Contemporary Legal Notes

Washington Legal Foundation

Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Data Privacy and Security: A Practical Guide for In-House Counsel

By
David Zetoony
Bryan Cave LLP

Foreword
By
Michael Kaplan
Senior Vice President, Chief Legal Officer,
and Chief Compliance Officer
Red Robin Gourmet Burgers, Inc.

Washington Legal Foundation
Contemporary Legal Note Series

Number 77
May 2016

TABLE OF CONTENTS

ABOUT WLF'S LEGAL STUDIES DIVISION iii

ABOUT THE AUTHOR iv

FOREWORD v

INTRODUCTION 1

I. DATA PRIVACY 1

A. Data Maps and Data Inventories 1
B. Website Privacy Policies 3
C. Social Security Number Privacy Policies 4
D. Mobile-App Privacy Policies 5
E. Privacy Certifications/Trustbrands 6
F. Employer Privacy Policies 7
G. Bring-Your-Own-Device Policies 8
H. Employee Monitoring 10
I. Social Media Privacy Concerns 11
J. Online Behavioral Advertising 12
K. Video Viewing Information 14
L. Geo-Location Tracking 14
M. Radio Frequency Identification 15
N. Email Marketing in the US 17
O. Email Marketing in Canada 18
P. Collecting Information from Children 20
Q. Facial Recognition Technology 21
R. Passing Data Between Retailers to Facilitate Transactions 22
S. Due Diligence in a Merger or Acquisition 23
T. Vehicle Event Data Recorders 24
U. Self-Driving Cars 25
V. FTC Tracking of Privacy Complaints 26
W. Companies the FTC Perceives as Top Violators 27
X. Companies the FTC Perceives as Emerging Threats 28
Y. Organizing Data Privacy Within a Company 28

II. DATA SECURITY 29

A. Written Information Security Policies 29
B. Encryption 30
C. Document Retention Periods 31
D. Cyber Insurance 32
E. Bounty or Bug Programs 33
F. Cyber Extortion 34

G. Ransomware 35
H. Federal Deposit Insurance Corporation Cybersecurity Examinations 36
I. Wire Transfer Fraud 37
J. Incident-Response Plans 38
K. Forensic Investigators 39
L. Credit-Monitoring Services 40
M. Reputation Management 41
N. Data-Breach Notification Laws 42
O. Cybersecurity Disclosures 43
P. Class-Action Litigation Trends 44
Q. Credit Cards and the Payment Card Industry's Data-Security Standard 45
R. Negotiating Credit Network Agreements 46
S. Credit Card Breaches 49
T. Causes of Healthcare Data Breaches 50
U. Healthcare Data-Breach Litigation 51
V. Healthcare Data-Breach State and Federal Enforcement 52
W. Healthcare Business Associates 53
X. Third-Party Vendor Management Programs 54
Y. Cloud Computing 55

III. DATA TRANSFERS FROM OTHER COUNTRIES 57

A. EU-US Safe Harbor Framework and its Validity 57
B. EU Model Clauses 57
C. EU Binding Corporate Rules 58
D. EU General Data-Protection Regulations 58
E. Data Transfers from Asia 58

GLOSSARY 60

ABOUT WLF'S LEGAL STUDIES DIVISION

Washington Legal Foundation (WLF) established our Legal Studies division in 1986 to address cutting-edge legal issues through producing and distributing substantive, credible publications designed to educate and inform judges, policy makers, the media, and other key legal audiences.

Washington is full of policy centers of one stripe or another. From the outset, WLF's Legal Studies division adopted a unique approach to set itself apart from other organizations in several ways.

First, Legal Studies focuses on legal matters as they relate to sustaining and advancing economic liberty. The articles we solicit tackle legal policy questions related to principles of free enterprise, individual and business civil liberties, limited government, and the Rule of Law.

Second, WLF's publications target a highly select legal policy-making audience. We aggressively market our publications to federal and state judges and their clerks; Members of Congress and their legal staff; executive branch attorneys and regulators; business leaders and corporate general counsel; law professors; influential legal journalists, such as the Supreme Court press; and major media commentators.

Third, Legal Studies operates as a virtual legal think tank, allowing us to provide expert analysis of emerging issues. Whereas WLF's in-house appellate attorneys draft the overwhelming majority of our briefs, Legal Studies possesses the flexibility to enlist and the credibility to attract authors with the necessary background to bring expert perspective to the articles they write. Our authors include senior partners in major law firms, law professors, sitting federal judges, other federal appointees, and elected officials.

But perhaps the greatest key to success for WLF's Legal Studies project is the timely production of a wide variety of readily intelligible but penetrating commentaries with practical application and a distinctly commonsense viewpoint rarely found in academic law reviews or specialized legal trade journals. Our eight publication formats are the concise COUNSEL'S ADVISORY, topical LEGAL OPINION LETTER, incisive LEGAL BACKGROUNDER, in-depth WORKING PAPER, practical CONTEMPORARY LEGAL NOTES, informal CONVERSATIONS WITH, balanced ON THE MERITS, and comprehensive MONOGRAPH.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "WLF," and every WLF publication since 2002 appears on our website at www.wlf.org.

To receive information about previous WLF publications, or to obtain permission to republish this publication, please contact Glenn Lammi, Chief Counsel, Legal Studies, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302, glammi@wlf.org.

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—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 in a variety of industries ranging from national department stores to restaurants to international outsourcers.

The author gratefully acknowledges the following Bryan Cave LLP attorneys' contribution to this CONTEMPORARY LEGAL NOTES:

Gupinder Assi (Singapore)
Chris Achatz, Associate (Boulder, CO)
Stephanie Bradshaw, Associate (Kansas City, MO)
Mary Beth Buchanan, Partner (New York, NY)
John Bush, Associate (Atlanta, GA)
Jana Fuchs, Associate (Hamburg, Germany)
Nicole Gates, Associate (Santa Monica, CA)
Jason Haislmaier, Partner (Boulder, CO)
Joshua James, Associate (Washington, DC)
Andrew Klungness, Partner (Santa Monica, CA)
Leila Knox, Associate (San Francisco, CA)
Richard Kuhlman, Partner (St. Louis, MO)
Michael Lanahan, Associate (St. Louis, MO)
LaDawn Naegle, Partner (Washington, DC)
Daniel Prywes, Partner (Washington, DC)
Tracy Talbot, Associate (San Francisco, CA)
Jena Valdetero, Partner (Chicago, CA)
Amber Williams, Privacy Intern (Boulder, CO)

FOREWORD

By
Michael Kaplan
Senior Vice President, Chief Legal Officer,
and Chief Compliance Officer
Red Robin Gourmet Burgers, Inc.

Virtually every company collects personal information from their customers and employees. More than 200 interwoven U.S. federal and state laws regulate the collection, processing, use, and storage of personal information. As the number of data-breach incidents continues to climb, this patchwork of federal and state data-privacy and security laws continues to expand both in size and complexity. As recent national headlines prove, the consequences of failing to safeguard personal information can be enormous: class-action lawsuits, government investigations and fines, and, perhaps most significantly, the loss of sales and brand reputation. The C-suite and corporate boards increasingly look to the in-house general counsel to guide their companies safely through this maze of legal and regulatory risks.

Do you feel prepared? For most in-house attorneys, the answer is "no." Their expertise probably lies in the areas of litigation, transactions, or employment law. My own background was in corporate and securities law. Like most in-house attorneys, I was unfamiliar with data-privacy and security issues when I made the transition to general counsel several years ago. And like most corporate counsel, I was uncertain how to chart the proper compliance course for my organization or where even to begin. Given the extreme complexity of data privacy and security rules, even the most seasoned in-house counsel may experience similar uncertainty. This Washington Legal Foundation (WLF) CONTEMPORARY LEGAL NOTES offers a roadmap for in-house counsel tasked with the daunting challenge of managing compliance in a high-risk legal environment.

When dealing with complex compliance challenges, corporate counsel are often better served by easily digestible summaries than dense legal memoranda. Over the past 20-plus years, I have heard frustrated business people implore outside counsel all too often, "Don't give me a legal treatise, just tell me what I am supposed to do." One of David Zetoony's strengths as an outside counsel is his ability to provide crisp advice and clear, actionable direction. That quality is positively reflected in this WLF paper.

The CONTEMPORARY LEGAL NOTES' title promises us a practical guide for navigating data-privacy and security issues, and it delivers. The paper is a concise but comprehensive overview of the vast legal and regulatory landscape, covering more than 50 distinct topics. Like any good travel guide, the paper introduces each of these 50 points of interest with a brief description, including its background and history, a straightforward translation of the local dialect of technical jargon and acronyms, and some statistical information so that readers can better appreciate its significance. Most importantly, it provides clear directions and actionable lists of "Areas to explore," "Things to do," and even "What to do in case of an emergency" for each topic area.

Both attorneys who are new to the in-house counsel world and those who have occupied that role for years—including compliance officers—will be turning to this guide regularly as data-privacy and security issues legal risks only intensify.

DATA PRIVACY AND SECURITY:
A PRACTICAL GUIDE FOR IN-HOUSE COUNSEL

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 the information technology ("IT"), human resources ("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.

As a result, 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 implicate data privacy and security. It is simply not possible to sit down and read a statute to get caught up.

This Washington Legal Foundation CONTEMPORARY LEGAL NOTES is intended to be a desk reference for in-house attorneys. It includes over 50 data privacy and security topics. The discussion under each topic is not styled in the form of a legal treatise. Instead, each section provides a straightforward overview of the law relevant to that topic, statistics to help understand the issue and benchmark its importance, and a functional list of bullet points or questions to immediately break down an issue.

I. DATA PRIVACY

A. Data Maps and Data Inventories

Knowing the type of data collected, where it is being held, with whom it is being shared, and how it is being 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 attempts to solve are relatively straightforward, the process of conducting a data map can be daunting depending upon the size and structure of an organization. In addition, it is important to remember that data constantly changes within an organization. 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.

Corporate counsel should consider the following when deciding whether to conduct a data map or a data inventory:

1. Which departments are most likely to possess data?
2. Who is the point person in each department responsible for data?
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 who 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?

#1: Privacy officers ranked maintaining a data map as their top priority.[1]

100%: Percentage of companies that identified maintaining a data map as relevant.[2]

33%: Percentage of companies that have a data map.[3]

17%: Percentage of companies that have a data map and use it to track the flow of data between systems.[4]

A data map should include:

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 within the organization has access to the data.
8. Who outside of the organization has access to the data.
9. Whether the data crosses national boundaries.
10. The retention schedule (if any) applied 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] *Ibid.*
[3] *Ibid.*
[4] *Ibid.*

10 minutes: Average time it takes for a person to read a privacy policy.[5]

244 hours: Amount of time it would take a person to read the privacy policies of all the unique websites they visit in a year.[6]

$0.59: Premium that study participants were willing to pay to purchase a $15 item from a website that proactively displayed strong privacy protections instead of from one with no privacy position.[7]

B. Website Privacy Policies

Although financial institutions, healthcare providers, and websites directed to children are required to create consumer-privacy policies under federal law, 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. 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.

