EMPLOYMENT AND ECONOMIC DEVELOPMENT

GRAY PLANT MOOTY 150

A Legal Guide To PRIVACY AND DATA SECURITY

2016

A Collaborative Effort

Minnesota Department of Employment and Economic Development

Gray Plant Mooty

A Legal Guide To
PRIVACY AND DATA SECURITY

is available without charge from the Minnesota Department of Employment and Economic Development, Small Business Assistance Office, 1st National Bank Building, 332 Minnesota Street, Suite E-200, St. Paul, MN 55101-1351.
Telephone: (651) 556-8425 or (800) 310-8323
Fax: (651) 296-5287 | Email: deed.mnsbao@state.mn.us
Website: http://mn.gov/deed/business/help/sbao/
This guide is also available from Gray Plant Mooty, 500 IDS Center, 80 South Eighth Street, Minneapolis, MN 55402
Telephone: (612) 632-3000

Upon request, this publication can be made available in alternative formats by contacting (651) 259-7476.

The Minnesota Department of Employment and Economic Development is an equal opportunity employer and service provider.

A Legal Guide To PRIVACY AND DATA SECURITY

March 2016

Primary Author: Michael R. Cohen
CIPP/US, CIPP/E

A Collaborative Effort

Minnesota Department of Employment and Economic Development
Gray Plant Mooty

Copyright © 2016 Minnesota Department of Employment and Economic Development and Gray Plant Mooty

ISBN 1-888404-71-X

TABLE OF CONTENTS

DISCLAIMER v

INTRODUCTION.....vi

LEGAL BASIS FOR A RIGHT TO PRIVACY.....1

FEDERAL LAWS GOVERNING DATA PRIVACY AND SECURITY 3

Welcome to federal data privacy law and the world of acronyms 3

The Use and Disclosure of Financial Information 4

Gramm-Leach-Bliley Act (GLBA) 4

Fair Credit Reporting Act (FCRA) and Fair Accurate Credit Transactions Act (FACTA) 10

Use and Disclosure of Medical Information 15

The Health Insurance Portability and Accountability Act (HIPAA) 15

Medical Research - The Common Rule 20

Federal Trade Commission Act (FTC Act) 20

FTC Online Behavioral Advertising Principles 30

Children's Online Privacy And Protection Act (COPPA).....31

Controlling The Assault Of Non-Solicited Pornography And Marketing Act (CAN-SPAM) 36

The Telephone Consumer Protection Act (TCPA) [47 U.S.C. § 227].....38

Telemarketing and Consumer Fraud and Abuse Prevention Act [15 U.S.C. §§ 6101-6108].....43
Deceptive Mail Prevention and Enforcement Act (DMPEA)....44
Junk Fax Prevention Act (JFPA) 44
Computer Fraud and Abuse Act (CFAA) [18 U.S.C. § 1030 (c)] 45
Electronic Communications Privacy Act (ECPA) [18 U.S.C. §§ 2510-3127] 46
Federal Laws Related To Social Security Numbers 47
The Drivers Privacy Protection Act (DPPA) [18 U.S.C. §§ 2721-2725] 48
Video Privacy Protection Act (VPPA) [18 U.S.C. § 2710] 49
Other Federal Privacy Laws 49
The National Institute Of Standards And Technology (NIST) Cybersecurity Framework 52
Proposed Federal Legislation 53

PRIVACY AND THE EMPLOYMENT RELATIONSHIP 57
Discrimination Laws 58
Protected Activity Laws 59
Applicant Screening Laws 63
Employee Privacy Considerations 65
Federal Laws Applicable To Electronic Communications and Data 68
The Electronic Communications Privacy Act (ECPA or the "Wiretap Act") 69
The Stored Communications Act (SCA) [18 U.S.C. § 2701, et seq.] 69
The Computer Fraud and Abuse Act (CFAA) [18 U.S.C. § 1030, et seq.] 70

References and Recommendations 71
Safeguarding Confidential and Proprietary Information ..71
Employer Policies and Practices 72

STATE DATA PRIVACY AND SECURITY LAWS 75
Minnesota Data Privacy and Security Laws 76
Minn. Stat. § 325M.01 Internet Service Providers ..76
Minn. Stat. § 609.527 Identity Theft 76
Minn. Stat. § 325E.61 Data Breach Notification 76
Minn. Stat. § 13.055 Data Breach Notification 76
(Government Agencies) 76
Minn. Stat. § 13.0 Minnesota Government Data Practices Act 77
Minn. Stat. § 13.15 Government Websites 77
Minn. Stat. § 325E.64 Plastic Card Security Act 77
Minn. Stat. § 325E.59 Use of Social Security Numbers 77
Minn. Stat. § 626A.02 Wiretap law 77
Internet Service Providers [Minn. Stat. § 325M.01] 77
California 106
Massachusetts 109
Other State Privacy and Breach Notification Laws 110
State Breach Notification Laws 110
State Data Protection and Security Laws 112

GLOBAL PRIVACY AND DATA SECURITY LAW 113
EU 1995 Data Directive 114
Transfer of Personal Data Outside Of The European Union 120
Prior US-EU Safe Harbor 121
Model Contracts 124
Binding Corporate Rules 124

CANADA 127
Personal Information Protection and Electronic Documents Act (PIPEDA) 127
Canada Anti-Spam Law [SC 2010,C23] 129

BEST PRACTICES 131
Key Questions Every Business Should Ask Related To Data Privacy and Security 131
Establish a Compliance Program 135
Customized Program 135
Security Incident and Data Breach Plan 135
Mitigating Risk By Contract 139
Insurance 140
Physical Safeguards/Office Design 141
Storage And Maintenance Of Electronic Data 142
Document Retention - Storage And Maintenance Of Hard Copies 142
Technical Safeguards 143
Encryption, Encryption, Encryption 144
Limit Access 144
Limit Data Collected 145
Remote Access 145
Administrative Safeguards 146

FINAL THOUGHTS - WHAT IS NEXT? 149

PRIVACY LAW TIMELINE 155

SOURCES OF INFORMATION ON DATA PRIVACY AND SECURITY 159
Other government sites and publications that provide privacy related information. 160
Other Useful Websites 161
Selected Books, Articles and Treatises on Privacy 162

DISCLAIMER

This Guide is designed to alert businesses to legal issues related to privacy and data security. It is intended as a guide and not as a definitive source to answer your legal and business questions. It should not be relied upon for specific legal advice. Legal and other professional counsel should be consulted. Gray Plant Mooty and the Small Business Assistance Office cannot and do not assume responsibility for decisions made based upon the information provided in this Guide.

INTRODUCTION

Google glasses, drones the size of a butterfly, secure microchips replacing magnetic stripes on credit cards, sensors the size of a grain of sand swallowed by patients and that transmit data directly to the physician, automobiles that drive themselves, "Big Data," the so-called 'Internet of Things" – all of these are already pushing the limits of privacy advocates, regulators, consumers, lawyers and the businesses adopting these new technologies.

In 1890 Samuel Warren and Louis Brandeis wrote in their seminal Harvard law review article entitled "The Right to Privacy" that privacy is the "right to be left alone". Widely regarded as the first publication in the United States to advocate for a legal right to privacy this article has been the inspiration for many American jurists considering the legal right to privacy. Brandeis and Warren wrote this article in response to the then new intrusive technology known as photography and the sensational and scandalous articles being written by journalists. [4 Harvard L. R. 193 (Dec. 15, 1890)]

In 2012 Supreme Court Justice Sotomayor wrote in her opinion in *United States v. Jones* 132 S. Ct 945,957 (2012),"[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks…"

This was followed by a unanimous Supreme Court ruling in 2014 that police must obtain a warrant to search the vast amount of information on a suspect's cellphone. In the opinion, Chief Justice John Robert states that cellphones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California* 573 U.S. (2014).

On November 2, 2015 the United States Supreme Court heard oral arguments in ***Spokeo v. Robins*** (No. 13-1339), a case that may have a significant impact on privacy litigation. The question at issue is whether or not a person who has had their personal information disclosed online, with no further harm, has a right to sue. If the Court finds no right to sue it will be a major blow to privacy advocates. If however, the Court determines that Mr. Robins has the right to sue, the plaintiff's bar may rejoice as class action lawsuits are filed against companies which handle personal information online.

In 2016 the FBI and Apple argued over the FBI demand that Apple unlock the security features of an iPhone that belonged to a terrorist. A judge in California issued an order requiring Apple to assist the FBI while a judge in the Eastern District of New York denied an FBI motion to require Apple to unlock an iPhone belonging to a meth dealer. This issue of privacy vs. government access will likely continue to be debated in Congress and the courts.

So how far have we come from a time when cameras alone were seen as intrusive to the current concerns of privacy advocates over iPhone encryption, drones and Google glasses?

Minnesota businesses of all sizes collect, store, and share personal information about individuals. While new technology and access to information allows for greater innovation and delivery of products and services, it also creates a challenge. How does a business optimize the information available and remain in compliance with the

evolving and ever-changing legal landscape? How does a business not compromise consumer privacy as more and more information is shared and collected? What about privacy rights of employees and prospective employees?

The scope and type of personal data collected by businesses continue to grow as does the ease of gathering and storing the data. A small thumb drive containing all of a business' trade secrets and employee information can be easily removed and transported in a person's pocket. New technology allows for the tracking of consumer preferences and information, including their exact location, making it possible to do real-time targeted marketing.

The aggregation of consumer data by data brokers is increasingly being monetized and used by businesses as even more detailed information about consumers becomes available. Big data is viewed as both a savior in medical research and a menace to privacy. The so-called "Internet of Things" allows for household appliances and cars to collect and share personal consumer data like never before.

High profile data breach incidents such as those experienced by Target and other national retailers exemplify the need for businesses to take a serious look at data privacy and security issues and how they fit within their business operations. Potential breaches are not simply the result of lax computer systems and poor data security. A business can be just as liable for a data breach by leaving job applications in a public dumpster or mailing medical information to the wrong patient due to a printing error.

While it is impossible for a business to become an expert in all of the laws related to data privacy and security, it is our hope that this Guide will at least provide a basic understanding of the wide variety of laws and how those laws may impact your business.

This Guide was prepared for Minnesota-based businesses. Data, however, crosses state and national borders, and thanks to the internet, most businesses have now become global. It is no longer safe to just consider Minnesota and U.S. laws and federal regulations when it comes to data privacy and security. For this reason we have included some basic information on data privacy laws outside of the United States.

New Developments. This is the second version of the Guide and covers some of the key privacy and data security developments since the first version was published in 2014. The most significant changes took place outside the US but continue to shape the privacy practices of online companies with a global reach. There were two noteworthy legal developments. First was the invalidation of the EU-US Safe Harbor Framework relied upon by thousands of US companies to support cross-border data transfers. Second, was the the proposed new EU General Data Protection Regulation (GDPR).

Twenty years after passing the EU Data Directive, and following years of negotiation, agreement was finally reached in December 2015 on the GDPR. While the GDPR does not take effect until 2018 businesses should consider how they will comply with this new law. In 2015 the EU also invalidated the EU-U.S. Safe Harbor Agreement, a long standing data transfer mechanism. On February 2, 2016 the European Commission and U.S. Department of Commerce announced an agreement in principle (not yet fully ratified and approved) for a new data transfer framework, the EU-U.S. Privacy Shield, to replace the invalidated Safe Harbor Agreement. The Privacy Shield includes a new federal ombudsman to oversee intelligence access to EU citizen data, a multi-step complaint resolution process for EU citizens, and a number of other new provisions. President Obama signed into law the Judicial Redress Act on February 24, 2016. The Act grants non-U.S. citizens certain rights, including a private right of action for alleged privacy violations that occur in the U.S. The passing of this Act was an important step towards approval of the Privacy

Shield that replaces the EU-US Safe Harbor and allows the transfer of personal information from the EU to the USA. Both the GDPR and Privacy Shield are covered in this new version of this Guide.

