect data in the first place, to process it, or to send it to a third party (regardless of the third party's location). As a result, before implementing a model contract a company that intends to transmit data should examine the national laws in the country in which it sits to determine whether it has appropriately collected personal information and whether its intended processing of that information is legally permitted.

Step 2 – Implementation of applicable Model Contract.

The first step when implementing a model contract is to determine which of the three templates should be used. That determination largely depends upon whether the company receiving the data will be a "data controller" or a "data processor" under EU law. A "data controller" is defined within the EU Directive as a company that "determines the purposes and means of the processing of personal data." Whether an organization is, or is not, a data controller is not controlled by contract, data ownership, or data license – it is based upon whether, in fact, an entity determines how data is processed. Specifically, the term has been interpreted as applying to any entity that determines "how long data shall be stored," or "who shall have access to the data." If some, or all, of these decisions are made jointly with other organizations both organizations are considered data controllers. A "data processor" is defined within the EU Directive as a company that acts only on "behalf of the controller" and does not, by itself, have a right to determine the means or purpose of processing. As a result, a company that is able to determine how long data is stored, when data is destroyed, and/or to whom data is given does not qualify as a "data processor" under the Directive. If the recipient is a data controller, one of the two controller-controller model contracts should be selected; if the recipient is a data processor, the controller-processor model contract should be selected.

Once the correct model contract has been selected, a company can revise and modify it to suit their needs – so long as the modifications do not interfere with the substantive rights and obligations contained within the template. For example, a company can decide whether the model contract should be a stand-alone agreement, an exhibit to an existing agreement between the parties, or integrated into a larger contract.

Step 3 – National law administrative requirements (e.g. notification or registration with local Data Protection Authority).

Many countries within the EU currently require that a company that enters into a model contract take the additional step of notifying the country's Data Protection Authority of the existence of the agreement. Notification requirements differ by country. For example, some countries simply require that the Data Protection Authority be alerted that a transfer is occurring; other countries require that the model contract be filed with the Data Protection Authority. These national requirements will largely be removed over the next couple of years as European data privacy laws are unified as part of pan-Europe privacy reforms that began with the passage of the General Data Protection Regulation (GDPR).

## D. EU Binding Corporate Rules

The following provides background concerning the approved Binding Corporate Rules ("BCR") procedure. BCRs are in-kind privacy rules and standards that allow multinational groups of companies to transfer personal data within their group of companies, including to corporate affiliates outside of the EU. In order to obtain approval at a BCR, a company's privacy policy has to demonstrate that it ensures an adequate level of data protection and respective safeguards under EU law. BCRs are an internal tool only and do not allow for any data transfers outside of a corporate group.

Companies should go through the following five steps if they choose to obtain BCR approval:

Step 1: Designate the lead EU data protection authority ("DPA"), *i.e.* the authority which will be handling the EU co-operation procedure among the other European DPAs.

Step 2: Draft and submit a BCR which meets the safeguards required by the Directive.

Step 3: The lead authority will start the EU co-operation procedure by circulating the draft BCR to the relevant DPA, *i.e.* of those countries from where entities of the group transfer personal data to entities located outside of the EU.

Step 4: The EU co-operation procedure is closed after the countries under mutual recognition have acknowledged receipt of the BCR and those which are not under mutual recognition have determined that the BCR provides sufficient safeguards.

Step 5: When the draft BCR has been considered final by all concerned DPAs, the company requests authorization to transfer data on the basis of the adopted BCR.

The new General Data Protection Regulation (GDPR) will simplify binding corporate rules and streamline the approval process, such that the rules will need to be approved by a single data protection authority instead of several.

Currently, binding corporate rules are only a tool to transfer personal data within a corporate group. Under the new GDPR this tool may be utilized by "groups of enterprises engaged in a joint economic activity" as well.

## E. Data Transfers From Asia

Europe has had data protection laws in place for over a decade. Such laws regulate how data relating to individuals (such as employees or customers) can be collected, used and transferred.