Factors counsel should consider when drafting or reviewing a privacy policy:

1. Is the organization subject to a federal law that requires a privacy policy to take a particular form or include particular information?
2. Does the privacy policy describe the main ways in which the organization collects information?
3. Does the privacy policy describe the ways in which the 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 the organization's assets?
6. Would the privacy policy interfere with future ways in which the organization may want to monetize data?
7. Does the privacy policy use terms that might be misunderstood or misinterpreted by a regulator or a plaintiffs' attorney?
8. Does the privacy policy comply with the laws in each jurisdiction to which the organization is subject (*e.g.,* CalOPPA)?
9. Should the privacy policy only govern information collected via the organization's website, or all information collected by the organization?

[5] 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 at 541 (2008).
[6] *Ibid.*
[7] 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.

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 the 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 the 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

The Social Security Administration established Social Security Numbers ("SSN") 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. Congress later barred agencies from disclosing SSN to third parties. Federal law does not, however, regulate private sector use of SSN.

Based upon a growing recognition that SSN can be used to perpetrate identity theft, state legislatures have passed statutes regulating the private sector's use of SSN. Among other things, these statutes prohibit organizations from 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 companies to securely destroy SSN when the information is no longer in use.

1936: Year SSN were created.[8]

$30: Cost on the black market to obtain a dossier with a consumer's SSN.[9]

$500/month: Civil penalty imposed by one state for failing to adopt a privacy policy when collecting SSN.[10]

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.

---

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

[9] 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.

[10] TEX. BUS. & COM. CODE § 501.052(a), 501.053(a).

3. Who within the organization will have access to SSN.

4. How the organization will protect SSN.

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.[11]

D. Mobile-App Privacy Policies

$2,500: Possible penalty under California law for each app downloaded without a privacy policy.[12]

11%: Percentage of banking-related apps that contain "harmful" code.[13]

>60%: Percentage of popular dating apps vulnerable to hacker exfiltration of personally identifiable information.[14]

Many of the most popular mobile apps collect personally identifiable information ("PII"). 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 addition, the California Attorney General dictates that applications that collect personal information are required to post a privacy policy pursuant to CalOPPA.

Corporate counsel should consider the following privacy issues if their organization develops mobile apps:

1. Does the app have a privacy policy? Privacy policies are a best practice if the app will be used in connection with PII. As discussed above, if the app solicits information from California residents, a privacy policy may be required.

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.

3. How is PII 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 a mobile app's privacy policy should state accurately where PII is stored.

4. Does the app communicate PII 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 PII? A 2013 study concluded that 18 percent of apps sent usernames and passwords by non-

[11] MICHIGAN COMPILED LAWS § 445.84(1)(e), (2).

[12] California Attorney General Website, *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law* (Oct. 30, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance.

[13] Pierluigi Paganini, *11 Percent of Mobile Banking Apps Includes Harmful Code*, SECURITY AFFAIRS (Feb. 7, 2015), http://securityaffairs.co/wordpress/33212/malware/mobile-banking-apps-suspect.html.

[14] PR Newswire, *IBM Security Finds Over 60 Percent of Popular Dating Apps Vulnerable to Hackers* (Feb. 11, 2015), http://www.prnewswire.com/news-releases/ibm-security-finds-over-60-percent-of-popular-dating-apps-vulnerable-to-hackers-300034321.html.

encrypted communications.[15] Consider stating within the app's privacy policy whether the app transmits PII, and, if so, whether the information is encrypted in transit.

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

7. Can access to the app be revoked remotely? The revocation of access to an app potentially raises privacy concerns that may need to be addressed in a privacy policy.

E. Privacy Certifications/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 displaying 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%: Percentage of consumers that are worried about online privacy.[16]

76%: Percentage of consumers who claim they look for privacy certifications and seals on a website.[17]

~50%: Percentage of consumers who say that they would share their interests with advertisers *if* the advertiser's privacy policy was "certified."[18]

2: The number of certifying agencies the FTC has alleged offered deceptive seals.[19]

Factors counsel should consider regarding the organization's purchase of 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 the purchasing organization's practices meet the certifying agency's standards?

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

5. Has the certifying agency been investigated by the Federal Trade Commission ("FTC"), or another consumer protection authority, for deceptive or unfair practices?

---

[15] *Ibid.*
[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/.
[19] *In the Matter of True Ultimate Standards Everywhere, Inc., a corporation, d/b/a/ TRUSTe, Inc.*, No. C-4512 (Mar. 18, 2015), https://www.ftc.gov/system/files/documents/cases/150318trust-edo.pdf; *Federal Trade Commission v. ControlScan, Inc.* Civ. No. 1 1--CV-0532 (N.D. Ga. Mar. 8, 2010), https://www.ftc.gov/system/files/documents/cases/20100308controlscan.pdf.

6. If so, can counsel be 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 the 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 its website if the license expires?

9. Have plaintiffs' 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

5: The number of states that have enacted statutes that may require employers to create employee privacy policies.[20]

$500: The fine assessed under New York's statute to employers that unlawfully disseminate an employee's SSN.[21]

$275,000: The damages awarded to a group of Michigan employees who sued their union after it failed to safeguard their SSN.[22]

In 2005, Michigan became the first state to pass a statute requiring employers to create an internal privacy policy that governs disclosure of some forms of highly sensitive information about their employees. Michigan's Social Security Number Privacy Act expressly requires employers to create policies concerning the confidentiality of employees' SSN and to disseminate those policies to employees. New York has adopted a similar statute. Connecticut, Massachusetts, and Texas have statutes mandating the establishment of privacy policies that could also apply in the employer-employee context.

Companies should determine 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.

When drafting or reviewing an employee privacy policy, counsel should consider the following:

1. Does the privacy policy capture the main ways in which the 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 policy limit access to information or documents that contain employee SSN and other personal information?

---

[20] 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).

[21] N.Y. LAB. LAW § 203-d(3).

[22] John F. Buckley & Ronald M. Green, STATE BY STATE GUIDE TO HUMAN RESOURCES LAW § 1.36 (2015).

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

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

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

8. Can the average employee understand the privacy policy?

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

10. Does it comply with the laws in each jurisdiction in which the organization is subject?

G. Bring-Your-Own-Device 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: People who will bring smartphones to work by 2017.[23]

>$300: The anticipated amount that the typical organization will spend per employee in 2016 on mobile applications, security, management, and support.[24]

>38%: The percentage of companies that expect to stop providing devices to workers by 2016.[25]

Counsel should consider the following when drafting a BYOD policy:

1. Is the scope of the 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 provide the basis for a BYOD policy. 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 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

[23] Matt Hamblen, *With BYOD Smartphones on the Rise, IT Headaches Will Become Migraines*, COMPUTERWORLD (Jan. 27, 2014), http://www.computerworld.com/article/2487005/byod/with-byod-smartphones-on-the-rise-it-headaches-will-become-migraines.html.
[24] David A. Willis, *Bring Your Own Device: The Facts and the Future*, GARTNER (Apr. 11, 2013), https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf.
[25] *Ibid*.

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 their data will be "floating" on multiple devices by limiting the types of data accessible to mobile devices (*e.g.*, email) and 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).

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

74%: Percentage of organizations that currently allow or plan to allow BYOD.[26]

42%: Percentage of employees that log onto their business email while on sick leave.[27]

<10%: Percentage of companies that report having complete awareness of what devices access their networks.[28]

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.

6. What procedure is in place for an employee to report a missing mobile device? Employees should report a missing device to someone—perhaps the IT department or help desk—so that the organization can follow its device removal policy.

7. What steps does the organization take to disseminate its mobile device policies? Organizations often rely on their IT staff, self-help materials, and employee certifications to ensure employee awareness and 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 who 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.

[26] Teena Hammond, *Research: 74 Percent Using or Adopting BYOD*, ZDNET (Jan. 5, 2015), http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/.
[27] Bas Van Den Beld, *The Power of Mobile*, STATE OF DIGITAL (Feb. 24, 2012), http://www.stateofdigital.com/the-power-of-mobile/.
[28] Ingram Micro Advisor, *23 BYOD Statistics You Should Be Familiar With*, http://www.ingrammicroadvisor.com/big-data/23-byod-statistics-you-should-be-familiar-with.

H. Employee Monitoring

Federal laws prohibit the interception of another's electronic communications, but they 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 exceptions may apply once the personal nature of a communication is determined. Also, 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.

80%: Percentage of employers who actively monitor their employees electronically.[29]

2: States that require notice to employees of electronic monitoring.[30]

23: States that introduced or considered legislation in 2015 prohibiting employers from requesting passwords to social media accounts.[31]

18: States that passed legislation prohibiting employers from requiring access to social media accounts.[32]

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

Employers may also monitor what an employee posts publicly to social media. However, under many states' 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 access private content. 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 their telephone network without the consent of one or both parties to the communication. If all parties are in California, notification must be provided (such as through a beep) that the call is being recorded.

Counsel should consider the following when crafting employee-monitoring policies:

---

[29] *Is Employee Monitoring Legal?*, IN CONTEXT: THE OFFICIAL SPECTORSOFT CORPORATE BLOG (Feb. 10, 2014), http://www.spectorsoft.com/blog/20140210-is-employee-monitoring-legal.html.

[30] National Conference of State Legislatures, *State Laws Related to Internet Privacy* (Feb. 24, 2015), 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).

[31] National Conference of State Legislatures, *Access to Social Media Usernames and Passwords* (Sept. 14, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

[32] Aliah D. Wright, *More States Ban Social Media Snooping*, Society for Human Resource Management (Aug. 12, 2014), http://www.shrm.org/hrdisciplines/technology/articles/pages/social-media-snooping.aspx.

1. Does the organization publish an acceptable use policy?
2. Does the acceptable use policy explain what employees may and may not do on the internet while at work?
3. Does the acceptable use policy explain the disciplinary consequences of violating the policy?
4. Can the organization block or otherwise restrict access to internet sites that are barred under the acceptable use policy?
5. Does the 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 the organization's employees consented?
7. If the organization monitors phone calls, does it have a policy to cease monitoring when a call is clearly personal in nature, and does it follow that policy?
8. Can employees argue that they have an expectation of privacy to their work emails or to their work phone calls?
9. Is the organization monitoring emails to or from password-protected personal accounts?
10. Are organization 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 the use of third-party social media websites offers businesses significant advantages, such use 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 the business or its customers. To the extent that the social media platform's privacy practices are not consistent with the practices of the organization, they may contradict or violate the privacy notice that the organization provides to the public.

Counsel evaluating an organization's use of social media should consider the following:

1. How would a data breach of social media platforms affect the organization? Does counsel have a plan if the organization's social media account is breached?
2. Does the organization share information with an intermediate service provider, such as a social media analytics company, to provide or analyze social media services?

1. Is the organization's internal data or customer personal information protected under its agreements with third parties, including social media platforms?
2. What types of customer personal information are solicited, collected, maintained, or disseminated via the organization's social media platforms (*e.g.*, geo-location)?
3. Does the organization display information or images of users or other people, including its employees? Did the people in the images give their permission and/or sign a release?
4. Is the organization's client list private? Do its employees connect to clients on social media?
5. How is information about customers that is collected from social media sites stored? Do any third parties have access to that information?
6. Do users log in to services or make purchases through a social media platform?
7. What type of personal information do customers share on social media platforms?
8. Does the organization's use comply with the platform's policy for collecting data from users? Does the organization review the platform's policies regularly?
9. Does the organization have a social media policy governing employees' use of social media, particularly pertaining to sharing confidential customer and organizational data on the platform?
10. How does the organization's IT team manage the security and passwords for its social media sites?