The FTC continues to be the grand enforcer of data privacy and security rights in the US. One company ***Lifelock, Inc***. agreed to pay $113 million following an FTC action based on data privacy and security claims. This Guide covers two challenges by *Wyndham* and ***LabMD*** to the FTC'S authority as the principal federal privacy and data security regulator. (See pages 27-29).

At the end of this Guide we offer best practices and a list of sources and references for further information on these issues. In this version we have also added a Privacy Law Timeline.

We welcome your comments on this Guide and any suggestions you might have for data privacy and security issues to cover in future editions.

Finally, I would like to thank George Meinz, Jesse Berg, Meghann Kantke, Maisa Frank, Leah Leyendecker and members of the Privacy and Security Group at Gray Plant Mooty and summer associates Lynn Ling and Pa Nhia Vang for their support in preparing **A Legal Guide to Privacy and Data Security**.

Michael R. Cohen, CIPP/US, CIPP/E

Gray Plant Mooty

March 2016

LEGAL BASIS FOR A RIGHT TO PRIVACY

Sources of privacy law include constitutional law, tort law, contract law, federal and state laws and regulations, and foreign laws.

Constitutional. There is no explicit reference to privacy as a right in the United States Constitution. The United States Supreme Court has however held in several cases that there exists a right to privacy or at least a "reasonable expectation of privacy" as implied in the First, Third, Fourth, Ninth, and Fourteenth amendments. [See *Olmstead v. United States*, 277 U.S. 438 (1928), *Katz v. United States*, 389 U.S. 347 (1967), *Griswold v. Connecticut*, 381 U.S. 479 (1965), *Roe v. Wade*, 410 U.S. 113 (1973), *Whalen v. Roe*, 429 U.S. 589 (1977).]

In *United States v. Jones*, 132 S. Ct 945 (2012) the installation of a GPS device by law enforcement in a car without a warrant was found to constitute a search under the Fourth Amendment because it represented a trespass on a person's property. In concurring opinions it was noted that the use of long term surveillance violates a "reasonable expectation of privacy." This was followed by *Riley v. California*, 573 U.S. (2014) where the Supreme Court ruled that the contents of mobile devices are protected by the Fourth Amendment's warrant requirement.

There are now explicit data privacy provisions in the constitutions of at least ten states including Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington.

There is no explicit data privacy provision in the Minnesota State Constitution.

Tort law. The tort of invasion of privacy has been identified and described in the Restatement (Second) of Torts § 652(1977) ("Restatement") and includes 1) intrusion upon seclusion, 2) public disclosure of private facts, 3) appropriation of name or likeness, and 4) publicly placing a person in false light. Other torts and causes of action related to privacy may include defamation, assault and battery, trespass, breach of confidentiality, intentional infliction of emotional distress, negligence, and right of publicity.

In a Minnesota case, *Lake v. Wal-Mart Stores, Inc.* 582 N.W.2d 231 (Minn. Sup. Ct. 1998) the Minnesota Supreme Court recognized a right to privacy in Minnesota, and adopted the Restatement definitions for three of the Restatement torts- intrusion upon seclusion, appropriation, and publication of private facts. [See also *Bodah v. Lakeville Motor Express, Inc.,* 663 N.W.2d 550 (Minn. 2003) and the common law of privacy discussed on pages 66-67.]

Contracts. Confidentiality agreements and related contracts may have specific provisions restricting the right to use or disclose information and are generally governed by state law. Terms of Use and Privacy Policies that appear on websites may also be enforceable. Business Associate agreements may be required under the Health Insurance Portability and Accountability Act ("HIPAA"). See discussion of Business Associate agreements on page 18.] Commercial agreements now also include provisions on handling personal information and data security [See pages 139-140 for Mitigating Risk By Contract.] Social media platforms such as Facebook have terms of use and privacy policies that include provisions regarding the sharing of personal information. [See Minnesota Department of Employment and Economic Development and Gray Plant Mooty publication *A Legal Guide to the Use of Social Media in the Workplace. July 2013*.]

FEDERAL LAWS GOVERNING DATA PRIVACY AND SECURITY

HIPAA, COPPA, CAN-SPAM, ECPA, GLBA, TCPA, FCRA, FACTA, CFAA….

> **Welcome to federal data privacy law and the world of acronyms.**

There is no single federal law governing data privacy and security in the United States. There are, however, many different requirements for implementing data security procedures or protecting personal data that can be found in a host of federal laws.

Most of the federal laws that cover data privacy and security obligations for businesses are specific to certain industries and types of information such as:

Financial information. The Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA) and Fair and Accurate Act Credit Transactions Act (FACTA)

Healthcare and medical information. The Health Insurance Portability and Accountability Act (HIPAA)

Other federal laws cover specific activities that may use personal information such as:

Telemarketing. (including text messages used for marketing purposes). The Telephone Consumer Protection Act (TCPA)

Commercial email. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)

The online collection, use, and disclosure of information from children. The Children's Online Privacy and Protection Act (COPPA).

Other key federal laws that are discussed in this section of the Guide include the Telemarketing and Consumer Fraud and Abuse Prevention Act, Deceptive Mail Prevention and Enforcement Act, Junk Fax Prevention Act, the Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (CFAA), Drivers Privacy Protection Act, (DPPA), Video Privacy Protection Act (VPPA) and other "safeguard" regulations imposed by the Federal Trade Commission Act as necessary to regulate unfair and deceptive trade practices.

At the end of this section we have listed some other federal laws that govern privacy rights but that may be more focused on government obligations and not the private sector.

The absence of a single comprehensive federal data privacy and security law in the United States forces a business to become familiar with a variety of federal and state laws that may impact their operations.

The Use and Disclosure of Financial Information

Gramm-Leach-Bliley Act (GLBA)

Among other things, the Gramm-Leach-Bliley Act (GLBA) regulates the collection, use, protection, and disclosure of nonpublic personal

information by financial institutions. With respect to banks and credit unions, the Consumer Financial Protection Bureau (CFPB), the Office of the Comptroller of Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) are the primary regulators and enforcers of the GLBA. The Federal Trade Commission (FTC) is the primary enforcer of the GLBA for all financial institutions other than those banking entities.

The definition of "financial institution" is quite broad and includes businesses that are significantly engaged in providing financial products or services such as check-cashing businesses, mortgage or nonbank lenders, loan brokers, financial and investment advisors, real estate service providers, insurance, debt collectors, and businesses providing retail financing to consumers. A Minnesota business can also be covered under these laws if they collect and maintain financial information for companies that fall directly under these laws.

Purpose. The purpose of the GLBA is to restrict the sharing of customers' financial information by requiring financial institutions to give customers notice of their privacy practices, providing a right of a consumer to opt-out of certain types of sharing, and requiring financial institutions to implement appropriate safeguards to protect their customers' "nonpublic personal information."

Definition of Nonpublic Personal Information. The privacy provisions of the GLBA apply only to "personally identifiable financial information." 15 U.S.C. § 6809(4).

Sharing of Information with Affiliated Companies. The GLBA does not prohibit the sharing of nonpublic personal information with affiliates. However, the Fair Credit Reporting Act (FCRA) does limit the sharing of certain financial information with affiliates for marketing purposes and requires that consumers be given notice of the affiliate sharing and the right to opt-out. 15 U.S.C. § 1681s-3.

Sharing of Information with Third Parties. Nonpublic personal information can be shared with nonaffiliated companies only if the individual is first given a right to opt-out of the sharing and does not do so or if the consumer consents to the sharing. 15 U.S.C. § 6802(b). There are a number of exceptions to the requirement of providing a right to opt-out for otherwise normal business activities and legal requirements such as responding to subpoenas, or delivering the information to service providers or consumer reporting agencies. The financial institution may also be required to have a contract in place with the third party that requires the party to maintain the information as confidential.

Restrictions. Financial Institutions cannot disclose account numbers or credit card numbers for direct marketing purposes. 15 U.S.C. §6802(d).

Privacy Notices. Financial institutions must provide a written notice to customers of their privacy policies. 15 U.S.C. § 6803(a).

Security. Financial institutions must develop, implement, and maintain a comprehensive information security program. 16 C.F.R. § 314.3(a).

Preemption. The GLBA does not preempt state laws that may provide greater privacy protection to consumers. 15 U.S.C. § 6807(b).

GLBA Privacy and Safeguards Rules. The GLBA regulations consist of a "Privacy Rule" (requiring disclosure to consumers about the use and dissemination of their financial information) and a "Safeguards Rule" (requiring safeguarding any financial information obtained from an individual that is not publicly available). Subject to certain exceptions, financial institutions are also prohibited from disclosing any "nonpublic personal information" to unrelated third parties without first giving customers the ability to opt-out of the sharing.

Consumer Distinguished from Customer. Nonpublic personal information under GLBA is any "personally identifiable financial information" that is not publicly available and is capable of personally identifying a consumer or customer. A consumer is anyone who has obtained a financial product or service but does not necessarily have an ongoing relationship with the financial institution and a customer is a person with an ongoing relationship with the financial institution.

GLBA Requirements. The GLBA requires the financial institution to 1) notify its customers about its information-sharing practices and provide customers with a right to opt out if they do not want their information shared with certain unaffiliated third parties (GLBA Financial Privacy Rule), and 2) implement a risk - based written security program to protect nonpublic personal information from unauthorized disclosure (GLBA Safeguards Rule), and 3) provide notice of its information sharing to consumers in some situations.

GLBA Notice and Disclosure Requirements. A customer is entitled to receive the financial institution's privacy notice both when the relationship is created and annually thereafter. A customer is entitled to receive the financial institution's privacy notice if the financial institution intends to share the customer's nonpublic personal information with certain third parties. The privacy notice itself must be a clear, conspicuous, and accurate statement of the financial institution's privacy practices. It must state 1) the categories of information that the financial institution collects and discloses, 2) the categories of affiliated and nonaffiliated entities with which it shares information, 3) that the consumer or customer has the right to opt out of some disclosures, and 4) how the consumer or customer can opt out (if an opt-out right is available).

GLBA Consent Requirements. There are no requirements for affirmative consent from a customer or consumer but a financial institution is required at the time of setting up the customer

relationship and annually thereafter to 1) notify customers and consumers of the institution's privacy policy and practices, and 2) provide the individual with "reasonable means" to opt out of certain uses and disclosures of the individual's non-public personal information. Consent can be obtained through written, oral or electronic means.

No Opt-Out Required. A financial institution does not need to provide an opt-out right to the individual in certain defined circumstances, including when nonpublic personal information is shared 1) for the purpose of administering or enforcing a transaction that a customer requests or authorizes, or 2) with outside companies that provide essential services to the financial institution, such as data processing or servicing accounts, if certain conditions are met (like contractually binding the outside company to protect the confidentiality and security of the data).

GLBA Privacy Rule. Under the GLBA Privacy Rule, financial institutions are restricted as to when they may disclose consumer personal information to nonaffiliated third parties. Financial institutions must provide "Privacy Notices" to their customers about their information-sharing practices. Subject to certain exceptions, customers may opt-out if they do not want their information shared with nonaffiliated third parties. The form of these notices may vary based on the relationship with the consumer and the data sharing practices of the business. The Privacy Rule includes several model "safe harbor" notices that can be used by any company to describe their privacy practices and provide the necessary opt-out for sharing of certain information.

GLBA Safeguards Rule. The GLBA Safeguards Rule requires financial institutions, or those handling financial information, to have a written information security plan that describes their program to protect customer information. The plan must be appropriate for the size, scope of activities, and sensitivity of the customer information collected by the business.

The plan required by the Safeguard Rule requires the business to 1) designate one or more employees to coordinate an information security program; 2) identify and assess the risks to customer information in each relevant area of operation, and assess the effectiveness of the current safeguards; 3) develop a plan for safeguarding customer information, and regularly monitor and test the safeguards program; 4) exercise due diligence in selecting service providers (third-party vendors) and require them to implement safeguards; and 5) evaluate and adjust the program as needed.