In Asia, many countries have historically relied on constitutional laws or sector based rules to protect personal data and until recently, only a few countries had any form of consolidated data protection legislation. With the need to promote the cross border flow of information, many Asian countries have in the last few years adopted consolidated data protection legislation and others are expected to follow. The following briefly summarizes the data protection laws among the major Asian countries:

| | |
|---|---|
| 8<br>The number of Asian countries that have enacted consolidated data protection legislation | 4<br>The number of major Asian countries that require most companies to appoint a data protection officer. |
| 3<br>The number of Asian countries that have enacted data breach notification legislation | 5<br>The number of Asian countries that have restrictions on the cross-border transfer of data. |

If your organization operates in Asia, or collects personal information about Asian residents, consider the following:

1. What laws apply to the collection and use of personal information of individuals?

2. Do I have to obtain consent in order to collect personal data, and if so, what level of consent is required, (e.g. explicit, implied)?

3. What information do I have to provide to data subjects in Asia about the personal information being collected and processed and in what form does this have to be provided?

4. Are there special categories of sensitive personal information to which additional restrictions apply?

5. Are there any restrictions on the collection, use or transfer of personal information for marketing purposes?

6. Are there any restrictions on transferring the data out of the jurisdiction in which it is collected and how can these be overcome?

7. Are there any data localization laws that would require me to retain the information in the local jurisdiction?

8. Do I have to appoint a data protection officer in the local jurisdiction?

9. Do I have to comply with local data protection laws if I am only processing personal information?

10. What are the penalties for non-compliance with any applicable data protection laws?

# GLOSSARY

The following is a quick-reference to defined terms or acronyms that are used in this handbook:

| | |
|---|---|
| AMP | Administrative Monetary Penalties under CASL |
| BCP/DR | Business Continuity Planning / Disaster Recovery Plan |
| BCR | Binding Corporate Rules |
| BYOD | Bring your own device |
| CalOPPA | The California Online Privacy Protection Act, Cal. Bus. & Prof. Code 22575, *et seq.* |
| CAN-SPAM Act | Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 |
| CASL | Canadian Anti-Spam Law |
| CEM | Commercial Electronic Message under CASL |
| Consumer Sentinel | A collection of databases maintained by the FTC that tracks complaints submitted by consumers concerning data privacy, data security, advertising, and marketing practices of organizations. |
| COPPA | The Children's Online Privacy Protection Act |
| CPO | Chief Privacy Officer |
| CRTC | Canadian Radio Television and Telecommunications Commission |
| DAA | Digital Advertising Alliance |
| Directive | The EU Data Protection Directive 95/46/EC. |
| DOPAA | Delaware Online Privacy and Protection Act |
| DPI | The FTC's Division of Planning and Information. |
| DPIP | The FTC's Division of Privacy and Identity Protection. |
| FDIC | Federal Deposit Insurance Corporation |
| FFIEC | Federal Financial Institutions Examination Council |
| FTC | Federal Trade Commission |
| FTCA | Federal Trade Commission Act |
| HHS | The Department of Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| Interagency Guidelines | Interagency Guidelines Establishing Information Security Standards pursuant to the Gramm-Leach-Bliley Act |
| NAI | Network Advertising Initiative |
| OCR | The Office of Civil Rights within the Department of Health and Human Services |

| | |
|---|---|
| PCI | Payment Card Industry |
| PFI | A forensic investigator certified by the PCI Council |
| PHI | Protected Health Information |
| RA | Resolution Agreement entered with the Department of Health and Human Services |
| ROSCA | The Restore Online Shoppers' Confidence Act |
| Safe Harbor | The US-EU Safe Harbor certification process. |
| SSN | Social Security Number |
| WISP | A written information security program. |

# CONTRIBUTORS

Chris Achatz, Associate (Boulder, Colorado)

Stephanie Bradshaw, Associate (Kansas City, Missouri)

John Bush, Associate (Atlanta, Georgia)

David Chen, Associate (Boulder, Colorado)

Nicole Gates, Associate (Santa Monica, California)

Jason Haislmaier, Partner (Boulder, Colorado)

Joshua James, Associate (Washington DC)

Leila Knox, Associate (San Francisco, California)

Richard Kuhlman, Partner (St. Louis, Missouri)

Michael Lanahan, Associate (St. Louis, Missouri)

Mary Logenbaker, Associate (St. Louis, Missouri)

Tracy Talbot, Associate (San Francisco, California)

Jena Valdetero, Partner (Chicago, California)

David Zetoony, Partner (Washington DC / Boulder, Colorado)