80%: Percentage of Fortune 500 companies on Facebook.[33]

97%: Percentage of Fortune 500 companies with a corporate presence on LinkedIn.[34]

75%: Percentage of online adults using social-networking sites.[35]

2 million: Number of Facebook, LinkedIn, Google, and Twitter passwords stolen in 2013 hack.[36]

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 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

[33] Nora Ganim Barnes and Ava M. Lescault, *The 2014 Fortune 500 and Social Media: LinkedIn Dominates as Use of Newer Tools Explodes*, UMASS. DARTMOUTH, http://www.umassd.edu/cmr/socialmediaresearch/2014fortune500andsocialmedia/.

[34] *Ibid.*

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

[36] Jose Pagliery, *2 Million Facebook, Gmail and Twitter Passwords Stolen in Massive Hack*, CNN Money (Dec. 4, 2013), http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/.

tracking cookies on the computers of people who visit the site, so that those individuals can be monitored across a behavioral advertising network.

2: Number of state statutes that may require companies to disclose the use of third-party behavioral advertising.[37]

102: Number of companies that are members of NAI.[38]

129: Number of companies that are members of DAA.[39]

858: Number of references on the FTC's website to "behavioral advertising."[40]

2-60: The number of tracking cookies placed by the top 5 retailers on their websites.[41]

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 and have 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 could be interpreted as requiring websites to notify consumers if they permit third-party behavioral advertising.

Factors to consider when evaluating an organization's online behavioral advertising practices:

1. Does the privacy policy comply with state-law mandates concerning the disclosure of first-party online behavioral advertising?
2. Does the privacy policy comply with state-law requirements concerning the disclosure of third-party online behavioral advertising?
3. Does the 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?
4. If so, do all of the behavioral advertisers permitted to use the website allow opt out via the NAI and/or DAA mechanisms?
5. Who has the authority to permit third parties to place cookies on the website?
6. Has the legal department reviewed the contracts with each behavioral advertiser with whom the organization has a relationship to verify that their privacy practices are in legal compliance and comport with the standards of the organization?
7. Have the cookies that are placed or tracked on the organization's website been audited?
8. Has the accuracy of the description of behavioral advertising contained on the website been verified?

[37] CAL BUS. & PROF. CODE §§ 22575(b)(5)-(7).
[38] Companies listed on http://www.networkadvertising.org/participating-networks as of May 2016.
[39] Companies listed on http://www.aboutads.info/participating as of May 2016.
[40] Based upon Google search restricted to FTC.gov conducted in May 2016.
[41] Top 5 retailers as identified by the National Retail Federation. Quantity of cookies identified by Ghostery on retailer home page on May 6, 2016.

K. Video Viewing Information

Congress passed the Video Privacy Protection Act ("VPPA") in 1988 in reaction to a fear that people other than consumers and video rental stores could collect information on consumers' 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 US Supreme Court, had his video rental history published by a newspaper.

41%: Percentage of US homes with access to a subscription-based video-on-demand service.[42]

>191 hours: The amount of time spent by an average consumer viewing video content each month.[43]

$2,500: Potential liability per violation of the VPPA.[44]

Among other things, the VPPA limits disclosure of rental and sales records by videotape service providers to the providers' consumers, people who have those consumers' consent, and law-enforcement agencies that have a warrant, subpoena, or court order. Recently, the plaintiffs' bar has tried to revive the VPPA by applying its provisions to websites that stream movies and digital content.

Organizations that rent, sell, or stream video content should consider the following questions to reduce liability risk under the VPPA:

1. Does the organization fall under the definition of a videotape service provider or a provider of similar audio-visual materials as those terms are defined under the VPPA?
2. Does the organization share information concerning consumers' video viewing habits with any third parties?
3. Which platforms does the organization use to provide access to videos? Do those platforms transmit personal information?
4. Does the organization obtain consent prior to sharing information about consumers who 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 city, state, zip code, or precise information that pinpoints the consumer's location to within a few feet, such as 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 the consumer requests. 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 of using a device, application, or website.

---

[42] Nielsen, *The Total Audience Report Q4 2014* (Mar. 11, 2015), http://www.nielsen.com/content/corporate/us/en/insights/reports/2015/the-total-audience-report-q4-2014.html.
[43] *Id.* at 12.
[44] 18 U.S.C. § 2710(c)(2)(A).

Every 10 Minutes: The frequency with which some apps, like weather apps, request geo-location data.[45]

91%: Percentage of adults who "agree" or "strongly agree" that consumers have lost control over how often personal information is collected and used by companies.[46]

73%: Percentage of times that an app will share geo-location information with an advertising network when asked.[47]

85%: Percentage of smartphone users who prefer mobile apps over mobile websites.[48]

10-20%: How much more marketers pay for online ads that include geo-location information.[49]

Although no federal statute currently regulates the use, collection, or sharing of geo-location data specifically, the FTC has taken the position that precise geo-location information is a form of "sensitive" personal information. The agency 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 Federal Trade Commission Act's general prohibition against unfair or deceptive practices. In addition, Congress and state legislatures have considered several proposals that would expressly regulate the data.

Organizations that collect geo-location information should consider the following questions:

1. Why is geo-location information being collected?
2. Is the least granular (*i.e.,* most general) location information possible being collected to most effectively provide a product or a service to the consumer?
3. How often must geo-location information be collected?
4. Is the user aware that geo-location information is being collected?
5. Does the user have the option to disable the collection of geo-location information?
6. Do the users 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 names?
7. Will the geo-location information be shared with third parties such as advertisers? If yes, how much and how often will it be shared?
8. Is the geo-location information encrypted in transmission from the consumer and/or at rest within the organization?

M. Radio Frequency Identification

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

[45] 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.
[46] Mary Madden, *Privacy and Cybersecurity: Key Findings from Pew Research*, Pew Research Center (Jan. 16, 2015), http://www.pewresearch.org/key-data-points/privacy/.
[47] Elizabeth Dwoskin, *Where Were You 3 Minutes Ago? Your Apps Know,* WALL ST. J. (May 23, 2015), http://blogs.wsj.com/digits/2015/03/23/where-were-you-3-minutes-ago-your-apps-know/.
[48] Andrew Sosa, *Important Considerations in Mobile App Development*, Businesscollective, http://startupcollective.com/important-considerations-in-mobile-app-development/.
[49] Dwoskin, *supra* note 47.

powered by electromagnetic induction from the magnetic fields that are produced by a RFID reading device in close proximity ("passive RFID").

RFID tags have been utilized in many industries. Manufacturers use them to track parts within a factory, or the location of a final product in a production line. Companies in the agricultural sector implant RFID tags in livestock for the identification of animals. In the payments sector, some payment cards have been embedded with RFID chips so consumers can process a payment by holding their payment card within close proximity of a point of sale device that was enabled with a RFID reader. As payment cards have shifted toward embedded microprocessors, the use of RFID technology has declined.

$11.1 billion: Size of the RFID technology market.[50]

24: States that have enacted privacy statutes focused on RFID technology.[51]

274: The number of wallets advertised by a prominent retailer as containing RFID blocking technology.[52]

Privacy advocates have complained that RFID technology could expose consumer products that contain PII to interception or eavesdropping. Specifically, media reports have expressed concern that identity thieves could use remote RFID readers to steal information from RFID-enabled payment cards or identification cards. To date, however, this concern has not materialized.

Organizations considering the use of RFID technology to track consumers, or to save personal information, should consider the following:

1. What, if any, personal information does the 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 consumers be fully assured that the RFID tag cannot be intercepted?
7. Does the organization have a process for periodically evaluating any changes concerning the security of RFID tags?
8. Does the organization's proposed use of RFID technology comport with state laws?

[50] Statista.com, *available at* http://www.statista.com/statistics/299966/size-of-the-global-rfid-market/ (last visited Nov. 2015).
[51] 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. 2015).
[52] Search of Walmart.com for "RFID Wallet" conducted in November 2015.

N. Email Marketing in the US

$44.25: Average return on each dollar of email marketing investment.[53]

2.5 billion: Estimated number of email users.[54]

139.4 billion: Projected number of daily business emails in 2018.[55]

9,185: Number of complaints received by the FTC in a year concerning unsolicited email.[56]

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. When followed, the 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 compliance with 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.

The basic requirements of CAN-SPAM are:

1. Does the email message include: (a) complete and accurate transmission and header information; (b) a "From" line that identifies the business as the sender; (c) a "Subject" line that accurately describes the message; and (d) an effective "opt-out" mechanism?
2. Does the email either contain an email address, physical address, or other mechanism that the recipient may use for opting out of future marketing emails?
3. Is the opt-out mechanism effective for at least 30 days after the email is sent?
4. Does the organization honor all requests to opt out within 10 days?
5. Does the organization's mailing list include any recipient that has asked not to receive email?
6. Has the effectiveness of the opt-out mechanism been tested?
7. Have the vendor contracts been reviewed to determine each party's responsibilities with regard to CAN-SPAM compliance?
8. Are addresses of people who have opted out transferred outside of the organization?

---

[53] Amanda Nelson, *25 Mind Blowing Email Marketing Stats*, Salesforce Blog (July 12, 2013), https://www.salesforce.com/blog/2013/07/email-marketing-stats.html.
[54] *Ibid*.
[55] Sara Radicati, *Email Statistics Report, 2014-2018* (Apr. 2014), Radicati.com, http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf.
[56] FTC, *Consumer Sentinel Network Data Book for January–December 2014* (Feb. 2015), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

9. Does the organization use open relays or open proxies to send marketing emails?

O. Email Marketing in Canada

$10 million: The maximum Administrative Monetary Penalty that the CRTC can assess against a company for a violation of CASL.[57]

$1.1 million: The largest Administrative Monetary Penalty that has been issued since CASL came into force on July 1, 2014.[58]

200,000+: CASL-related complaints filed with the CRTC between July 1, 2014 and January 6, 2015.[59]

July 1, 2017: The date that a private right of action for CASL violations becomes available.[60]

On July 1, 2014, the central provisions of the Canadian Anti-Spam Law ("CASL") went into force. These provisions generally prohibit the sending of a Commercial Electronic Message ("CEM") without a recipient's express consent, unless the CEM contains certain proscribed sender identification information and an effective unsubscribe mechanism. CASL provides a number of nuanced exceptions to the express consent requirements of the law. The Canadian Radio-television and Telecommunications Commission ("CRTC") enforces CASL. The CRTC has several compliance tools to enforce CASL, including the issuance of Administrative Monetary Penalties 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 four major CASL enforcement actions, but many investigations are ongoing and further clarification with regard to the most heavily utilized exceptions is expected.

Consent Exceptions:

1. <u>CASL does not apply to electronic messages sent</u>:
    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, if the message complies with the "listed" country's spam laws
    f. By a sender who has a "family" or "personal" relationship with the recipient

[57] CASL, § 20(4).
[58] Government of Canada, *CRTC Notice of Violation: 3510395 Canada Inc. (Compu.Finder)* (Mar. 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* (Jan. 15, 2015), http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html.
[60] CASL, § 91.