Examples of such safeguards that can help protect against unauthorized access to, or use of, nonpublic personal information of individuals include 1) data encryption; 2) authentication mechanisms; 3) background checks; and 4) frequent monitoring and testing of information security protocols and systems.

Both the GLBA Privacy and Safeguard Rules require ongoing monitoring and changes. Those responsible in a business for GLBA compliance should periodically update the written information security plan as necessary to keep up with any changes in the law, as well as potential data security threats, or its own business practices.

GLBA Data Breach Notification Requirements. GLBA does not include an explicit data breach notification requirement. Using their authority under the GLBA, the federal bank regulatory agencies issued an Interagency Guidance that requires financial institutions to adopt policies and procedures regarding unauthorized access to customer information. This includes notifying both the regulator and the customer when there has been an unauthorized access to "sensitive customer information." Sensitive customer information generally includes a customer's name, address, or telephone number combined with one or more of the following items of information about the customer: 1) social security number, 2) driver's license

number, 3) account number, 4) credit or debit card number, or 5) a personal identification number or password that would permit access to the customer's account.

GLBA Enforcement. GLBA is enforced by eight federal regulatory agencies, including the FTC and the federal banking agencies, as well as state insurance regulators. **GLBA does not include a right for individuals to bring private actions.**

Potential Liability. GLBA has severe civil and criminal penalties for noncompliance including fines and imprisonment. If a financial institution violates GLBA the institution may be subject to a civil penalty of up to $100,000 for each violation. Officers and directors of the institution may be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation. Additionally, the institution and its officers and directors may be subject to criminal fines and imprisonment of up to five years. Criminal penalties of up to ten years' imprisonment and fines of up to $500,000 (for an individual) or $1 million (for a company), are possible if the acts are committed or attempted while violating another U.S. law, or as part of a pattern of illegal activity involving more than $100,000 in a year.

Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA)

The Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act (FACTA) is related to the GLBA and limits how consumer reports and credit card account numbers can be used and disclosed. FCRA applies to businesses that compile "consumer reports" as well as those who use such reports (lenders and employers) or those who provide consumer credit information to credit reporting agencies (lenders, creditors, and credit card companies).

What is a Consumer Report? A consumer report is any communication issued by a consumer reporting agency that is used to evaluate a consumer's eligibility for credit or insurance that relates to a consumer's creditworthiness, credit history, credit capacity, character, or general reputation.

Purpose. Companies falling under these laws are required to implement programs to help mitigate the risk of identity theft and unauthorized access to consumer financial credit reports. FCRA requires companies that use credit reports to give consumers notice when their report is investigated or used to deny an application for credit or employment.

Employment. A business that uses information obtained from consumer reporting agencies for employment purposes, including background checks, must comply with FCRA by 1) obtaining consent of the person to conduct background check using a consent form required by FCRA, 2) notifying the person if any adverse action is taken based on information in the report, and 3) identifying the consumer reporting agency so that the accuracy and completeness of the report can be challenged by the person.

Credit Report. FACTA allows consumers to receive upon request a free credit report once per year from the consumer credit reporting company and, in appropriate circumstances, to place fraud alerts on their credit histories to reduce identity theft.

Credit Card Numbers. Businesses are also (with some exceptions) prohibited from printing more than five digits of a consumer's credit card number on receipts provided to the cardholder at the point of sale.

Consumer Access. FACTA gives consumers access to their credit report, and in some instances, their credit score, and requires the business to give consumers (or employees) notice of how their credit score was used in developing the interest rates or adverse terms offered to consumers.

FACTA Requirements. Consumer reporting agencies and any other businesses that use consumer reports are required to adopt procedures for properly disposing of consumer report information (the FACTA Disposal Rule). Companies are prohibited from using certain credit information received from an affiliate to market goods or services to a consumer unless the consumer is given notice of the sharing, a reasonable opportunity to opt-out, and a simple and reasonable method for opting-out (the FTC Affiliate Sharing Rule)

Identity Theft (the FACTA Red Flags Rule). The so-called Red Flags Rule required by FACTA and issued jointly by the FTC and the federal banking agencies requires "financial institutions" and "creditors" with "covered accounts", as defined in the Red Flags Rule to develop and implement written programs that can help to reduce identity theft. These rules may also apply to businesses that offer home or personal services on a recurring basis, such as cleaning services, lawn services or personal care services, where the services are provided and the customer is billed later. All companies covered by the rules are required to establish an Identity Theft Prevention Program (much like the Safeguard Rule under the GLBA) to detect, prevent, and mitigate identity theft. Companies subject to the Red Flags Rule are required to establish and implement a program appropriate for the size of their business and the type of information stored in their systems.

These written programs are supposed to identify the relevant "red flags" of identity theft including: 1) unusual account activity, 2) fraud alerts on a consumer report, and 3) attempted use of suspicious account application documents.

More information on the Red Flags Rule and how to implement an appropriate identity theft program is available from the FTC website.

Consumer Financial Protection Bureau. The Consumer Financial Protection Bureau (CFPB), a relatively new federal agency created under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, has primary rulemaking authority for the FCRA as well as the Electronic Funds Transfer Act, the Fair Debt Collection Practices Act, and certain sections of GLBA. The CFPB is an independent agency within the Federal Reserve System. Among the rules adopted by the CFPB are new requirements regarding the use of consumer reports by employers when conducting background checks on employees or job applicants.

Enforcement. The FTC retains rulemaking authority regarding the FACTA Disposal Rule, Red Flags Rule, and GLBA Safeguards Rule. The FTC can also carry out certain investigations and enforce consumer protection laws with regard to nonbank financial institutions that are outside the enforcement authority of the CFPB and the banking regulators.

Civil Liability. Any person that negligently violates the FCRA may be liable for the actual damages incurred by the consumer together with reasonable attorneys' fees. 15 U.S.C. § 1681o. Any person that willfully violates the FCRA may be liable to the consumer for any actual damages sustained by the consumer or statutory damages of not less than $100 and not more than $1000, punitive damages, and attorneys' fees and costs. 15 U.S.C. § 1681n. Additionally, the FTC can impose administrative penalties under the Federal Trade Commission Act.

FTC Enforcement Actions Under FCRA. A data broker, Spokeo, marketed consumer profiles to employers. Spokeo paid $800,000 to settle the charges after the FTC rejected their claim that they were not a consumer reporting agency and therefore not covered by FCRA. According to the FTC, Spokeo sold personal profiles that it had assembled, including information gleaned from social media, to HR, recruiting, and screening businesses as information

they could then use in deciding whether or not to interview or hire a candidate. [See *U.S. v. Spokeo, Inc.* No. 2:12-cv-05001 (C.D.Cal. 2012).]

Telecheck Services, Inc., one of the largest check authorization service companies, agreed to pay $3.5 million and to alter their business practices as necessary to settle FTC charges that it violated FCRA. [See *U.S. v. Telecheck Services, Inc. et al.*, No. 1:14-cv-00062 2014).] This followed an earlier FTC settlement with Certegy Check Services, Inc., another check authorization company for $3.5 million based on similar charges of FCRA violations. [See *U.S. v. Certegy Check Services, Inc.*, No. 1:13-cv-01247 (D.C. 2014).] [For other FTC enforcement actions see pages 24-26.]

Credit Card Data and the Payment Card Industry Data Security Standards ("PCI-DSS"). In addition to the federal laws discussed above and certain state laws, [See Minn. Stat. § 325E.64 discussed on pages 96-98] businesses handling credit card data are self-regulated through the Payment Card Industry (PCI) Security Standards Council. The Council has developed the comprehensive Payment Card Industry Data Security Standards (PCI-DSS) followed by merchants and "all entities that store, process or transmit cardholder data." PCI-DSS requires the installation and maintenance of firewalls, system passwords, encryption of cardholder data across open or public networks, use of anti-virus software, employee access restrictions, physical access restrictions, development of a credit card specific security policy, and restricts the retention of cardholder data. These standards are mandatory for any businesses handling credit card data. Larger merchants may be required to pass regular external security assessments and be subject to frequent scans to assess technical vulnerabilities. Failure to comply with PCI-DSS can result in significant penalties in the event of a data breach.

Use and Disclosure of Medical Information

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA does not just apply to health care providers. HIPAA governs ***individually identifiable health information.*** It applies broadly to health plans, health care providers, data processors, pharmacies, and other entities that come into contact with this information, including so-called "business associates" that do not deliver health care directly but provide services to the "covered entity."

The Department of Health and Human Services (HHS) issued regulations for the privacy and security of medical information otherwise known as the "Privacy Rule" and the "Security Rule."

Privacy Rule. Standards for the privacy of individually identifiable health information are set forth in the HIPAA Privacy Rule. The Privacy Rule refers to this health information as "protected health information" or PHI, which includes information related to the past, present, or future physical or mental health or condition, the provision of health care to an individual, or the past, present or future payment for such health care which is created or received by a covered entity. The Privacy Rule limits any entity covered under HIPAA to disclosure of PHI to: (1) the individual; (2) for use in treatment, payment, or health care operations; (3) for certain purposes where an individual has been given an opportunity to opt-out; (4) when required by law or other strong public interest policy; or 5) for other purposes pursuant to an "authorization" that meets certain requirements spelled out in the Privacy Rule.

Security Rule. Security standards for the protection of electronic PHI are set forth in the HIPAA Security Rule.

Prior to passage of the Health Information Technology for Economic and Clinical Act (HITECH Act) business associates were liable only

indirectly for their violations of the commitments set forth in a business associate agreement with a covered entity. HITECH obligates business associates to comply with all of the HIPAA Security Rule and many parts of the HIPAA Privacy Rule. Violations of HIPAA requirements by business associates expose those organizations to enforcement actions by the HHS Office for Civil Rights. HITECH also changed many of the substantive requirements of the Privacy Rule, including adopting more restrictive guidelines to govern marketing activities using PHI. In addition, HITECH gave HIPAA enforcement authority to state attorneys general. The HITECH Act also created an obligation for covered entities, their business associates, and in some cases vendors used by covered entities, to notify individuals when the security or privacy of their PHI had been compromised. [See breach notification on page 18-19.]

Application. HIPAA applies to "covered entities" and "business associates" as defined in the regulation 45 C.F.R. § 160.103. It applies to those who transmit PHI electronically as part of certain "standard transactions." This means that most health care providers who deal with insurance such as doctors, hospitals, insurance companies, and pharmacies are subject to HIPAA. Business associates that create, receive, maintain, or transmit PHI on behalf of covered entities (and subcontractors that engage in similar types of activities on behalf of business associates) are also directly subject to the HIPAA Security Rule and parts of the Privacy Rule.

Scope. HIPAA is limited to covered entities over which the United States government has enforcement authority. However, certain business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of the United States.

Data Covered. Protected health information or PHI is individually identifiable health information that is maintained or transmitted by a covered entity or business associate.

General Obligations. HIPAA regulates the use and disclosure of PHI and the collection, use, maintenance, or transmission of electronic PHI, and requires that covered entities provide a notice of privacy practices. In addition, HIPAA establishes certain "individual rights" (such as the right to access PHI, or request an amendment of PHI, in a designated record set).

HIPAA Requirements. HIPAA requires (with some exceptions) that covered entities: 1) use, request, and disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request (HIPAA Privacy Rule); 2) implement data security procedures, protocols, and policies at administrative, technical, physical, and organizational levels to protect electronic PHI (HIPAA Security Rule); 3) comply with uniform standards created for certain electronic transactions (HIPAA Transactions Rule); and 4) notify individuals if there is a security breach (and requires that business associates of HIPAA-covered entities notify these covered entities in the event of a security breach).

Notice and Disclosure Requirements. The HIPAA Privacy Rule requires each covered entity provide notice to individuals of its privacy practices and of the individuals' rights under HIPAA, generally on the first visit for treatment. The Privacy Rule sets out specific requirements for the contents and method of the notice.

Individual Access to Collected Data. Under HIPAA, individuals have the right (with some exceptions) to: 1) request access to their PHI, 2) make corrections to their PHI, and 3) request an accounting of the manner in which their PHI has been used and disclosed.

Restrictions on Sharing Data with Third Parties. Unless the HIPAA Privacy Rule establishes regulatory permission for a covered entity to use or disclose PHI for a specific purpose, either generally (such as treatment or payment) or subject to a particular process (such as disclosures to law enforcement or judicial or administrative proceedings), the Privacy Rule requires covered

entities to obtain "authorization" from the individual. The Privacy Rule outlines specific requirements governing procedural and substantive requirements for obtaining authorization.

Business Associate Agreements. Covered entities are permitted to disclose PHI to business associates if the parties enter into an agreement that generally requires the business associate to: 1) use the information only for the purposes required or permitted by the covered entity, 2) safeguard the information from misuse, and 3) help the covered entity to comply with its duties under the Privacy Rule. In addition, the Privacy Rule and Security Rule set forth very specific requirements for what needs to be included in these business associate agreements. When a covered entity has knowledge that its business associate has materially breached or violated the applicable agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, to terminate the contract. If termination of the agreement is not feasible, a covered entity must report the problem to the HHS Office for Civil Rights.

Data Security Requirements. The HIPAA Security Rule requires covered entities to implement data protection policies and reasonable security procedures, including: 1) administrative safeguards, which generally include administrative activities such as assigning responsibility for the security program to the appropriate individuals or requiring security training for employees, 2) physical safeguards, which include physical mechanisms required to protect electronic systems, such as limiting access to electronic PHI to authorized individuals, and 3) technical safeguards, which include automated processes designed to protect data and control access, such as using authentication controls and encryption technology.

Breach Notification Requirements. HHS also requires covered entities to notify individuals when their unsecured PHI has been breached. This change resulted from the HITECH Act enacted in 2009. HITECH defines a "breach" to be the acquisition, access, use

or disclosure of PHI in a manner that is not permitted by the Privacy Rule. Unsecured PHI is PHI that is not secured in accordance with certain National Institute of Standards and Technology (NIST) standards recognized by the Secretary of HHS. [See discussion of NIST on pages 52-53.] Affected individuals must be notified "without unreasonable delay" and no later than 60 days after discovery of the breach. If a breach exceeds 500 people HHS and the media must also be notified within this same time frame. HHS must also be notified annually of any data breaches regardless of size.

In 2013 the HIPAA Omnibus Rule revised the Breach Notification Rule to alter the standards for determining when a breach has occurred. Under the Omnibus Rule, the acquisition, access, or use of PHI in a manner not permitted under the Privacy Rule is presumed to be a breach, unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised (based on an analysis that looks to certain factors spelled out in the regulations). If the covered entity or business concludes that use or disclosure not permitted by the Privacy Rule does not rise to the level of compromising the PHI, the burden is on the covered entity/business associate to justify that decision in the event of an investigation by regulators.

HIPAA Exemptions. HIPAA does not apply to information that does not meet the definition of PHI such as: 1) information that is not individually identifiable because it is "de-identified" (as defined in the Privacy Rule), or 2) information that is used by individuals or entities that do not fall within the definitions of "covered entities" or "business associates" of covered entities. There are additional exemptions from the restrictions on disclosure of PHI for law enforcement purposes or to avert a serious public health threat.

Enforcement. HIPAA is enforced by the Office of Civil Rights within HHS. This office can initiate investigations into covered entities' information handling practices to determine whether they

are complying with the HIPAA Privacy Rule. Individuals also have the right to file complaints with HHS about privacy violations. In addition, the HITECH Act gave state attorneys general the right to initiate enforcement actions under HIPAA. **HIPAA does not include a right for individuals to bring private actions**.

Civil and Criminal Liability. A person who violates HIPAA due to willful neglect and does not correct the violation within 30 days can be fined $50,000 per violation. Potential criminal penalties for HIPAA violations include fines of $50,000 to $250,000 and up to ten (10) years in prison. Criminal enforcement via the Department of Justice and civil enforcement occurs through the HHS Office for Civil Rights. As noted above, state attorneys general can now also bring HIPAA actions in accordance with the HITECH Act.

Medical Research - The Common Rule

Regulation 45 C.F.R. § 46.01, otherwise known as the Common Rule, ensures that the rights of an individual are protected during a research project and applies to most federally-funded research. Privacy and confidentiality are key elements along with informed consent of the person involved in the research.

Federal Trade Commission Act (FTC Act)

Section 5 of the Federal Trade Commission Act (FTC Act, 15 U.S.C. § 45) is a federal consumer protection law that prohibits unfair or deceptive commercial practices and has been applied to business practices that affect consumer privacy and data security. The FTC is the most active federal agency relative to privacy matters and has initiated enforcement actions against businesses for, among other things, 1) failure to comply with statements made in their website privacy policies, 2) making material changes to privacy policies without adequate notice to consumers, and 3) failure to provide reasonable and appropriate security and protections to safeguard consumer information.

Entities Subject to FTC Act. The FTC Act and related FTC-issued rules and guidelines apply to most companies and individuals doing business in the U.S. The Act does not focus on one specific industry or type of data

Type of Data Regulated. There is likewise no specific category or type of personal information that is regulated under the FTC Act. It broadly prohibits unfair and deceptive acts or practices that affect consumer personal information.

Unfair or Deceptive. Section 5 of the FTC Act prohibits "unfair or deceptive trade practices in or affecting commerce." The FTC has enforced the FTC Act against companies that have made false or deceptive claims about privacy and security of customer data.

The FTC has brought several actions against companies that claimed in a privacy policy that they employed reasonable measures to protect customer data. The FTC concluded that the security measures used by the businesses were insufficient. Similarly, if a company states on its website that customer information will never be shared, that statement may be considered "deceptive" if the information is disclosed to third-party service providers or even to acquiring entities in an asset sale.

A good way to learn how to avoid an FTC enforcement action is to review the FTC actions and determine what activities caused concern. We have listed a few of these FTC actions in this Guide. More details on FTC enforcement and consent decrees can be found at the FTC website.

Privacy Notices and Policies. Although the FTC Act does not specifically require that a "Privacy Notice" be posted on a company's website, the FTC has consistently maintained the position that the use or dissemination of personal information contrary to a posted privacy policy is a deceptive trade practice under the FTC Act. The key to compliance with the FTC Act is therefore to make sure

that your website privacy statement or notice is consistent with actual practice. The easiest way to get in trouble with the FTC for a violation of the FTC Act is to have a privacy policy on a website that suggests that no personal information will be shared with any third party when such information is actually shared.

Transparency. Say what you do and do what you say. The FTC has taken the position that if a company discloses a privacy policy, it must comply with it.

Retroactive Material Changes to Website Privacy Policy. It is a potential violation of the FTC Act for a company to retroactively make material changes to its privacy policy without providing consumers with notice of those changes and the opportunity to opt out of the new privacy policy.

Consent Requirements. Although the FTC Act does not expressly address consent, website operators that revise their privacy policies should obtain affirmative express consent (that is, allow consumers to opt-in) before using their data in ways that are materially different from the privacy policy that was in effect when the data was collected.

Individual Access to Collected Data and Right to Correct or Delete Data. The FTC Act and most federal and state privacy laws, (with the exception of HIPAA and some California laws) do not provide individuals with specific rights to access or correct their personal information. COPPA is enforced by the FTC and requires that website operators allow parents to 1) view the personal information collected by a website about their child, and 2) delete and correct that information. Note that COPPA applies to children under the age of 13.

The White House's 2012 Consumer Data Privacy Bill of Rights contained in the report Consumer Data Privacy in a Networked World states that, "companies also should provide consumers with

reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation." This is not a law but there may be more voluntary codes of conduct or new laws passed as a result of this report. [See discussion of the so-called California Eraser law that went into effect in 2015 on pages 34 and 108.]

In May 2014, The European Court of Justice recognized the controversial "right to be forgotten." [See page 156]

Data Security Requirements. The FTC Act does not specifically address data security. The FTC has, however, brought enforcement actions alleging that the failure to take reasonable and appropriate steps to protect personal information is an "unfair act or practice" in violation of the FTC Act. For example, the FTC has found violations of the FTC Act where a company 1) failed to encrypt information while it was in transit or stored on the network, 2) stored personally identifiable information in a file format that permitted anonymous access, 3) did not use readily accessible security measures to limit access, 4) failed to employ sufficient measures to detect unauthorized access or conduct security investigations, and 5) created unnecessary business risks by storing information after it no longer had any use for the information, in violation of bank rules. [See Wyndham case discussed on pages 27-29.]

Restrictions on Sharing Data with Third Parties. The FTC Act does not expressly prohibit the sharing of personal information with third parties. However, a business can get into trouble when it states that it will not rent, sell, or otherwise disclose personal information to third parties, but then it does.

Enforcement. The FTC is the primary enforcer of the FTC Act and is also responsible for the enforcement of some other federal privacy laws for businesses that are not subject to other federal regulations, including GLBA, COPPA, FCRA, and FACTA. Actions

the FTC can take include 1) starting an investigation, 2) issuing a cease and desist order, or 3) referring to the Department of Justice for filing a complaint in court.

Sanctions and Other Liability. The FTC Act provides penalties of up to $16,000 per offense. Criminal penalties include imprisonment for up to ten years. The FTC can also 1) obtain injunctions, 2) provide restitution to consumers, and 3) require repayment of investigation and prosecution costs. Persons and entities who obtain, attempt to obtain, cause to be disclosed, or attempt to cause to be disclosed customer information of a financial institution (relating to another person) through false, fictitious, or fraudulent means, can be subjected to fines and imprisoned for up to five years.

Criminal penalties of up to ten years' imprisonment and fines of up to $500,000 (for an individual) or $1 million (for a company) may be imposed if the acts are committed or attempted while violating another U.S. law, or as part of a pattern of illegal activity involving more than $100,000 in a year.

FTC Enforcement Actions. Important lessons can be learned from previous FTC investigations, settlements, and consent decrees. Settlements with the FTC and other government agencies also often provide for onerous reporting requirements, audits, and monitoring by third parties. Most FTC consent decrees include a 20 year term with regular audits of the company privacy practices. By reviewing these FTC actions and consent decrees, a business might learn what activities might be challenged by the FTC. Notable examples of FTC enforcement actions include:

***In re Google* (2012)**. Google paid a $22.5 million fine to the FTC following a charge that it had placed tracking cookies on computers of Safari users. This was in violation of an earlier settlement with the FTC regarding the extent of control users were given over the use of their data. *United States v. Google, Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012)

In re Facebook (2011). The FTC charged Facebook with making changes to its privacy policy that resulted in users having data exposed to the public without warning or obtaining consent from the users. The FTC alleged both deception (failure to properly notify users) and unfairness (making material retroactive changes to privacy policies without consent). Facebook was required to develop and implement a "comprehensive privacy program" and be open to privacy audits for the next 20 years. (FTC File No. 092-3184)

***In re Toysmart.com* (2000)**. An internet toy seller went bankrupt and planned to sell its customer database to pay back creditors. The FTC found this to be a deceptive practice in that its privacy policy stated that customer data "is never shared with a third party." Toysmart.com settled and allowed the bankruptcy court to approve of the buyer and required the buyer to limit how it could use the customer data. *FTC v. Toysmart.com LLC* No. 00- 11341-RGS (D. Mass. July 21, 2000)

***In re CVS Caremark* (2009)**. The operator of the largest pharmacy chain in the United States agreed to pay $2.25 million to settle charges brought by the FTC and HHS for violating consumer and medical privacy laws. CVS had allegedly been disposing of patient information via unsecured trash containers. (FTC File No. 072 3119)

***In re TJX, Inc.* (2008).** The parent company of several major retailers, in settling charges of failing to adequately protect customers' credit card numbers, agreed to allow comprehensive audits of its data security system for 20 years. TJX was accused of storing unencrypted sensitive information, failing to limit unauthorized wireless access to networks, and not employing appropriate security safeguards. (FTC File No. 072-3055)

***In re Choicepoint* (2006)**. A database owner and data broker, agreed to pay $15 million to settle charges filed by the FTC for failing to adequately protect the data of millions of consumers.