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"

    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 corporate counsel should consider when evaluating CASL:

1. Has an assessment of the organization's electronic communications been performed to determine if they qualify as CEMs?
2. Do any consent exceptions apply to the organization or the organization's CEMs, or does it have a special relationship with the recipient such that consent is implied?
3. If no consent exception applies, has the organization implemented a procedure to capture "express consent," including providing: (a) the purpose of requesting consent; (b) the name of the entity requesting consent; (c) a mailing address as well as a phone number, email, or web address; (d) a statement that consent can be withdrawn; and (e) an affirmative opt-in mechanism?
4. Do the CEMs include the proscribed sender indemnification information and a functioning unsubscribe mechanism?
5. Does the organization honor all requests to unsubscribe within 10 days?
6. Does the organization's mailing list include any recipient that has either unsubscribed from its CEMs or no longer qualifies for a consent exception?
7. Does the organization scrub its mailing list against the organization's "do not e-mail list"?
8. Has the organization implemented procedures to test the effectiveness of its unsubscribe mechanism?
9. Has the organization reviewed its vendor contracts to determine each party's responsibilities with regard to CASL compliance?

10. Does the organization's CASL compliance program involve senior management and include a written policy, risk assessments, record keeping, staff training, and a complaint-handling process?

P. Collecting Information from Children

549: Number of complaints received by the FTC about companies violating COPPA.[61]

33: The most complaints received against a single company.[62]

24: Number of enforcement actions taken by the FTC under COPPA.[63]

$3 million: The largest COPPA fine obtained by the FTC.[64]

The Children's Online Privacy Protection Act regulates information collection from children over the internet. 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, such as 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 online games or sweepstakes.

The most common complaints about children's websites:[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.

When counsel review an organization's website, they should determine the following:

1. Does the website ask children to provide information?
2. If not, does it automatically collect information about a child's computer or session?
3. Would the website appeal to children?
4. Has the FTC received complaints about it? If so, how many and what issues were raised in the complaints?
5. Does the website ask for parents' permission to collect information about children?

[61] Based upon analysis of consumer complaints received by the FTC between January 2008 and August 2013.
[62] *Ibid.*
[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. Playdom, Inc.*, Case No. CV11-00724 (C.D. Cal. May 24, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/05/110512playdomconsentorder.pdf.
[65] Based upon analysis of consumer complaints received by the FTC between January 2008 and August 2013.

6. Does it verify that the parent is the actual parent of a child?
7. Has the verification mechanism been approved by the FTC?
8. Does the website's privacy policy comply with COPPA?
9. Can the organization 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 the organization?

Q. Facial-Recognition Technology

1: Number of years that an organization is allowed to keep biometric data under Texas law after the purpose for which it was collected has expired.[66]

30%: Percentage increase in accuracy of facial recognition algorithms over a three-year period.[67]

80: Number of public comments received following an FTC workshop on facial recognition technology.[68]

5: Number of state data-breach notification laws that may apply to facial recognition telemetry if lost or stolen.[69]

$5,000-$25,000: The range of possible fines and damages that could be assessed under state law for each violation of a facial recognition statute.[70]

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 identify employees or criminals), marketing to consumers (*e.g.*, cameras that identify particular customers), or designing products that quickly categorize digital media (*e.g.*, photograph sorting).

No federal statute 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.

Two states have enacted statutes that govern the technology. Those statutes require that a company notify state residents that the technology is in use and obtain the consent of those subject to the technology.

The FTC recommends the following practices 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.
3. **Sensitivity of Video Feed**. Companies should consider the sensitivity of the data that they capture including, specifically, not placing cameras in areas in

[66] *See*, *e.g.*, 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).

which consumers would not expect them (*e.g.,* locker rooms, bathrooms, healthcare 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. Passing Data Between Retailers to Facilitate Transactions

Online retailers often gather information about a consumer that the retailer may use to identify other products, services, or companies in which the consumer may be interested. For example, if a consumer purchases an airplane ticket to Washington DC, the consumer may want information about amenities at the airport, hotels, or popular restaurants.

$63.4 billion: Amount spent per year by consumers online.[71]

4: Number of FTC enforcement actions initiated under ROSCA.[72]

100%: Percentage of ROSCA cases that have been filed by the FTC in federal district court, as opposed to an administrative adjudication.[73]

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.

Counsel should consider the following questions 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 items, would they likely think that the organization, or a third party, is processing the transaction?
5. Is the total cost of each third-party product clearly and conspicuously disclosed?

[71] comScore, *comScore Reports $56.1 Billion in Q1 2014 Desktop-Based U.S. Retail E-Commerce Spending, Up 12 Percent vs. Year Ago* (May 13, 2014), http://www.comscore.com/Insights/Press-Releases/2014/5/comScore-Reports-56-1-Billion-in-Q1-2014-Desktop-Based-US-Retail-ECommerce-Spending-Up-12-Percent-vs-Year-Ago.
[72] Enforcement actions reviewed as of July 2015.
[73] *Ibid.*

6. If the consumer indicates that they wish 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? If so, will the consumer be charged 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?

S. Due Diligence in a Merger or Acquisition

$3 million: Civil penalty imposed upon acquirer for violations of COPPA that occurred prior to sale.[74]

21: Number of times hackers penetrated a target's systems *before* the target was acquired and investigated by the FTC.[75]

9: Number of months hackers continued to penetrate a target's systems *after* the target was acquired and investigated by the FTC.[76]

The FTC can hold an acquirer responsible for the poor data-privacy and security practices of a company that it acquires. Evaluating a potential target's data-privacy and 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, and were discovered months after the transaction closed.

Counsel should consider the following due-diligence questions in a merger or acquisition transaction:

1. Has the target received a regulatory inquiry concerning its data-privacy and security practices?
2. Has it received litigation claims concerning its data practices?
3. Has it tracked complaints submitted to it by consumers?
4. Has it tracked complaints submitted by consumers to the government?
5. Is it subject to a sector-specific data-privacy or security law?
6. Does it have an appropriate Written Information Security Program?
7. Does it have an appropriate Incident-response plan?
8. How has it dealt with prior security incidents and security breaches?
9. Has it conducted and documented internal security assessments?
10. Has it conducted and documented external security assessments?
11. If the target accepted payment cards, are any vulnerabilities identified in its most recent Report on Compliance?

[74] *United States (FTC) v. Playdom*, *supra* note 64.
[75] *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.
[76] *Ibid.*

12. Does its internal privacy policies and procedures comply with legal standards?
13. Does its external privacy policies and procedures comply with legal standards?
14. Has it conducted a data map or a data inventory?
15. What are the target's data-retention policies?
16. With whom does it share data?
17. Does it have a vendor management program in place?
18. Have the vendors used by the target provided appropriate contractual protections?
19. Did it have a system in place to identify privacy or security problems?
20. Did it have employees focused on data-privacy or data-security issues?

T. 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.

96%: An estimate of the percentage of new passenger cars equipped with event data recorders.[77]

17: The number of states that have passed legislation protecting the privacy of data on event data recorders.[78]

7: The number of exceptions included in some state statutes for who may access the data.[79]

In December 2012, the National Highway Traffic Safety Administration ("NHTSA") 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, NHTSA never finalized the rule. Nonetheless, some estimates indicate that manufacturers have already equipped most passenger cars 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.

Important factors that counsel should consider if their organization utilizes event data recorders:

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

[77] Nat'l Highway Transp. Safety Admin., *U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety* (Dec. 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.

[78] 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.

[79] *See*, *e.g.*, ARK. CODE § 21-112-107 (2015).

2. If the organization intends to use event data recorder information, which state statute governs that use?
3. If the 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 the organization has obtained consent, is the consent current and valid?

U. Self-Driving Vehicles

68%: Percentage of global automotive industry executives who expect self-driving cars to be on the market by 2025.[80]

54 million: The projected number of self-driving cars on the road globally by 2035.[81]

$87 billion: The market opportunity for car manufacturers, technology developers, and original equipment manufacturers by 2030.[82]

$1.3 trillion: Annual savings in the U.S. after full market penetration of self-driving cars.[83]

Self-driving cars, or autonomous vehicles, may be the greatest disruptive innovation to travel in the next 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 cybersecurity risks. To date, five states and the District of Columbia have enacted laws that addresses autonomous vehicles or autonomous technology, but none of these 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 to that data and the risk of cyber attach increases. Hackers could potentially 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 self-driving car.

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

[80] *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.
[81] IHS Automotive, *Self-Driving Cars Moving into the Industry's Driver's Seat* (Jan. 2, 2014), http://press.ihs.com/press-release/automotive/self-driving-cars-moving-industrys-drivers-seat.
[82] Lux Research, *Set Autopilot for Profits: Capitalizing on the $87 Billion Self-Driving Car Opportunity* (Apr. 29, 2014), https://portal.luxresearchinc.com/research/report_excerpt/16874.
[83] Morgan Stanley, *Autonomous Cars: The Future Is Now* (Jan. 23, 2015), http://www.morganstanley.com/articles/autonomous-cars-the-future-is-now/.

1. Do current regulations cover the organization's self-driving car? If so, what aspect of the self-driving car do these regulations cover, and what do those regulations require?
2. What types of data does the organization's driverless technology collect?
3. Who else has access to the data and what are these third parties doing with it.
4. Does the organization have a duty to notify the driver of the self-driving car of the data it is either actively or passively collecting?
5. Does the organization have a duty to notify the driver if it loses the data or, based on the data, the organization is aware of conditions that could put the driver in danger?
6. What choices has the organization given, or is it required to give, the driver of the self-driving car?
7. Has the organization attained appropriate releases of liability permitted under current regulations?
8. Is the organization's self-driving car or driverless technology susceptible to a cyberattack?
9. Has the organization tested and determined that its driverless technology is highly resilient to cyber threat?
10. Has the organization procured insurance in sufficient amounts to cover likely risks and threats?

22 million: Number of consumer complaints maintained in Consumer Sentinel.[84]

89.9%: Percentage of FTC enforcement actions that target a company found in Consumer Sentinel.[85]

28: Number of government agencies that wend complaints to Consumer Sentinel.[86]

195: Number of distinct "law violations" tracked by the FTC.[87]

122–8,293: Quantity of complaints filed per month against the top 50 organizations tracked.[88]

V. FTC Tracking of Privacy Complaints

The FTC collects complaints against 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 the FTC and other consumer-protection regulators use 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

[84] FTC, *Consumer Sentinel Network Data Book for January-December 2013*, at 3 (Feb. 2014) (9 million complaints from Consumer Sentinel and 13 million from do-not-call database).
[85] FTC, *Fiscal Year 2014 Performance Report and Annual Performance Plan for Fiscal Years 2015 and 2016*, at 48, https://www.ftc.gov/system/files/documents/reports/1-fy-2015-2016-performance-plan-fy-2014-performance-report/pprfy15-16.pdf.
[86] FTC, *Consumer Sentinel Network Data Contributors*, https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors.
[87] Based upon Law Violation Codes used within the FTC's Consumer Sentinel database.
[88] FTC, *Top Companies Receiving Complaints in Consumer Sentinel* (Nov. 1, 2014-Nov. 30, 2014).

believes may have a suspicious pattern of consumer complaints.[89] More information about both reports can be found in Sections W and X below. The vast majority of FTC enforcement-action target companies are identified within the FTC's database.

The FTC's maintenance of this database implicates the following questions in-house counsel should consider:

1. Has the organization been identified as a potential enforcement target on the FTC's Top Violator or Surge reports?
2. Does the organization routinely track the quantity of complaints that the FTC maintains about it?
3. Is the volume of complaints filed about the organization above or below those of others in the industry?
4. If the FTC or another regulator searched for the complaints about the organization what potential compliance issues would they identify?
5. If the organization were investigated by the FTC, is the volume of complaints filed about it easily explained?
6. Is the volume of the organization's complaints trending up or trending down?
7. Have plaintiffs' law firms investigated the organization's complaint volume?

W. Companies the FTC Perceives as Top Violators

Each month the FTC's Division of Planning and Information ("DPI") creates a "Top Violators" report that ranks the 50 organizations with the greatest volume of consumer complaints in that month. 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. Seventy-eight percent of companies in the top 20 violators reported that the FTC has investigated their advertising, marketing, data-privacy, or data-security practices.[90] For organizations that are new to the report, DPI reviews their complaints and summarizes the issue or issues that have been raised by consumers.

The FTC's Top Violators Report raises the following questions:

1. Is the organization identified on the current Top Violators Report?
2. Has it ever been identified on a Top Violators Report?
3. If the organization is not listed on the Top Violators Report, how close is its complaint volume to those organizations that are on the list?
4. Are competitors in the organization's industry identified on the Top Violators Report?
5. If so, and if the FTC initiated an investigation of a competitor, what impact would that have on the organization?

---

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

[90] Based upon a review of the top 20 violators from complaints volume between Nov. 1, 2009-Dec. 12, 2014, excluding companies not subject to FTC jurisdiction and complaints that do not relate to corporate behavior (*e.g.*, imposter or spoofing).

6. If so, do the complaints filed against the competing organization suggest legal compliance issues which may put the organization at risk?
7. Are companies that provide service to the organization on the Top Violators Report?
8. Are clients of the organization on the Top Violators Report?
9. If so, and if a FTC investigation were to be initiated against a client, could it have a negative impact on the organization?
10. Does the organization have a system in place to quickly identify any pertinent changes to the Top Violators Report?

85%: Percentage of CPOs that spend at least 50% of their time on privacy-specific activities.[91]

9: The average number of years of experience CPOs have in privacy-related roles.[92]

63%: Percentage of privacy offices that are housed within the legal department.[93]

41%: Percentage of CPOs that report directly to the General Counsel.[94]

3.3–25: The range of full-time employees per company retained by Fortune 1000 companies to deal specifically with privacy-related issues.[95]

X. Companies the FTC Perceives as Emerging Threats

Each month, the FTC's DPI creates a "Surge" report that identifies those organizations with the greatest increase in the volume of consumer complaints. 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.

The Surge Report raises the following questions:

1. What is the typical month-to-month variation in the organization's complaint volume?
2. Does the organization's typical variation indicate a high likelihood of being identified on a Surge Report?
3. What is the typical month-to-month variation of competitors?
4. What is the typical month-to-month variation of clients?
5. What is the typical month-to-month variation of service providers?

Y. 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

[91] IAPP, *Benchmarking Privacy Management and Investments of the Fortune 1000* at 13 (2014), https://iapp.org/resources/article/full-report-benchmarking-privacy-management-and-investments-of-the-fortune-1000/.
[92] *Id.* at 11.
[93] *Id.* at 21.
[94] *Id.* at 24.
[95] *Id*. at 17, 20. 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.

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.

If an organization is creating a privacy office or reviewing the scope of an existing office, it should 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. 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).
8. Conducting a data inventory or a data map.
9. Monitoring or auditing the organization's privacy-related practices.
10. Reporting to senior management any significant privacy-related risks or concerns.
11. Managing the cross-border transfer of information between jurisdictions with different privacy standards.
12. Working with developers, designers, or marketers to design privacy protections into new products, services, or promotions.

II. DATA SECURITY

A. Written Information Security Policies

Although federal law only requires that financial institutions and healthcare providers maintain a written information security policy ("WISP"), approximately 34 states have enacted legislation that requires organizations in other industries 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 WISP.

State statutes most commonly protect the following types of personal information:[100]

4: Number of states that require that some, or all, of a security program be in writing.[96]

3: Number of states that require an employee to be designated to maintain a security program.[97]

7: Number of states that require a security provision be included in contracts with service providers.[98]

$100-$500,000: Range of state safeguard-law penalties.[99]

- Social Security Numbers: 91%
- Financial Account Numbers: 74?
- Driver's License Numbers: 72%
- Health Records: 31%
- Federal, State, or Local Tax Returns: 15%
- Biometric Data: 12.5%

An organization's WISP typically will include the following sections:

1. Designated employee responsible for overseeing security program.
2. Procedures for appropriately destroying documents with sensitive data.
3. Encryption standards for mobile devices.
4. Encryption standards for transmitting sensitive information.
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. 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 readable text. Most statutes and regulations that require companies to utilize encryption do not mandate that a specific encryption standard be used. Some statutes do, however, require 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

[96] Bryan Cave LLP, *Survey of State Safeguard Laws* (2015).
[97] *Ibid.*
[98] *Ibid.*
[99] *Ibid.*
[100] *Ibid.*

6: Number of states that require sensitive information to be encrypted when sent across public networks.[101]

1: Number of states that explicitly require sensitive information to be encrypted when sent wirelessly.[102]

1: Number of states that explicitly require sensitive information to be encrypted when stored on laptops or on portable devices.[103]

51: Number of state data-breach notification statutes that contain an exemption for encrypted data.

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.

Counsel should consider the following factors regarding an encryption policy:

1. What types of data does the organization encrypt?
2. Is the data encrypted at rest?
3. Is the data encrypted in transit?
4. What encryption standards are used at rest and/or in transit?
5. Are those standards considered "strong" within the security community?
6. Is there evidence that those encryption standards have been compromised?
7. Is there a process to review the sufficiency of the encryption standard periodically (*e.g.,* once a year)?
8. Has the organization contractually agreed to maintain a specific encryption standard?

C. 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 the organization has less data to protect and less opportunity for it 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. Organizations wishing to minimize their data must also consider what business information they will need in the future and the impact limiting consumer or employee records may have on potential legal disputes. 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.

Considerations for designing a retention policy:

1. Does the organization systematically track all of the data fields that it collects from consumers and employees?
2. Does the organization systematically apply retention periods to each data

[101] *Ibid.*
[102] *Ibid.*
[103] *Ibid.*

> 8,000 emails: Average population of an employee's inbox.[104]

16 million: Number of pages of Excel data files that could be on a 100GB hard drive.[105]

9 months-18 months: Length of time identifying search history is kept by major search engines.[106]

field that it collects?

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 the organization's industry and for the type of data at issue?

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

6. If the organization anonymizes data, is its process legally sufficient?

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

8. If the organization decides to retain other data and documents, how does that retention increase or decrease its legal risk?

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

10. How can the organization irrevocably destroy unneeded data?

D. Cyber Insurance

Most organizations understand insurance is needed to cover risks to their property, such as fire or theft, or their risk of liability if someone is injured in the workplace. But, a substantial number of organizations do not carry coverage for data breaches despite the growing risk of such events. While many insurance companies offer cyber insurance, not all policies are created equal.

19%: Percentage of companies that had cyber insurance in 2015.[107]

52%: Percentage of companies that believed their exposure to cyber risk would increase in the next 24 months.[108]

46%: Percentage of companies that did not plan to purchase cyber insurance in the next 24 months.[109]

Why is buying cyber insurance difficult?

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

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

---

[104] Dave Troy, *The Truth About Email: What's A Normal Inbox?*, Pando.com (Apr. 5, 2013), https://pando.com/2013/04/05/the-truth-about-email-whats-a-normal-inbox/.
[105] *See* Lexis Nexis, *How Many Pages in a Gigabyte?*, https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf.
[106] *Another Step to Protect User Privacy*, Google Official Blog (Sept. 8, 2008), https://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html; Yahoo, *Data Storage and Anonymization FAQ*, https://policies.yahoo.com/us/en/yahoo/privacy/topics/datastorage/index.htm.
[107] Ponemon Institute, *2015 Global Cyber Impact Report* (Apr. 2015), http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf.
[108] *Ibid.*
[109] *Ibid.*

3. Policies often cover security but not privacy risks.

Items counsel should review when the organization shops 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 utilize for legal representation, forensic investigations, and/or crisis management?

E. Bounty or Bug Programs

426: The number of organizations that have established data security bounty programs.[110]

53%: The percentage of bounty programs that pay a bounty.[111]

$50k: One of the largest maximum rewards offered through a bounty program.[112]

$100-$25,000: Typical range of rewards offered for programs that pay monetary compensation.

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. The merits of listening to the security concerns of people outside of an organization are open to debate, however. 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.

Below is a checklist for organizations that are contemplating a bounty program or are evaluating the structure of their existing program:

- If an organization does not enact a bounty program:
    1. What are the practical implications if the organization views any hack as "unauthorized?"

[110] Vulnerability Laboratory, *Bug Bounties, Rewards, and Acknowledgements*, http://vulnerability-lab.com/list-of-bug-bounty-programs.php.
[111] *Ibid*.
[112] Google Chrome-posted maximum for compromise of a Chromebook, https://www.google.com/about/appsecurity/chrome-rewards/index.html.

2. What are the practical implications if a "white hat" hacker tries to breach security with no guidelines on how one 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 the organization?
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 the organization?
5. Would the organization view an unsolicited request for payment by a hacker as extortion?

- If an organization does enact a bounty program:
  1. Will the organization be encouraging more breaches?
  2. Is the organization confident that it can track/monitor successful participants?
  3. Will all of the systems be "in scope" for the bounty program?
  4. Should certain forms of attack be prohibited (*e.g.*, denial of service attacks)?
  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?
  7. Will the organization proactively disclose the level of compensation that a participant should expect?
  8. What conditions of confidentiality will be imposed on participants?
  9. How can unintentional access or acquisition of sensitive personal information be avoided?
  10. How will the organization receive and document security vulnerabilities?
  11. Will it utilize a third party that manages, hosts, or provides a framework for the program?

9,715: Number of entities that reported being victimized by cyber extortion over a six-month period.[113]

85%: Estimate of the percentage of cyber-extortion cases that are not reported.[114]

$2,500-$100,000: Range of unsolicited financial demands related to alleged security vulnerabilities made to Bryan Cave LLP clients between 2014 and 2015.

F. 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 it. Threats may include exploiting a security vulnerability identified by

[113] *Ibid*.
[114] NYA International, *Cyber Extortion Risk Report* (Oct. 2015) at 3.

the extorter, reporting the organization's security vulnerability to the press, or reporting the organization's security vulnerability to regulators.

The following provides a checklist for organizations that are confronted by an 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, does the organization have evidence that the extortionist has not disclosed the information or shared it with others?
4. If an extortion demand is paid, what is the likelihood that the organization will receive similar demands in the near future?
5. If the 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 the organization's cyber-insurance policy?