Choicepoint had failed to exercise proper credentialing procedures that resulted in fraudulent access of personal information and identity theft by those accessing the information. (FTC File No. 052-3069)

In re Microsoft Corp.* (2002)**. (FTC File No. 0123240, M03) and ***In re Guess.com Inc. (2003). (FTC File No. 0223260) In both of these actions the FTC claimed that the companies misrepresented security protections on their websites and failed to provide even the most basic data security safeguards. No data was actually lost in either of these cases and there was no data breach. Still, the promise or misrepresentation of data security was sufficient for the FTC to take action. Neither Microsoft or Guess paid a fine but they were required to establish extensive written security programs and remain open to privacy audits for 20 years.

***In re HireRight Solutions, Inc.* (2012).** (FTC File No. 102- 3130) (FTC File No. 102- 3130) Employment background checking company providing "consumer reports" failed to use reasonable procedures to assure the maximum possible accuracy of the information, failed to give consumers copies of the reports, and failed to investigate consumer disputes. It agreed to pay $2.6 million for FCRA violations in addition to other corrective actions.

On December 17, 2015, ***LifeLock, Inc.*** agreed to pay $113 million to settle charges made by the FTC that the company had failed to create and maintain a comprehensive information security program to protect customers personal data, including social security and bank account information. This was largest monetary award obtained by the FTC in an order enforcement action.

Challenging FTC Jurisdiction In Data Security Actions. Does the FTC have the authority to regulate and impose data security standards on private businesses under the FTC Act?

For the first time, a business challenged the very authority of the Federal Trade Commission (FTC) to regulate the data security practices of private businesses in ***FTC v. Wyndham Worldwide Corp.*** No. 2:13cv1887 (D.N.J. 2014).

The FTC alleged that franchisor Wyndham Hotels and Resorts, along with its affiliates, engaged in deceptive practices by misrepresenting that it used "industry standard practices" and "commercially reasonable efforts" to secure the data it collected from guests and in unfair practices by failing to protect customer data. Between 2008 and 2010, a criminal organization hacked into the property management system multiple times, and accessed credit card information from several hundred thousand guests. For its remedies, the FTC sought both monetary damages and a permanent injunction requiring Wyndham and its franchisees to better secure their systems.

The FTC has been increasingly aggressive in bringing enforcement actions against private businesses under the FTC Act following data privacy and security breaches. Because these actions generally have been resolved through settlements and consent decrees, there are very few court opinions defining the boundaries of FTC authority in this area.

In fact, Wyndham was the first company to overtly challenge the FTC's authority to regulate and impose data security standards on businesses through enforcement actions under the FTC Act.

In a motion to dismiss that was denied in April 2014, Wyndham essentially argued that Congress never granted the FTC such broad authority to regulate in this area, and even if it did, the FTC has not provided businesses with fair notice of what data security practices it believes the FTC Act forbids or requires.

A court decision in favor of Wyndham and limiting the FTC investigative and enforcement powers would have had a profound impact on data privacy and security law enforcement. But the court denied Wyndham's motion and affirmed the FTC's enforcement authority including claims of inadequate data security.
On December 9, 2015, Wyndham entered into a settlement agreement with the FTC that, among other things, requires the establishment of a comprehensive information security program designed to protect cardholder data that conform to PCI-DSS, annual information security audits, and safeguards in connection with franchisee servers. The Wyndham obligations remain in effect for 20 years.

Unique Issues For Franchised or Fragmented Businesses. The Wyndham case also highlights the unique issues for franchised or licensing based systems relative to legal compliance with data privacy and security laws. Computer systems that are fully integrated or that stand-alone and that collect personal data may hold differing legal risks in the event of a data breach. These liability issues should be carefully considered when establishing the computer systems, data access, and the relevant agreements between the various parties. The 20 year FTC/Wyndham settlement agreement requires the company to conduct annual information security audits and maintain safeguards in connection with franchisee servers.

FTC Setback. Just weeks before the Wyndham settlement, the FTC lost a case it had brought against cancer screening laboratory LabMD. The laboratory had been accused of two data breaches when a company spreadsheet with sensitive personal information was found on a peer to peer network. On November 13, 2015, after seven years of litigation, an FTC Chief Administrative Law Judge dismissed the FTC complaint since it failed to prove that LabMD's alleged failure to employ reasonable and appropriate data security caused, or was likely to cause, substantial injury to consumers. The

Judge stated that the alleged unreasonable data security of LabMD cannot properly be declared an unfair act or practice in violation of Section 5(a) of the FTC Act. Some suggest that this case may result in FTC enforcement actions being more focused on cases where actual harm can be demonstrated and not the mere possibility of harm to consumers.

Largest Monetary Award Ever Obtained By FTC. LifeLock, Inc. agreed, on December 17, 2015, to pay $113 million to settle contempt charges that it violated a 2010 court order to secure personal information of consumers and stop deceptive advertising. The FTC alleged the failure to establish and maintain a comprehensive information security program to protect user sensitive personal information including social security, credit card, and bank account numbers as well as false advertising that LifeLock protected sensitive data with the same high level safe guards used by financial institutions.

Dental Practice Provider Settles FTC Charges. On January 5, 2016, Henry Schein Practice Solutions, Inc., a provider of office management software for dental practices, agreed to pay $250,000 to settle FTC charges that it falsely advertised the level of encryption it provided to protect patient data.

Deceptive Advertising. The FTC Act also governs deceptive practices in advertising, including direct-mail communications. The Act requires businesses to use truth-in-advertising, meaning that 1) the advertising must be truthful and not deceptive; 2) the advertisers must have evidence to back up their claims; and 3) the advertising must be fair, or not likely to cause substantial consumer injury. In determining whether an advertisement meets these criteria, the FTC will consider both the express and implied claims made by the advertisements, and information that is omitted. Penalties for a violation of the Act include cease and desist orders, civil penalties, and corrective advertising.

FTC Online Behavioral Advertising Principles

The FTC's Online Behavioral Advertising Principles appear in a report that was prepared by the FTC staff in 2009. These principles apply to website operators that engage in behavioral advertising (also called contextual advertising and targeted advertising). While compliance with the principles is voluntary, many companies adopt them as best practices. The FTC report and principles suggest ways that businesses using online advertising can protect consumer privacy while collecting information about their online activities.

According to these principles website operators that collect or store consumer data for behavioral advertising purposes must do the following:

- provide reasonable security for that data;
- retain data for only the time necessary to fulfill a legitimate business or law enforcement need;
- disclose to consumers their data collection practices tied to online behavioral advertising;
- disclose that consumers can opt-out of (that is, say "no" to) these practices;
- provide a mechanism to the consumer for opting out (for example, by allowing the consumer to electronically check a box indicating that the consumer is opting out or by sending an email to the operator); and
- obtain affirmative express consent (which can be provided online) from consumers before collecting or using sensitive consumer data in connection with online behavioral advertising. Sensitive data includes (but is not limited to): 1) financial data, 2) data about children, 3) health information, 4) precise geographic location information, and 4) social security numbers.

The extent and type of protections given to consumer data should be based on the: 1) sensitivity of the data, 2) nature of the company's business operations, 3) types of risk the company faces, and 4) reasonable protections available to the company.

The FTC has also issued other guidelines and publications relating to privacy and data security that are useful for establishing best practices. Two examples are ***Protecting Consumer Privacy in an Era of Rapid Change*** and ***Self-Regulatory Principles for Behavioral Advertising***.

Self-Regulation of Behavioral Online Marketing. In addition to the FTC's efforts to educate businesses, efforts have been made by industry organizations to self-regulate and offer best practices. Guidance can be found from the following organizations for activities and best practices related to online behavioral advertising:

American Association of Advertising Agencies

Association of National Advertisers

Council of Better Business Bureaus

Direct Marketing Association

Interactive Advertising Bureau

Mobile Marketing Association

Children's Online Privacy And Protection Act (COPPA)

The federal government has focused a great deal of attention on websites (that collect personal information) directed at children under the age of 13. The Children's Online Privacy and Protection Act (COPPA) (15 U.S.C. §§ 6501-6506) requires operators of websites directed at children under the age of 13 (or websites that knowingly collect information from children under 13) to provide a detailed privacy notice regarding their collection and use of children's data

online. COPPA also requires that the operator of the website obtain "verifiable parental consent" before collecting or using children's information beyond a one-time inquiry. The operator must provide parents with the ability to review the information collected from the child and ask for it to be deleted at any time.

FTC amendments to COPPA in 2013 expanded the definition of "personal information" to include persistent identifiers, such as IP addresses and mobile device IDs, that recognize users over time and across different online services. As a result, behavioral advertising on child–directed online services now requires parental notice and consent. COPPA now also applies to geo-location information.

According to COPPA, personal information is defined as individually identifiable information about a child that is collected online, such as:

- A full name.
- A home address.
- Online contact information.
- A telephone number.
- A social security number.
- A persistent identifier that can be used to recognize a user over time and across different websites or online services.
- A photo, video, or audio file, where such file contains a child's image or voice.
- Geo-location information sufficient to identify a street name and name of a city or town.
- Information concerning the child or the child's parents that an operator collects online from the child and combines with an identifier described above.

COPPA's requirements include, among other things, that these websites or online services:

- Provide a privacy notice on the site (including a clear and prominent link to the notice from the home page and at each area where it collects personal information from children) that informs parents about their information gathering practices.
- Before collecting, using, or disclosing personal information of children:
  - o provide direct notice to parents (containing the same information required in the website notice); and
  - o obtain (with some exceptions) "verifiable parental consent." The method for obtaining consent varies depending on the type of use that will be made.
- On request, provide parents of children who have given personal information with:
  - o a description of the types of personal information collected;
  - o an opportunity to prevent any further use or collection of information; and
  - o a reasonable means to obtain the specific information collected.
- Maintain procedures to ensure the confidentiality, security, and integrity of the personal information collected.

Privacy Notice Under COPPA. Children's websites must post privacy notices that describe "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information." 15 U.S.C. § 6502(b)(1) (A)(i).

Parental Consent - Opt-in Required. "Verifiable parental consent" is required for the collection, use, or disclosure of personal information from children. Websites cannot condition a child's participation in a game or receipt of a prize or the disclosure of more information than is necessary to participate in any activity. 15 U.S.C. § 6502(b) (1)(C).

Third-Party Ad Networks and Mobile Apps. The 2013 COPPA amendments now hold websites and mobile apps liable for collection by third party ad networks and plug-in providers for the absence of parental notice and consent. Third-party ad networks and third-party social plug-ins must also comply with COPPA if their operators have actual knowledge that such personal information is being collected from children.

California Eraser Law. In 2015 a new law in California became effective that requires mobile app developers and website operators to allow anyone under the age of 18 to have certain information deleted from their records. Note that COPPA applies to children under 13. This so-called "eraser law" is discussed later in this Guide under California laws. (See pages 108)

Best Practices/Safe Harbor. The Children's Advertising Review Unit (CARU), part of the Advertising Self-Regulatory Council (ASRC) administered by the Better Business Bureau, was established to police children's marketing and COPPA compliance. CARU has created a "safe harbor program" to give businesses specific guidelines and steps to follow to ensure compliance with FTC regulations. (See http://www.caru.org and pages 160-161)

A business that follows the CARU guidelines that have been approved by the FTC will be deemed to have satisfied the COPPA requirements. 15 U.S.C. § 6503.

COPPA Enforcement. COPPA is enforced by the FTC and violations of COPPA are considered an unfair and deceptive trade practice under the FTC Act. **There is no private cause of action under COPPA.** State attorneys general can also bring civil actions under COPPA as necessary to protect the public interest and can obtain injunctions and damages.