G. Ransomware

1,402: Number of entities that reported being victimized by ransomware over a six-month period.[115]

$300: The average ransom amount associated with ransomware.[116]

250%: Percentage increase in new crypto-ransomware families.[117]

$200-$5,000: Typical range of ransomware financial demands.[118]

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 infamous ransomware family and first appeared in 2013.

Considerations for in-house counsel if the 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?
3. Is it possible for the organization to recover the impacted files using backup systems?

---

[115] FBI*, 2014 Internet Crime Report* at 47, IC3.gov (last viewed Nov. 22, 2015).
[116] Symantec, *Security Response: The Evolution of Ransomware* (Aug. 6, 2015) at 5.
[117] *Ibid.* (increase between 2013 and 2014).
[118] FBI, *Ransomware on the Rise: FBI and Partners Working to Combat this Cyber Threat* (Jan. 20, 2015).

4. Is the variant of ransomware involved associated with a known criminal enterprise?
5. If the 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?
6. Is cyber extortion and/or ransomware covered under the organization's cyber-insurance policy?

H. Federal Deposit Insurance Corporation Cybersecurity Examinations

Federal Deposit Insurance Corporation ("FDIC") 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: Number of IT examinations at financial institutions and technology service providers conducted by FDIC in a year.[119]

8-10 days: Time spent by FDIC to perform an IT examination at a financial institution found to have adequate security.[120]

15-20 days: Time spent by FDIC to perform an IT examination at a financial institution found to have some degree of supervisory concern.[121]

20%: Percentage of consent orders issued in 2015 specifically citing deficiencies in IT as a basis for the order.

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

[119] FDIC Office of Inspector General, Report No. EVAL-15-003 (Mar. 2015).
[120] *Ibid*.
[121] *Ibid*.

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 bank have a plan for how it would communicate a breach to bank customers, regulators, and law enforcement?
9. Has the bank retained cyber-insurance coverage? Does management understand what is, and what is not, covered under the policy?
10. Does the bank have external resources already identified, and under contract, to provide assistance in the event of a security incident?

I. Wire Transfer Fraud

7,066: Number of businesses victimized by wire transfer fraud.[122]

$747 million: Amount of money lost in the US due to wire transfer fraud.[123]

14%: Percentage of businesses that were the subject of attempted or actual wire transfer fraud.[124]

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 it had made payment. The scam can lead to significant contractual disputes between the victims as to who should bear the loss.

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.

[122] FBI, *Alert No. I-082715a-PSA* (Aug. 27, 2015), http://www.ic3.gov/media/2015/150827-1.aspx#fn2 (time period for reporting 10/1/2013 – 8/1/2015).
[123] *Ibid.*
[124] Association for Financial Professionals, *2014 AFP Payments Fraud and Control Survey Report of Survey Results* at 6 (Apr. 2014), http://www.regions.com/virtualdocuments/2014_AFP_Payments_Fraud_Survey.pdf.

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.
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.

Victims of wire fraud should consider:

1. Notifying the receiving bank and requesting that a freeze be placed on any remaining funds.
2. Notifying law enforcement.
3. Investigating whether the organization's email system may have been compromised.
4. Asking business partners to investigate whether their email systems may have been compromised.

J. 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 likely required by contract 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 are 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. Such a plan can also provide a reference guide for the type of actions common to most security investigations.

Corporate counsel may have the following concerns about the organization's incident-response plan:

1. It has little relationship to how the organization actually handles security incidents.
2. It has never been tested.

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

$17/record: Amount by which one study suggests having a written incident-response plan lowers the cost of a data breach.[125]

22%: Percentage of companies that have no incident-response plan.[126]

78%: Percentage of companies with a plan lacking a scheduled review or that have never reviewed the plan.[127]

17%: Percentage of companies unsure if their plan is effective.[128]

Below is a checklist for drafting an effective incident-response plan. An effective plan:

1. Assigns a specific person or group to lead an investigation.
2. Provides a clear path for escalating information about an incident.
3. Discusses the need for preserving evidence.
4. Incorporates the legal department where appropriate to preserve attorney-client privilege.
5. Discusses how the organization will communicate externally concerning an incident.
6. Includes contact information for internal resources.
7. Includes contact information for pre-approved external resources.
8. Is reviewed annually.
9. Is tested.

K. 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-house counsel must 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.

$1.5 million: Highest amount spent on a forensic investigation.[129]

$119,278: Average amount spent on a forensic investigation.[130]

$38,500: Median amount spent on a forensic investigation.[131]

When retaining a forensic investigator, corporate counsel should consider the following:

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?

---

[125] Ponemon Institute, *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness* at 1 (Sept. 2014), http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.
[126] *Ibid.*
[127] *Id.* at 21.
[128] *Id.* at 4.
[129] Statistics based upon cyber liability insurance claims. Net Diligence, *Cyber Claims Study 2014* at 12 (2014), http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf.
[130] *Id.* at 13.
[131] *Ibid.*

3. Is there a master service agreement already in place?
4. Does the agreement contain data-privacy or data-security provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?
5. Is the agreement structured to protect attorney-client privilege?
6. Does the forensic investigator understand what the organization expects of it with regard to maintaining attorney-client privilege?
7. Does the agreement include sufficient protections in the event that the forensic investigator is breached?
8. If the organization has cyber insurance, is the forensic investigator a preferred provider and/or approved by the insurer?
9. Does the forensic investigator represent a business partner of the organization that may have an interest in the incident? If so, is there a potential conflict of interest?

L. Credit-Monitoring Services

Organizations are not generally required to offer services to consumers whose information was involved in a breach. Nonetheless, many organizations choose to offer credit reports, credit monitoring, identity restoration services, and/or identity-theft insurance. In addition, if the organization offers one of these services, laws in California and Connecticut prohibit 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 harm that might result from the breach that triggered the offering. In addition, some courts have considered businesses' voluntary offers of credit-related services to be an admission that consumers' credit is, in fact, at risk.

When evaluating a credit-related service, corporate counsel should consider the following:

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?

58%: Percentage of consumers who believe an organization should provide credit monitoring following a breach.[132]

25%: Percentage of companies that offer some form of credit-related service in their breach-notification letters.[133]

6x: The odds of being sued decrease by this amount when an organization offers free credit monitoring.[134]

4: The number of credit-monitoring services the FTC has investigated for unfair or deceptive practices.

$0.25-$2.00: 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.

[132] Ponemon Institute, *The Aftermath of a Mega Data Breach: Consumer Sentiment* (Apr. 2014), http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.
[133] *Ibid.*
[134] 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 it stops providing service?
5. Has the credit-monitoring company provided the organization with adequate assurances (and indemnifications) if the information provided to it (*e.g.*, customer lists, lists of impacted consumers, or lists of impacted employees) itself becomes breached?
6. Is the organization indemnified if the credit-monitoring company's products are alleged to be unfair or deceptive?
7. Is the organization indemnified if the credit-monitoring company is negligent in providing monitoring services?
8. Has the organization been given a copy of all materials, including marketing materials, enrollment terms, insurance contracts, etc., that relate to the service being offered so that it knows what its customers/employees are being provided?
9. What service-level guarantees does the credit-monitoring company make with regard to its accessibity to enrollees?
10. Has the credit-monitoring company received any complaints, either from regulators or consumers, about its product offerings or service?

M. Reputation Management

72%: Percentage of people whot reported that they "trusted" family-owned businesses.[135]

45%: Percentage of people who reported that they "trusted" big business.[136]

12%: Percentage of customers who boycott a retailer if a data breach has been reported.[137]

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

[135] Edelman, *2015 Edelman Trust Barometer* at 7, http://www.edelman.com/insights/intellectual-property/2015-edelman-trust-barometer/trust-and-innovation-edelman-trust-barometer/executive-summary/.
[136] *Ibid.*
[137] 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.

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 greater reputational injury. Due to the complexities involved, many companies retain third-party communications, public relations, or reputational consultants to help manage reputational impact.

Counsel should consider the following factors 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 organization's industry?
3. What was the most publicized breach that it handled? (Remember that high publicity does *not* necessarily signify an effective reputation-management strategy).
4. What other breach-related services does it 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?

N. Data-Breach Notification Laws

A national legal standard governing businesses' obligations after a data breach does not currently exist. Instead, 47 states, as well as the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, have each enacted notification statutes. Alabama, New Mexico, and South Dakota do not have such a law, although their citizens may be covered in some situations by the data-breach laws of other states.

Some considerations when evaluating state data-breach laws include:

1. In which jurisdiction do the data subjects reside? Do the laws of those jurisdictions purport to be extraterritorial?
2. Is the 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 grant organizations to provide notice?

51: Number of states and territories with a breach notification law.

40%: Percentage of state laws that require notifying regulators after some breaches.

20%: Percentage of state laws that expressly confer a private right of action to consumers.

6. Do the applicable statutes require that the organization notify state regulators?
7. Do the applicable statutes require that notification letters contain specific types of information?
8. Do the applicable statutes prohibit organizations 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 the organization to notify any third parties?

O. Cybersecurity Disclosures

85%: Percentage of Fortune 500 companies that identified cybersecurity risk in a 2012 SEC filing.[138]

46%: Percentage of Fortune 500 companies in 2012 that described the extent of cybersecurity risk as "critical," "significant," "materially harmful," or "seriously harmful."[139]

53%: 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.[140]

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"). 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 that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents. The staff made clear, however, that a number of disclosure requirements may impose an obligation on an issuer to disclose such risks and incidents. The Cybersecurity Disclosure Guidance identified and discussed certain of those requirements, including disclosures required in risk factors, management discussion and analysis, 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 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

[138] Willis*, Finex North America Alert*, 2013, http://www.willis.com/documents/publications/Services/Executive_Risks/2013/FinexNA_Cyber_Update_v.pdf.
[139] *Ibid.*
[140] Protiviti, *Executive Perspectives on Top Risks for 2015*, http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2015.pdf.

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.

Public companies should, with regard to cybersecurity disclosures:

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 on active shelf registration statements, share buyback programs and other ongoing securities market activities.
5. Ensure involvement by the board of directors or the board's risk management committee in the cybersecurity risk assessment and disclosure planning.

P. Class-Action Litigation Trends

Media reports have generated a great deal of concern about and misunderstanding over data security breach-related class actions. In large part, the quantity (and success) of class-action litigation has been exaggerated.

The following provides an overview of the risks associated with lawsuits following data-security breaches.

1. Four percent of data breaches lead to litigation.[141]
2. The odds of being sued increase by three times if a company's unauthorized disclosure or disposal of data caused the breach. [142]
3. The odds of being sued decrease by a factor of six if a company provides free credit monitoring after a breach. [143]
4. The settlement rate for data-breach lawsuits is 52%.[144]
5. The likelihood of settlement increases by 30% after certification of a data-breach class action.[145]
6. The odds of settlement increase by a factor of ten when the cause of the breach is a cyberattack.[146]
7. Approximately 110 data-breach class actions were filed in 2015.[147]

[141] *Ibid.*
[142] *Ibid.*
[143] *Ibid.*
[144] *Ibid.*
[145] *Ibid.*
[146] *Ibid.*

8. Those class-action filings targeted 25 different defendants.[148]
9. The plaintiffs alleged 24 different legal theories in those lawsuits.[149]

Factors corporate counsel should consider when assessing the likelihood of their companies receiving a class-action complaint following a data breach:

1. Is a plaintiffs' firm examining government records for information relating to the organization's data-security practices? For example, has it submitted requests to the FTC under the Freedom of Information Act?
2. Was the quantity of records lost lower than 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 the organization offer credit monitoring, identity theft insurance, and/or credit repair services?
7. If so, what percentage of impacted consumers availed themselves of the offer?
8. Has the jurisdiction in which the organization is most likely to be sued (*e.g.*, its place of incorporation or where it primarily operates its business) permitted other data security class-action complaints to proceed past the pleadings stage?
9. Has the media widely reported on the data breach?
10. If so, did the media report the data breach before, or after, the company notified impacted consumers?

Q. Credit Cards and the Payment Card Industry's Data-Security Standard

Credit card acceptance agreements and card network rules require retailers to comply with the Payment Card Industry Data Security Standard ("PCI DSS"). While not all data incidents arise from PCI DSS non-compliance, if the business has a data breach where credit card data is stolen, and it is not in compliance with PCI DSS at the time the breach occurred, the business will have much larger fines and fees from the banks, card brands, and processors. In addition, PCI DSS non-compliance increases the risk exposure of a breach. As one leading forensic investigation company stated: businesses really need "all those stinking patches on all your stinking systems."[150]

---

[147] Bryan Cave LLP, *Bryan Cave 2015 Data Breach Litigation Report*, http://bryancavedatamatters.com/wp-content/uploads/2015/04/2015-Data-Breach-Litigation-Report.pdf.
[148] *Ibid.*
[149] *Ibid.*
[150] Verizon, *2015 Data Breach Investigations Report*, available at http://www.verizonenterprise.com/DBIR/2015/.

Retailers should consider the following factors when evaluating compliance with the 12 requirements of PCI DSS:

1. Are there any deficiencies identified in the organization's latest "Report on Compliance," and are the issues being remediated?
2. Have concerns been raised about the scope of the organization's latest "Report on Compliance?"
3. If PCI DSS non-compliance is identified, does this trigger contractual notification or remediation requirements for the organization?
4. With new technologies, is the organization's vendor contractually required to meet PCI DSS standards?
5. Do the device vendors and manufacturers meet requirements, such as PIN Transaction Security ("PTS") standards?
6. Is the organization's Payment Application Data Security Standard ("PA-DSS") validated?
7. Does its Point-to-Point Encryption ("P2PE") meet the PCI P2PE standard?
8. Have the vendors that access, transmit, or store credit or debit-card data provided the organization with appropriate indemnification in the event of a breach caused by the vendor or its equipment?

99.9%: Percentage of breaches that were caused by a vulnerability that was published in the data-security community for more than a year before being exploited.[151]

150+: Number of security controls required under the PCI DSS.[152]

12 Months: The frequency within which large retailers must audit and certify their compliance with the PCI DSS.[153]

R. Negotiating Card Network Agreements

Credit cards are the primary form of payment for most retailers. In order to process credit cards, a retailer must enter into an agreement with a bank and a payment processor that will process credit-card transactions on its behalf. Those agreements can be deeply complex and often have significant impacts on a retailer's financial liability in the event of a data breach. Indeed, in many cases the contractual liabilities that flow from the credit-card processing agreement surpass all other financial liabilities that arise from a breach including litigation, regulatory investigations, and the cost of conducting an investigation.

Key contractual provisions in card-processing agreements include:

1. Card Network Rules, PCI/EuroPay, MasterCard, and Visa ("EMV"), and related obligations:
    a. Incorporation of Card Network Rules:
        - Is the vendor required to comply with card network rules? Does the contract specifically reference the security

[151] *Id.* at 18.
[152] Payment Card Industry, *Data Security Standard v. 3.1*, https://www.pcisecuritystandards.org/security_standards/documents.php ("PCI DSS 3.1").
[153] American Express Merchant Regulations (Apr. 2014); Discover Merchant Operating Regulations (Apr. 2014); MasterCard Security Rules and Procedures (Feb. 2015); Visa Service Rules (Apr. 2015).

rules of the card networks— Discover Information Security and Compliance, Cardholder Information Security Program, or other?

- Is the vendor required to comply with PCI DSS?
- Is there a requirement to comply with processor's or merchant bank's Operating Guidelines? Was a copy provided to the vendor?

b. Incorporation of EMV Compliance: Does the contract or correspondence confirm the services were EMV-compliant by October 2015?

2. Applicable Law: Is there a requirement for the vendor to comply with applicable laws and regulations? Does the provision reference privacy and data-security laws?
3. Subcontractors: Is the vendor responsible for acts and omissions of third-party providers? Is the vendor required to disclose any third-party subcontractor that accesses/stores/transmits PCI data?
4. Exclusivity: Are there any restrictions on retailer's ability to hire third parties?
5. Confidentiality / Data Security:
    a. Is the vendor subject to confidentiality obligations at least as protective as those in the processor agreement?
    b. Data storage: Does the vendor agree not to store/transfer PCI data or sensitive consumer data outside the US?
    c. Is the vendor required to maintain security safeguards or have other data-security requirements?
    d. Does the vendor provide representations or warranties about data security or the provision of services generally?
    e. Does the confidentiality provision require the vendor to notify retailer to give retailer a chance to obtain a protective order prior to disclosing confidential information in response to a request from a regulator or other third party?
6. Data Incident:
    a. Is the vendor required to notify retailer immediately of a data breach involving retailer data?
    b. Is the vendor required to cooperate in the event of a data breach?
    c. Is the vendor required to comply with payment card network rule requirements if a data breach occurs (*e.g.*, does the agreement require the vendor to hire a PCI Forensic Investigator)?
7. Reserve:
    a. Does the vendor have an unlimited right to establish a reserve?
    b. Are there reserve terms to protect the retailer, such as:

- A cap on the total reserve amount?
- A daily cap on the percentage of sales the 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 merchants' funds?

8. Service Level Agreement: Does the vendor have measurable, objective performance criteria?
9. Vendor Liability:
    a. Is the vendor liable for data breaches that occur within its systems?
    b. Does the vendor indemnify retailer for damages resulting from a data breach that occurs within its systems?
    c. Is there a mutual disclaimer of types of damages?
    d. Is there a mutual liability cap? An enhanced liability cap for data breach? What is excluded from the cap?
    e. Is the vendor liable for assessments from card networks resulting from a data breach that occurs within its systems? Does retailer have a right to appeal, or step into the shoes of the vendor to contest a card network assessment resulting from a data incident?
    f. Does the retailer have unlimited or uncapped liability to the vendor?
10. Audit:
    a. Does the retailer have a general audit right? A regulatory audit right?
    b. Does the retailer have a right to conduct a security audit?
    c. Is the vendor required to provide an annual Statement on Standards for Attestation Engagements, No. 16 Report on Controls at a Service Organization ("SSAE 16")?
    d. Does the retailer have a right to terminate if a material deficiency in the vendor's SSAE 16 report is noted that puts PCI data at risk.
    e. Is remediation required?
11. Insurance:
    a. Is the vendor required to have insurance?
    b. Does the insurance exclude or significantly sublimit the contractual liabilities incurred by the vendor?
    c. Does the insurance exclude or significantly sublimit PCI-related expenses?
    d. Is the insurance limit within the ballpark of that which would cover a catastrophic breach?

e. Is the vendor required to maintain the insurance, with similar substantive terms, throughout the life of the contract?

12. Term:

    a. What is the term?

    b. Does this agreement automatically renew? If so, how long is the renewal period?

    c. What date is the deadline for submitting a notice of non-renewal?

13. Termination and Termination Assistance:

    a. Be clear on events of default and the standards for termination of the contract.

    b. Is the vendor obligated to continue providing services in the event of termination/expiration?

    c. Is the vendor obligated to help transition data regardless of reason for termination?

14. Business continuity and disaster recovery:

    a. Does the vendor have adequate business resumption and disaster recovery plans?

    b. Does the contract address procedures when data is inaccessible?

15. Dispute resolution or arbitration provisions.

S. Credit Card Breaches

26: The number of separate contractual penalties, fines, adjustments, fees and charges that the credit card brands may assess upon a retailer.[154]

56 million: Largest number of credit card numbers impacted in a single breach in 2014 or 2015.[155]

73%: Percentage of data breach class actions that relate to credit card data.[156]

Businesses' acceptance of credit cards 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.

Retailers should consider these factors when preparing to respond to a credit card data breach:

1. Does the organization's payment-processing agreement cap or limit its contractual liability in the event of a data breach?

[154] American Express Merchant Regulations (Apr. 2014); Discover Merchant Operating Regulations (Apr. 2014); MasterCard Security Rules and Procedures (Feb. 2015); Visa Service Rules (Apr. 2015).
[155] Privacy Rights Clearinghouse, http://www.privacyrights.org/.
[156] Bryan Cave LLP, *Bryan Cave 2015 Data Breach Litigation Report*, http://bryancavedatamatters.com/wp-content/uploads/2015/04/2015-Data-Breach-Litigation-Report.pdf.

2. Does the organization's payment-processing agreement cap or limit the processor's liability in the event that it suffers a data breach?

3. Does the organization have a contractual obligation to notify its payment processor or merchant bank in the event of a possible security breach?

4. Have the vendors of the organization's point-of-sale equipment provided indemnification if their equipment causes a breach?

5. Are reporting structure and contact information included in the organization's incident-response plan?

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

7. If the organization has cyber insurance, are there any exclusions that would impact its coverage for credit card-related breach costs?

8. If the organization has cyber insurance, is there a sublimit for Payment Card Industry-related liabilities?

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

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

T. Causes of Healthcare Data Breaches

46%: Percentage of breaches caused by theft of hardware of all types.[157]

34%: Percentage of thefts involving stolen laptops.[158]

9%: Percentage of breaches caused by hacking/IT intrusions.[159]

3%: Percentage of breaches caused by improper disposal.[160]

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"). The information provided to HHS provides organizations with a high level of insight concerning the types of breaches that occur in healthcare industries.

The data collected by HHS in 2014 concerning breaches affecting 500 or more individuals show that low-tech breaches remain the most common form of data loss in the health sector—surpassing more publicized hacking events.

Corporate counsel should consider the following factors when reviewing an information security program in light of HHS data:

1. Are all laptops encrypted?

[157] 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.
[158] *Ibid.*
[159] *Ibid.*
[160] *Ibid.*

2. Is laptop encryption full-disk (*e.g.*, does it apply to the entire hard drive)?
3. Is laptop encryption also file-level (*e.g.*, would it apply if files were removed from the hard drive)?
4. Does the organization permit other types of portable media in its environment like USB drives?
5. If so, are those devices encrypted at the disk or file level?
6. Are passwords enforced on laptops and other types of portable media?