FTC COPPA Enforcement Actions. The following actions have been taken by the FTC against businesses for failure to comply with COPPA:

***FTC v. Rock You* (2012)**. Social gaming site allowed users to make slide shows with photos. To save the slide show a user had to enter an email address and password along with birthdate. This information was collected from children under 13. The investigation by the FTC also found that the game site lacked adequate security and exposed email addresses and passwords to potential hackers. The settlement and consent decree included extensive compliance monitoring that will remain in effect for the next 20 years. (FTC File No.1023120)

***In re Iconix Brand Group* (2009)**. For the collection of information from children without parental consent, the company paid a settlement fee to the FTC of $250,000. (FTC File No.0923032)

***FTC v. Playdom* (2011).** Playdom agreed to pay $3 million, the largest civil penalty assessed for a COPPA violation, for failing to provide proper notice or obtain parental consent. In this case the company had allowed children to post personal data on public pages and the privacy policy falsely stated that children under 13 were prohibited from posting personal data on the internet. (FTC File No. 1023036)

A good source of information on COPPA compliance and consent decrees can be found on the FTC website.

Controlling The Assault Of Non-Solicited Pornography And Marketing Act (CAN-SPAM)

Email Communications. . Email has become the most common form of communications with employees, customers, and other businesses. The low cost and convenience of email and the widespread use of the internet has made it a popular method for businesses to market their products and services. These features also make email easy to abuse, by both sending messages with unwanted content and sending an unnecessary volume of email. Because of the possibilities of abuse, laws at both the federal and state level have emerged to regulate the commercial use of email.

CAN-SPAM is a federal law designed to regulate the collection and use of email addresses for commercial purposes. CAN-SPAM prohibits the sending of a commercial email that uses 1) any false or misleading header information, and 2) subject lines that would likely mislead the recipient about a material fact regarding the contents or subject matter of the message.

Commercial email includes instances in which the primary purpose of the email is the commercial advertisement or promotion of a product or service, including content on websites. Messages with transactional or relationship content, such as updates about an already agreed-upon transaction, or other noncommercial content are exempt.

When messages have both commercial and transactional content, the primary purpose of the message is usually determined by the content. CAN-SPAM applies to messages directed to other businesses as well as those directed to consumers. Senders may also be liable for the messages that are forwarded on by third parties, if the sender provides an incentive for such forwarding.

CAN-SPAM Requirements. CAN-SPAM imposes several requirements on email senders. First, the message must use accurate header and routing information, including the originating domain name and email address. The message must also include a valid physical postal address where recipients can send mail to the sender. The message must use accurate subject lines, and identify itself as an advertisement. Finally, the message must provide an opportunity for the recipient to opt-out of future communications, and the sender must honor opt-out requests within ten (10) business days after receiving the request. Businesses should make sure that they do not ask for additional personal information when a recipient opts out. The only information necessary is the email address of the person opting out of future communications.

Penalties. Violations of the CAN-SPAM Act may result in civil penalties of up to $16,000 for each message that violates the Act. More than one person can be held liable. For example, both the company whose product is promoted in the message and the company that originated the message may be liable. Misleading claims about products or services may also be subject to the FTC Act as deceptive advertising (See page 29). In addition, criminal penalties and even imprisonment can apply for certain actions, such as accessing someone else's computer to send spam without permission, using false information to register for multiple email accounts or domain names, routing messages through other computers to disguise the origin of the message, or generating email messages through a "dictionary attack." A "dictionary attack" is the practice of sending email to addresses made up of random letters and numbers in the hope of reaching valid ones.

Enforcement. CAN-SPAM is enforced by the FTC and violations are deemed an "unfair and deceptive act or practice." 15 U.S.C. § 7706(a). State attorneys general can also bring actions for damages suffered by state residents as well as injunctive and equitable relief. Criminal penalties are available for predatory and abusive commercial email. [15 U.S.C. § 7703] **There is no private right of action under CAN- SPAM.**

More information on how to comply with CAN-SPAM can be found at the FTC's Bureau of Consumer Protection, Business Center website http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business. Canada has recently enacted one of the strictest laws to curb unsolicited commercial email with significant penalties for non-compliance (See pages 129).

Laws Restricting Cell Phone Marketing. Cell phones can receive two forms of unsolicited commercial advertising: text messages and phone calls. Unsolicited text messages fall under CAN-SPAM to the extent the message originates from internet addresses. Such text messages are subject to both CAN-SPAM and FCC regulations. Text messages that are sent from phone to phone do not involve internet domains and are therefore not subject to CAN-SPAM and the FCC. Phone to phone text messages are subject to the TCPA discussed below.

The Telephone Consumer Protection Act (TCPA) [47 U.S.C. § 227]

Text Messaging. All marketing through telephonic devices, including mobile phones, is controlled by the Telephone Consumer Protection Act (TCPA) passed in 1991, which falls under the FCC's jurisdiction. The TCPA allows individuals and private lawyers to file lawsuits and collect damages for receiving unsolicited telemarketing calls, faxes, pre-recorded calls, auto dialed calls, or text messages. Marketing through telephonic devices, including mobile phones, is covered by the TCPA. Purely informational calls and calls for noncommercial purposes are exempt but dual-purpose calls may be covered.

Consent Necessary for Commercial Text Message. Text messaging is gaining in popularity, in large part because texting has proven to be one of the more effective and targeted forms of marketing. The TCPA applies to both voice and short message

service (SMS) text messages if they are transmitted for marketing purposes. The FCC has added regulations to the TCPA so that effective October 2013, prior express written consent is required for all autodialed and prerecorded calls or text messages made to a cell phone or mobile device and prerecorded calls made to residential land lines for marketing purposes.

Electronic or digital forms of signature are acceptable for compliance with this consent requirement. The consent must be "unambiguous" meaning that the consumer must receive a "clear and conspicuous disclosure" that he or she will receive calls that deliver autodialed or pre-recorded telemarketing messages on behalf of a specific advertiser, that his or her consent is not a condition of purchase, and he or she must designate a phone number at which to be reached.

It is a best practice for advertisers to maintain each consumer's written consent for at least four years, which is the federal statute of limitations to bring an action under the TCPA. The FCC eliminated the "established business relationship" exemption so that advertisers can no longer rely upon a previous purchase to avoid the prior consent requirement. Since these FCC consent requirements under the TCPA are now in effect, a business should make sure that they comply and that any company hired to run a marketing campaign on their behalf complies with the TCPA, including the consent requirements.

Autodialers. Most applicable to text messaging, the TCPA restricts the use of autodialers and prohibits any autodialed calls to a wireless device that charges for usage, unless the consumer has specifically consented to the communication. SMS messages and text messages sent to a number of consumers at once almost always use an "autodial" function; therefore, companies are prohibited from sending such texts without consent.

Do Not Call Registry. The TCPA authorizes the Do Not Call Registry where people can register their numbers if they do not wish to receive telemarketing calls. Prerecorded messages without the consent of the recipient are prohibited. Fax and cell phone numbers can be registered as well as landlines. Once a consumer has put his or her personal number on the list, telemarketers cannot call (or text) them without express prior permission unless the parties have an established business relationship.

Enforcement. The TCPA allows for a private right of action (meaning consumers can sue a company directly claiming violation of TCPA) for $500 per infringing call or text message, or $1,500 per violation if the company willfully or intentionally violated the law. An individual can also sue for actual loss not to exceed $500 for each call received after requesting to be placed on the Do Not Call Registry. State attorneys general may also initiate actions against telemarketers engaging in a pattern or practice of telephone calls or other transmissions to residents of that state in violation of the TCPA. If the telemarketer acted willfully or knowingly the damages can be trebled.

TCPA Rulings. The following FCC rulings cover text messaging under the TCPA:

Nonadvertising Voice Calls and Text Messages to Wireless Numbers. On March 27, 2014, the FCC issued two rulings under TCPA clarifying that in certain circumstances, a sender may rely on third-party intermediaries to obtain consumers' consent to receive administrative text messages and prerecorded phone calls on their cell phones, and exempting package delivery service messages from certain TCPA requirements where specified conditions are met. The FCC also clarified that text-based social networks may rely on consumers' consent obtained and conveyed by an intermediary to send administrative text messages related to the service. [See *In re Cargo Airline Assoc.*, CG No. 02-278, FCC 14-32 (Mar. 27, 2014) and *In re GroupMe, Inc.*, CG No. 02-278, FCC 14-33 (Mar. 27, 2014).]

In these rulings the FCC further confirmed that 1) a caller is obligated to obtain express consent, and that the caller may be liable for TCPA violations even when relying on an intermediary's assertions, 2) by agreeing to participate in a social media service such as GroupMe, and providing a wireless phone number to do so, a consumer consents to receive administrative texts only for that specific group service, 3) an intermediary may only convey a consumer's consent. The intermediary cannot consent on a consumer's behalf.

TCPA Penalties Steep. With violations from $500 to $1,500 per text message, and private lawyers able to bring actions, these lawsuits are likely to grow. A business should therefore be careful how they use text messaging as a marketing tool.

TCPA Best Practice. Companies should create and maintain a tracking database for customers' consent to receive texts and follow up immediately when receiving a request to "unsubscribe" or "opt out" of future text messages or phone calls.

TCPA Allows Private Right of Action. Because of this private right of action under the TCPA and the prohibition against autodialed text messages in the TCPA, there have already been some significant legal actions taken against both large—and smaller— companies who have failed to comply with the TCPA regulations on mobile communications and text messaging. Notably, in 2011, a class action lawsuit was brought against Domino's Pizza for a text message campaign that the plaintiffs claimed was directed to consumers who had not previously consented to the communication. A similar case was brought against Papa John's in 2012. Domino's settled its TCPA class action suit in 2013 for just under $10 million. In 2013, Huffington Post was sued for sending out "news alerts" by text messaging at all times of the day and night, and not taking readers off their list when receiving requests to "UNSUBSCRIBE."

Robo-calls. Best Buy robo-calls that followed up on customer purchases that also described the "rewards program" were deemed an enticement to make future purchases and a violation of the TCPA. *Chesbro v. Best Buy*, 2012 WL 6700555, (9th Cir. 2012).

On March 28, 2014, in *Freddy D. Osorio v. State Farm Bank, F.S.B.*, the Court of Appeals for the Eleventh Circuit determined that a party making autodialed and prerecorded calls to cellphone numbers may be liable under the TCPA even where 1) the cellphone number has not been reassigned or 2) the caller believes it has obtained consent.

TCPA Intersection with HIPAA. The TCPA includes two regulatory exceptions for health care messages provided they are made by HIPAA covered entities or business associates. In 2014 there were several class action law suits alleging that prescription reminders violated the TCPA by sending automated or prerecorded calls or text messages without the required consent and without falling within a TCPA exception. The cases in this area highlight the distinction made between marketing and non-marketing communications. Calls and text messages received by an unintended recipient might result in an impermissible disclosure of protected health information and require breach notification. See July 10, 2015 FCC Ruling cited below for more details on compliance with the healthcare treatment exception.

TCPA Declaratory Ruling and Order. On July 10, 2015 the FCC released its ruling with clarification of a number of TCPA issues including the definition of autodialer, liability for calls made to reassigned phone numbers, a consumer right to revoke consent by any reasonable means, and new exceptions for financial and healthcare related calls. The FCC invoked its authority under the TCPA to exempt from the consent requirement various "free to end user "communications (no charge to recipient of call) that are "pro consumer messages" made by certain entities regarding time sensitive financial information and health treatment related messages.

Telemarketing and Consumer Fraud and Abuse Prevention Act [15 U.S.C. §§ 6101-6108]

The FTC and the FCC have promulgated several rules relating to deceptive telemarketing practices. The FTC's Telemarketing Sales Rule gives effect to the Telemarketing and Consumer Fraud and Abuse Prevention Act. The Telemarketing Sales Rule requires sellers to provide consumers with all information that would likely be material to the consumers' choice of goods or services, including information on cost and quantity, material restrictions, limitations or conditions, refund policies, and features such as free trial offers. The Telemarketing Sales Rule also prevents sellers from misrepresenting such material information. For outbound sales calls or upsells, these disclosures must be made promptly. Special requirements apply to prize promotions, credit card loss protection plans, and debt relief services.