U. 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 a suit proceed based solely on the allegation that the plaintiff is subject to an increased risk of harm as a result of the breach. The following chart 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 • Data loss, but no evidence of access or misuse • Data loss, but no evidence of identity theft • Loss of value of PHI because the PHI can be sold on the cyber black market • Patients' right to truthful information about the security of their PHI after the breach • Plaintiffs' receipt of unsolicited phone calls from telemarketers and scam artists, without evidence that such calls resulted from the breach • Costs incurred to travel to a different hospital with allegedly better security	• Plaintiffs' lost data has been actually accessed or misused • Plaintiffs with no prior history of identity theft become identity-theft victims shortly after breach • Plaintiffs' personal information had not previously been the subject of another unrelated breach • 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

Factors corporate counsel should consider when assessing litigation risk 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 the organization offer credit monitoring, identity theft insurance, and/or credit repair services?
8. If so, what percentage of impacted consumers availed themselves of the offer?
9. If filed as a class action, is the class representative's claim of identity theft premised on unique facts?

V. Healthcare Data-Breach State and Federal Enforcement

120,221: Number of HIPAA complaints received by OCR since 2003.[161]

990: Number of compliance reviews initiated by OCR.[162]

$4.8 million: Largest fine assessed by OCR.[163]

35%: Percentage of RAs that relate to theft of a laptop or portable device.[164]

The HHS Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules of 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 were required to comply with the HIPAA Breach Notification Rule beginning on September 23, 2009.

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 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.

What corporate counsel should consider when assessing the impact of an OCR investigation:

1. There is an upward trend in enforcement activities and fines.
2. Only a minority of investigations lead to fines and penalties.
3. Cooperation in government-initiated compliance reviews can be key to reducing the risk of a penalty.
4. Preventing unauthorized access to patient information on stolen laptops and portable electronic devices by encrypting the information and requiring passwords will reduce exposure.
5. Fewer than 25 companies have received fines or penalties from OCR.

---

[161] U.S. Dep't of Health and Human Servs., *Enforcement Highlights* (Sept. 30, 2015), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/.
[162] *Ibid.*
[163] U.S. Dep't of Health and Human Servs., *Data Breach Results in $4.8 Million HIPAA Settlements* (May 7, 2014), https://wayback.archive-it.org/3926/20150618190123/http://www.hhs.gov/news/press/2014pres/05/20140507b.html.
[164] The calculations do not include a "Civil Penalty" imposed in 2011 for an entity's failure to cooperate with the investigation, which resulted in a $4.3 million fine. This is the only "Civil Penalty" ever imposed.

W. Healthcare Business Associates

The Health Information Technology for Economic and Clinical Health ("HITECH") Act modified HIPAA by expanding the definition of Business Associates ("BA") and their responsibilities. 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 receive PHI
   - Maintain or store PHI even if they do not or cannot access the PHI
   - Offer personal health records
   - Provide data transmission services if they routinely access the PHI

Pursuant to HITECH and HIPAA, BAs are required to do the following:

1. Designate a security officer.
2. Perform a security risk assessment.
3. Implement administrative, physical, and technical safeguards.
4. Identify and report breaches and security incidents.
5. Develop policies for HIPAA/HITECH compliance program.
6. Impose disciplinary actions for HIPAA/HITECH violations.
7. Have business associate agreements with subcontractors.
8. Maintain documentation for six years.

As mentioned above, HHS's OCR enforces HIPAA and HITECH. OCR identified BAs as one of its top three enforcement priorities in 2016. Under HIPAA and HITECH, BAs are directly liable for compliance and subject to these monetary penalties:

Violation Category	Each Violation	Maximum Penalty per Identical Provision Violated in Calendar Year
Did Not Know	$100-$50,000	$1,500,000
Reasonable Cause	$1,000-$50,000	$1,500,000
Willful Neglect, Corrected	$10,000-$50,000	$1,500,000
Willful Neglect, Uncorrected	$50,000	$1,500,000

Key Considerations for BAs:

1. Determine if the organization is a BA.
2. Designate a person to oversee a HIPAA/HITECH Compliance Program.
3. Identify high risks, *e.g.*, mobile devices, emails, texting, medical devices.
4. Respond timely and effectively to breaches and security incidents.
5. Monitor, audit, and update privacy and security on an ongoing basis.

6. Know the terms of BA Agreements.
7. Prepare a contingency/disaster plan.
8. Maintain adequate cyber insurance.

X. 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 your relationship with your vendors. 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 vendors provide to the company and allow customers to realize the benefits of the arrangement, while mitigating the risk inherent in the vendor relationship.

Corporate counsel should consider the following when evaluating a vendor agreement:

1. What data and information will the organization share with your vendor?
2. Does the organization's vendor agreement require that the vendor use its data only to provide services to the contracting company?
3. Under what terms is the organization's vendor required to keep the data confidential?
4. Is the organization's vendor required to comply with government requests to produce the data?
5. Is the organization's vendor required to keep the data in a logically distinct manner?
6. What laws and industry regulations apply to the company with which the vendor will be required to comply?
7. Under what terms is the organization's vendor required to notify the organization if the vendor is breached?
8. Is the organization's vendor subject to the organization's privacy, cybersecurity, and data retention policies?
9. Does the organization's privacy policy allow the company to share data with a vendor?
10. After the termination or expiration of the vendor agreement, under what terms is the organization's vendor required to return the organization's data?

62%: The percentage of companies that evaluate the security risks of their third-party vendors.[165]

32%: The percentage of companies that require their partners and vendors to comply with their security practices.[166]

28%: The percentage of breaches attributable to a partner or vendor.[167]

[165] 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.
[166] PricewaterhouseCoopers, *PwC Viewpoint on Third Party Risk Management* (Nov. 2013), https://www.pwc.com/us/en/risk-assurance-services/assets/pwc-viewpoint-vendor-risk-management.pdf.
[167] *Ibid*.

11. What right does the organization's vendor have to withhold access to the organization's data or terminate service?
12. What rights does the organization have to audit its vendor's operational practices?
13. Is the vendor required to self-audit?
14. Have the vendor's past audits exposed any vulnerabilities, or has the vendor been breached in the past year?
15. Will the organization's vendor be required to maintain certain levels of insurance during the term of the vendor agreement?

Y. Cloud Computing

$78 billion to $235 billion: The amount companies spent on cloud services in 2011, compared to the projected amount that companies are estimated to spend by 2017.[168]

66%: Percentage of those companies with 100-249 employees that use a cloud service.[169]

64%: Percentage of eShop services that rely on cloud computing.[170]

71%: Percentage of companies that view data security as a concern in moving services to the cloud.

Most companies now use some form of cloud computing. 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 storage is breached.

To minimize data-security risks, companies should evaluate the following as they consider cloud computing:

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 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 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 nature of the data and the processing costs.

[168] IHS, *The Cloud: Redefining the Information, Communication and Technology Industry* (Feb. 2014), http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017.
[169] Franklin Morris, *Infographic: SMB Cloud Adoption Trends in 2014*, (http://www.pcworld.com/article/2685792/infographic-smb-cloud-adoption-trends-in-2014.html
[170] 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.

5. Who is responsible for backing up data?
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 Application Program Interfaces or features, or does it promise to provide future functionality? Depending on the circumstances, schedules can be a useful way to ensure certain necessary functionality remains in the service.
11. Will the network connections between the vendor and the customer provide sufficient bandwidth, 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.
12. Will the use of cloud services conform with any customer's industry-specific needs or regulations?
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?
15. Does the cloud vendor have adequate liability coverage? Although no one wants the agreement to reach that point, it is important to understand the extent to which the provider could absorb a loss that might impact many (or all) of its customers simultaneously.

III. DATA TRANSFERS FROM OTHER COUNTRIES

A. EU-US Safe Harbor Framework and its Validity

The EU Data Protection Directive 95/46/EC (the "Directive") creates the legal framework for the national data-protection laws in each EU member state. The Directive states that personal data may only be transferred to countries outside the EU when an adequate level of protection is guaranteed. Few exemptions apply, and the laws of the United States are not considered by the European Union as providing an adequate level of data protection. As a result, if a company intended to transfer personal information from the EU into the United States traditionally 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; and Binding Corporate Rules.

The EU-US Safe Harbor Framework ("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 covered by the Safe Harbor could no longer rely upon it as a basis of adequacy.

In February of 2016, the European Commission released the text of a new EU-US framework for data transfers called "Privacy Shield." Privacy Shield was designed to replace the invalidated Safe Harbor by imposing stronger obligations on U.S. organizations for protecting the personal data of EU individuals than were afforded under the Safe Harbor. Before Privacy Shield can become a functioning cross-border transfer mechanism, however, it must be reviewed by the EU's Article 29 Working Party (comprised of data protection authorities from each EU member state) and be formally adopted by the EU Commission. As of the writing of this Note, the Working Party had expressed concern that Privacy Shield would not provide adequate protections for personal information transferred to the US, and there is significant uncertainty as to whether the framework would be adopted by the EU Commission.

B. EU Model Clauses

The EU Commission has created model contracts for data transfers (the "Model Contracts") and determined that organizations which use the Model Contracts offer sufficient safeguards for cross-border data transfer as required by the Directive.

The EU Commission has issued three Model Contracts: two for transfers from data controllers to data controllers established outside the EU, and one for a transfer to a data processor outside the EU. Companies should go through the following three steps when using the Model Contracts:

1. National law compliance.
2. Implementation of applicable Model Contract.
3. National law administrative requirements (*e.g.*, notification or registration with the local Data Protection Authority).

C. EU Binding Corporate Rules

Binding Corporate Rules ("BCR") 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. BCR 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:

1. Designate the lead EU data protection authority ("DPA"), *e.g.*, the authority which will be handling the EU co-operation procedure among the other European DPAs.
2. Draft and submit a BCR which meets the safeguards required by the Directive.
3. The lead authority will start the EU cooperation procedure by circulating the draft BCR to the relevant DPA, *e.g.*, of those countries from where entities of the group transfer personal data to entities located outside of the EU.
4. Close the EU cooperation procedure 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.
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.

D. EU General Data-Protection Regulations

The EU General Data Protection Regulation (the "GDPR") was adopted by the EU Parliament last April 14, 2016. The GDPR will replace the EU Data Protection Directive (95/46/EC), which was implemented more than 20 years ago. After a two-year transition period to integrate the new obligations, the Regulation will be directly applicable in all EU Member States in June 2018.

The GDPR's aim is to unify data-protection law within the European Union and increase data subjects' rights. This involves strengthened obligations for companies in terms of compliance, as well as extended powers for Data Protection Authorities ("DPA")

E. Data Transfers from Asia

Data-protection laws have been in place in Europe 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 in the last few years have adopted consolidated data-protection legislation and others are expected to follow.

If an organization operates in Asia or collects personal information about Asian residents its counsel should consider the following:

1. What laws apply to the collection and use of the personal information of individuals?
2. Does the organization 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 does the organization 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 the organization to retain the information in the local jurisdiction?
8. Does the organization have to appoint a data-protection officer in the local jurisdiction?
9. Does the organization have to comply with local data-protection laws if it is only processing personal information?
10. What are the penalties for non-compliance with any applicable data-protection laws?

8: The number of Asian countries that have enacted consolidated data-protection legislation.

4: The number of Asian countries that require most companies to appoint a data-protection officer.

3: The number of Asian countries that have enacted data-breach notification legislation.

4: The number of additional Asian countries that highly recommend that companies issue notices in the event of a data breach.

5: The number of Asian countries that have restrictions on the cross-border transfer of data.

GLOSSARY

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

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

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 into 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