The Telemarketing Sales Rule also contains a number of privacy protections. These rules prevent calling numbers that are on the National Do Not Call Registry or on that seller's do-not-call list; denying or interfering with a person's right to be placed on any do-not-call registry; calling outside permissible calling hours; abandoning calls; failing to transmit caller ID information; threatening or intimidating a consumer or using obscene language; or calling or talking to a person with the intent to annoy, abuse, or harass the person called.

The Telemarketing Sales Rule applies to most businesses except for banks, nonprofits, insurance companies, and others that are regulated by state law. It also does not apply to unsolicited calls from consumers, telephone calls made by consumers in response to advertisements, and most business-to-business calls. Upsells within such calls are not exempt.

Deceptive Mail Prevention and Enforcement Act (DMPEA)

Sweepstakes and other contests are governed by the Deceptive Mail Prevention and Enforcement Act of 1999. The Act establishes opt-out procedures and a number of required disclosures for sweepstakes or contest mailings, as well as mailings of facsimile checks and mailings made to resemble government documents. Failure to comply with the Act can lead to an investigation by the U.S. Postal Service, civil penalties, and a mail-stop order. Sweepstakes and contests are also covered by various state laws and any company looking into sweepstakes promotions should be sure to comply with all relevant state laws and regulations. The Minnesota Attorney General's Office has a publication explaining the do's and don'ts of running a sweepstakes and similar promotions in Minnesota (See Minn. Stat § 325F.755 Prize Notices and Solicitations and http://www.ag.state.mn.us/consumer/publications/sweepstakesprizes.asp)

Junk Fax Prevention Act (JFPA)

In addition to regulations governing direct mailings, the TCPA, as amended by the Junk Fax Prevention Act, prohibits most unsolicited fax advertisements. The Junk Fax Prevention Act prohibits sending unsolicited advertisements to any fax machine, whether at a residence or business, without the recipient's prior express permission. Liability for a violation of the law applies to the company whose advertisement is sent, even if the sender is a third-party fax broadcaster.

An exception in the Junk Fax Prevention Act allows a person to send a fax to a recipient with whom the sender has an existing business relationship, so long as the recipient volunteered its fax number. Senders must honor requests from recipients to opt-out of receiving unwanted faxes. Placing oneself on a do-not-call list does not prevent fax solicitations. Fax machine numbers may however be separately registered.

Computer Fraud And Abuse Act (CFAA) [18 U.S.C. § 1030 (c)]

Purpose. The purpose of the CFAA is to prevent unauthorized access to computers and applies to any "protected computer" used in interstate commerce or communication. This broad definition has allowed the CFAA to be applied to any computer connected to the internet. The CFAA establishes multiple crimes and imposes criminal penalties when a person or entity "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer." 18 U.S.C. § 1030(a)(2)(c). The CFAA prohibits knowingly transmitting "a program, information, code or command" or "intentionally access[ing] a protected computer without authorization" that causes damage to a "protected computer." 18 U.S.C. § 1030(5)(A)(i).

Damage. Some of the CFAA provisions require that "damage" be proven in the form of "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e).

Civil and Criminal Remedies. Punishments range from fines to imprisonment of up to 20 years depending on the nature of the offense. **"Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages or injunctive relief or other equitable relief."** 18 U.S.C. § 1030(g). Damage must cause a loss aggregating at least $5,000 in value during any one year period to one or more individuals. 18 U.S.C. § 1030(e).

Exceeding Authorized Access. In some cases under the CFAA a violation is triggered when one "exceeds authorized access." This means to "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain and to alter." 18 U.S.C. § 1030(e)(6). (See further discussion of CFAA on page 70)

Electronic Communications Privacy Act (ECPA) [18 U.S.C. §§ 2510-3127]

The Electronic Communications Privacy Act (ECPA) was passed in 1986 to expand and revise federal wiretapping and electronic eavesdropping laws. It was envisioned to create "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." Congress also sought to support the creation of new technologies by assuring consumers that their personal information would remain safe.

Phone Conversations. ECPA includes the Wiretap Act, [18 U.S.C. §§ 2510-2522], the Stored Communications Act (SCA), [18 §§ 2701-2711], and the Pen Register Act, [18 U.S.C. §§ 3121-3127]. Wire communication refers to "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection." It essentially covers phone conversations. An oral communication is "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." This constitutes any oral conversation including phone conversations with a person where there is the expectation that no third party is listening.

Penalties. Individuals who violate ECPA face up to five years of jail time and a $250,000 fine. **Victims are also entitled to a civil suit of actual damages, in addition to punitive damages and attorneys' fees.**

Electronic Eavesdropping. ECPA protects a person's wire and electronic communications from being intercepted by another private individual. In general, the statute bars wiretapping and electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and the use or disclosure of information unlawfully obtained through wiretapping or electronic

eavesdropping. The Wiretap Act prohibits any person from intentionally intercepting or attempting to intercept a wire, oral or electronic communication by using any electronic, mechanical or other device. An electronic device must be used to perform the surveillance; mere eavesdropping with the unaided ear is not illegal under ECPA.

Exceptions. There are exceptions to this blanket prohibition, such as if the interception is authorized by statute for law enforcement purposes or consent of at least one of the parties is given. Although some states such as California prohibit the recording of conversations unless all parties consent, ECPA requires only one party to consent. An individual can record his own conversation without violating federal law. In the workplace, an employer would likely not violate ECPA by listening to an employee's communications if, for example, blanket consent was given as part of the employee's contract.

In addition to criminalizing the actual wiretapping or electronic eavesdropping, ECPA also prohibits an individual from disclosing such information obtained illegally if the person has reason to know that it was obtained illegally through the interception of a wire, oral, or electronic communication.

Email. The Stored Communications Act ("SCA") has been found to apply to all email stored in the United States whether it belongs to U.S. citizens or foreigners. [See *Suzlon Energy Ltd. v. Microsoft Corps.* 671 F.3d 726 (9th Cir. 2011) and further discussion of the SCA on pages 69-70.]

Federal Laws Related To Social Security Numbers

A social security number is a sensitive piece of information and remains one of the easiest ways for a criminal to pursue identity theft. There are a variety of federal and state laws that require

businesses to protect the confidentiality of social security numbers. Federal legislation specifically focused on restricting the use and disclosure of social security numbers has been introduced but no comprehensive law exists today at the federal level.

The GLBA and HIPAA protect the confidentiality of personally identifiable information, including social security numbers. FCRA limits access to credit data (including social security numbers) to those with a permissible purpose. FACTA (which amended FCRA) [FCRA and FACTA are discussed on pages 10-14] allows consumers who request a copy of their credit report to ask that the first five digits of their social security number not be included in the file.

The FTC may be able to exercise its authority under GLBA or Section 5 of the FTC Act (See pages 20-21) to pursue claims of unreasonable data security practices if it finds that social security numbers were being used as passwords for consumers to authenticate their identity. [See Solove and Hartzog, FTC and the New Common Law of Privacy, 114 Columb. L. Rev. 583 (2014).] Many states, including Minnesota, have passed laws that restrict the use and dissemination of social security numbers. [The Minnesota law appears on pages 88-91.] There is much variety in what the various state laws provide. Some states prohibit the request of a social security number to complete a transaction. Other states mandate a formal privacy policy for any entity that collects social security numbers.

The Drivers Privacy Protection Act (DPPA) [18 U.S.C. §§ 2721-2725]

The DPPA was enacted in 1994 and amended in 2000 to protect the privacy of personal information gathered by state departments or bureaus of motor vehicles. The DPPA was passed in reaction to the murder of an actress, Rebecca Schaeffer, who had been stalked by someone who had freely obtained her personal address from a publicly available state database that held drivers' records. The

DPPA allows plaintiffs to recover damages for each time the DPPA is violated.

In 2012 a former female police officer in Minnesota filed a lawsuit claiming that 100 fellow officers invaded her privacy when they looked up her driver's license photo in a database at least 400 times. She received a settlement payment of about $665,000 from several Minnesota cities where police officers had allegedly accessed her record.

Video Privacy Protection Act (VPPA) [18 U.S.C. § 2710]

The VPPA was passed after a newspaper obtained and published information about the video rental records of the Supreme Court nominee Robert Bork. The VPPA was enacted before video-streaming technology existed but has been found to apply to online services. The VPPA was also amended in 2013 to facilitate social media sharing of video viewing preferences when users consent to disclosure of information via the internet.

Other Federal Privacy Laws

Bank Secrecy Act, Pub. L. No. 91-508 requires banks to maintain reports of financial transaction as necessary to assist in government investigations.
Communications Decency Act, § 230(c) immunizes internet service providers from liability for content posted by others.

Privacy Act of 1974, 5 U.S.C. § 552a covers personal information maintained in government record systems.

Family Educational Rights and Privacy Act, 20 U.S.C. §§ 1221-1232 covers privacy of school records.

Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 subpoena or search warrant required for law enforcement to obtain financial records.

Foreign Intelligence Surveillance Act of 1978, 15 U.S.C. §§ 1801-1811 covers foreign intelligence gathering within the USA.

Privacy Protection Act of 1980, 42 U.S.C. § 2000 restricts government right to search and obtain work product of press and media.

Cable Communications Policy Act of 1984, 47 U.S.C. § 551 requires privacy protection for records maintained by cable companies.

Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a covers automated government investigations comparing computer files.

Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009 covers use of polygraphs by employers.

Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414 requires telecommunications providers to facilitate government interceptions of communications for surveillance purposes.

Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193 requires collection of personal information of all persons who obtain a new job for use in a database to help government officials track down parents delinquent in child support payments.

Identity Theft and Assumption Deterrence Act of 1998, 15 U.S.C. § 1028 makes it a crime to transfer or use fraudulent identification with the intent to commit unlawful activity.

Electronic Funds Transfer Act [Regulation E], protects consumers (but not businesses) from fraudulent transfers from bank accounts.

USA Patriot Act of 2001 amended a number of electronic surveillance and other laws to allow for easier access to information by government authorities.

USA Freedom Act of 2015 enacted surveillance reforms including the end of the National Security Agency's bulk collection of phone records and imposed other limits on the government collection of personal information.
Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801 makes it a crime to capture nude images of people when on federal property where the individuals would have a reasonable expectation of privacy.

The Securities and Exchange Commission (SEC) Safeguards Rule [Rule 30 of Regulation S-P] adopted by the SEC in 2000 and amended in 2005 requires every SEC registered investment adviser and other SEC registrants to adopt written policies and procedures that cover administrative, technical, and physical safeguards reasonably designed to 1) insure security and confidentiality of customer records and information, 2) protect against anticipated threats to security or integrity of customer records and information, and 3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Cybersecurity Information Sharing Act (CISA) was included in the budget and signed into law by President Obama on December 18, 2015. Its purpose is to prevent breaches of consumer data by offering legal protection to incentivize companies to share information about threats to their networks with the government and other businesses.

Judicial Redress Act Act was signed into law by President Obama on February 24, 2016. The Act grants non-U.S. citizens certain rights, including a private right of action for alleged privacy violations that occur in the U.S. The passing of this Act was an important step towards approval of the new EU-US Privacy Shield that would allow the transfer of personal information from the EU to the USA.

The National Institute Of Standards And Technology (NIST) Cybersecurity Framework

On February 12, 2014, NIST released the final version of its Framework for Improving Critical Infrastructure Cybersecurity ("NIST Framework"). The NIST Framework followed an Executive Order from the Obama Administration that called for its creation in February 2013. While use of the NIST Framework is voluntary, the federal government and others, including insurance companies, have been actively exploring ways to incentivize participation. The final version of the NIST Framework is the result of a year-long development process with significant public comment and working sessions with private sector and data security stakeholders. The NIST Framework can be used by a business as a risk management tool. It can help assess the risk of a cyber-attack, protect against attacks, and detect intrusions as they occur. According to NIST, the NIST Framework complements, but does not replace existing risk management processes and cybersecurity programs. It can, however, be used to assess and improve (if necessary) the already existing security practices.

The NIST Framework may become a de facto standard for determining whether or not a business has adequate data security safeguards in place. In the meantime, it is clearly worth considering the NIST Framework when adopting any extensive data security program since it may be viewed by some insurance companies as a prerequisite to coverage. Following the standards described in the NIST Framework might also serve as a defense against any FTC charge of inadequate data security.

Other Cybersecurity Standards. In addition to the NIST Framework, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have issued cybersecurity standards. These various cybersecurity standards enable organizations to practice safe security techniques and minimize successful cybersecurity attacks. They provide general outlines as well as specific techniques for implementing cybersecurity. In some cases obtaining certification under one of these standards might be a prerequisite to obtaining cybersecurity insurance. As noted above, it can also help defend against any FTC investigation and assertion of lax data security by a business.

Proposed Federal Legislation

In light of the massive data breach at Target and media attention on data privacy, there has been an increase in data privacy and security legislative initiatives at the federal level. Most of the efforts have been related to breach notification. Senator Patrick Leahy (D-VT) first introduced a version of his current legislative proposal nine years ago and has continued to reintroduce it but has yet to get it passed. Some of the current legislative initiatives include:

- Sen. Patrick Leahy's Personal Data Privacy and Security Act of 2014 (S. 1193) and its House counterpart introduced by Rep. Carol Shea-Porter (D-NH-01);
- Sen. Jay Rockefeller's (D-WV) Data Security and Breach Notification Act of 2014 (S. 1976);
- Sen. Thomas Carper's (D-DE) Data Security Act of 2014 (S. 1193);
- Sen. Pat Toomey's Data Security and Breach Notification Act (R-PA) (S. 1193); and
- Sen. Richard Blumenthal's Personal Data Protection and Breach Accountability Act (D-CT) (S. 1995).

While these bills vary in scope, definition and substance, they share a few common proposals. These proposals often require some form of baseline data security safeguards for organizations collecting, maintaining, using, or retaining certain types of personal information. They establish some form of federal breach notification law requiring businesses that maintain personal information to disclose a data breach, under certain circumstances, to affected consumers. Additionally, they also provide for explicit rulemaking authority to promulgate rules related to these data security safeguards and breach notification requirements.

The FTC is usually granted both rulemaking authority and enforcement abilities under these legislative proposals. The enforcement authority of the FTC could be expanded beyond the current "unfairness" test of the FTC Act. The FTC might also be granted the right to oversee comprehensive data security safeguards along with the ability to enforce federal breach notification laws. Civil penalties would also be a possibility if new legislation passed. In 2015 Congress once again failed to pass a comprehensive data breach notification law or any significant data privacy and security legislation. At least twelve different bills had been proposed in the House or Senate but remained stalled in committee.

The Data Security and Breach Notification Act (H.R. 1770) was one of the most high profile data breach notification bills and advanced further than most bills in 2015 but no action was taken beyond a mark up and amendment by the House Energy and Commerce Committee on April 15, 2015.

The proposed Data Security and Breach Notification Act of 2015 requires the Federal Trade Commission (FTC) to promulgate regulations requiring commercial entities, nonprofit and for-profit corporations, estates, trusts, cooperatives, and other specified entities that own or possess data containing personal information (covered entities), or that contract to have a third-party maintain or process such data for the entity, to implement information security policies and procedures for the treatment and protection of personal information.

The Act establishes procedures to be followed in the event of an information security breach. It requires a covered entity that discovers a breach to notify the FTC (unless the covered entity has already notified a federal entity designated by the Department of Homeland Security [DHS] to receive such information) and affected individuals. It sets forth requirements concerning such notification, including methods of notification and timeliness requirements. It allows an exemption from notification requirements if such entity reasonably concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. It establishes a presumption that there is no such risk for encrypted data.

The proposed legislation directs DHS to designate a federal entity that covered entities would be required to notify if a security breach involves 1) the personal information of more than 10,000 individuals, 2) a database containing the personal information of more than 1 million individuals, 3) federal government databases, or 4) the personal information of federal employees or contractors known to be involved in national security or law enforcement.
The Act requires the designated entity to provide each notice it receives to: the U.S. Secret Service; the Federal Bureau of Investigation; the FTC; the U.S. Postal Inspection Service, if mail fraud is involved; attorneys general of affected states; and appropriate federal agencies for law enforcement, national security, or data security purposes.

The proposed law sets forth enforcement provisions for the FTC, state attorneys general, and the Attorney General and establishes criminal penalties of a fine, imprisonment for up to five years, or both, for concealment of a security breach that results in economic harm of at least $1,000 to an individual.

Congress has had difficulty getting any legislation passed, which does not bode well for any comprehensive federal data privacy or breach notification laws. In the absence of a comprehensive federal data breach notification or other federal data privacy and security law, businesses will have to continue to consider the patchwork of state and federal laws discussed in this Guide.

PRIVACY AND THE EMPLOYMENT RELATIONSHIP

Technology And Social Media. Employers and employees are struggling to define the boundaries of appropriate employee use of technology, including social media, as well as appropriate employer monitoring and management of electronic data. In addition to concerns about employee productivity, the sophisticated electronic communication tools available to employees create new challenges for businesses to consider, including potential harm to reputation and brands, theft of trade secrets and other confidential information, and potential liability for employee behavior online. For example, an employer may be liable for an employee's online comments that are discriminatory or defamatory, even if the employee posts from a personal computer on personal time. Likewise, an employer may be liable for an employee's online endorsements of the employers' if the employee does not properly disclose her affiliation with the employer. In addition to current employee issues, many businesses are also increasingly using social media and other online technology tools to market their organization and to search for, recruit, and screen potential employees.

The legal obligations and rights of employers are continuing to evolve as technology changes. Nevertheless, employers can anticipate and plan for many of the legal risks associated with the use of technology in the workplace by applying existing laws to what we know about new electronic tools. Although new technological tools may ultimately be a "game changer" for employers, there are a number of practical steps that employers can take based on the law today to manage legal risk in this new frontier.

Discrimination Laws

Federal and Minnesota state law prohibit discrimination both in hiring and in employment on the basis of various legally protected class statuses, including race, color, creed, religion, national origin, sex, sexual orientation, marital status, disability, genetic information, receipt of public assistance, age, and military service. Most employers are aware of these restrictions and would never consider making a decision on the basis of an employee's protected class status. However, advances in technology have revolutionized both the hiring process as well as management of current employees. Employers should be aware of the ways in which discrimination laws could be impacted by these changes.

Protected Class Information. Employers generally may not ask applicants or employees about protected class status. In many cases, an employee's protected class status (such as race or gender) will be apparent to an employer. However, there are many circumstances where an employee's protected disability or religion would not be readily apparent to an employer. Resources available on the Internet—particularly social media—can complicate this delicate balance for employers.

In conducting an online search or reviewing social media sites of an applicant or an employee, an employer may learn information about the individual's protected class status. While employers in most cases are not prohibited from learning protected class information, they are prohibited from considering protected class information in making hiring and employment decisions. As such, having access to this information through online searches can increase the risk of a discrimination claim. Employers should therefore take special steps to wall off the individuals performing searches from the hiring or employment decision process to ensure that protected class information is not shared with or taken into account in the decision-making process.

Special Issues for Genetic Information. The ease in obtaining information about genetic information of employees also raises important employment law considerations for employers. The federal Genetic Information Nondiscrimination Act ("GINA") of 2008 provides that it is an unlawful employment practice for an employer or other covered entity to "request, require, or purchase genetic information with respect to an employee or family member of the employee." [See GINA § 202(a).] GINA defines "genetic information" broadly, providing that genetic information may include an individual's family medical history or an individual's own disclosure of a genetic condition. Minnesota state law also prohibits discrimination based on genetic information (See Minn. Stat. § 181.974).

Because genetic information may be obtained through an online or social media search, employers need to take care not to violate GINA in performing online applicant screening or gathering information about current employees. The Equal Employment Opportunity Commission's ("EEOC") final regulations implementing GINA provide some guidance on the acquisition of genetic information about applicants or employees via the internet and social media sites. According to the EEOC, an internet search on an individual that is likely to result in obtaining genetic information constitutes an unlawful "request" for genetic information, whereas acquisition of information from a social media platform where the employee has given the supervisor permission to access the profile is considered inadvertent. [See 29 C.F.R. § 1635.8.]

Protected Activity Laws

Various federal and state laws provide that employers may not take adverse action against applicants or employees based on certain legally protected activities. Accordingly, when online information about employees or applicants reveals protected activities by an individual, employers need to take care to ensure that they do

not consider or act on such information in making its hiring or employment decisions. The following is a summary of some of the laws that establish protected activities.

Protected Concerted Activity Under the National Labor Relations Act ("NLRA"). Several prohibitions found in the federal labor law – NLRA – apply to employers gathering information about applicants or employees through social media or other online searches. For example, Section 7 of the NLRA protects non-management employees' right to engage in concerted activity for mutual aid and protection and applies whether or not an employee is in a union. Section 7's rights are broad, encompassing outright union organizing and actions such as discussing or complaining about compensation or terms and conditions of employment. Section 8(a)(1) of the NLRA further provides that it is an unfair labor practice for an employer "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed by Section 7."

The NLRA prohibits employers from taking adverse action against an applicant or employee due to online information about the individual's protected Section 7 activities. The National Labor Relations Board ("NLRB" or the "Board"), which enforces the NLRA, has sided with employees who were terminated for off-the-clock comments made on Facebook, finding that the employees' comments were protected speech under the NLRA. In these and other "Facebook firing" cases, the Board has considered whether an employee is engaging in protected concerted activity or just airing an individual gripe, which is not protected. One way to tell the difference is to consider what happens after the initial post. If other employees express support or share the concern, and the conversation turns to "what should we do about this?" the employee's less-than-flattering initial post, along with the other employees' comments, are likely protected.

Not only is it unlawful for an employer to take adverse action against an applicant or employee because of Section 7 activities, the mere maintenance of a work policy or rule that chills Section 7 rights may amount to an unfair labor practice, even without evidence of policy enforcement. This is true even if the policy is not explicitly aimed at protected concerted activity. If it tends to chill employees' exercise of their Section 7 rights, it will be found unlawful.

The NLRB has put forth a two-step inquiry to determine whether a policy or work rule amounts to an unfair labor practice. The first step is to ask whether the rule explicitly restricts Section 7 rights. If it does, the policy is unlawful. If there is no explicit restriction, an employer should move to step two. In step two, an employer should ask three questions: 1) would employees reasonably construe the language to prohibit Section 7 activity?; 2) was the rule promulgated in response to union activity?; and 3) has the rule been applied to restrict the exercise of Section 7 rights? If the answer to any of these questions is yes, maintenance of the policy is an unfair labor practice.

The NLRB has focused its enforcement efforts on broad policies that could be construed to limit: 1) critical statements about the company or managers; 2) discussion of wages, hours, and other terms and conditions of employment; and 3) discussions with union representatives and coworkers. An employer thinking of developing a social media policy (or re-evaluating its current one), thus, has a number of factors to consider. First, the employer should determine whether a policy is necessary. Do the risks associated with having a policy outweigh the risks of going without one? If a policy is necessary, it is important to draft carefully and consult with an attorney. A lawful policy has clarifying language that restricts its scope to non-protected activity and includes examples of covered conduct that is clearly illegal or unprotected.

Lawful Consumable Products or Activities Laws. Employers that use the web or social media sites to screen applicants or to monitor employees might also uncover information about an individual engaged in alcohol use, smoking, or other lawful activities that an employer might disagree with or prefer the individual not do. However, Minnesota law prohibits employers from refusing to hire an applicant or taking adverse action against an employee for the consumption of lawful products, such as alcohol or tobacco, away from work during nonworking hours. [See Minn. Stat. § 181.938, Subd. 2.] Many other states have similar laws, and some even prohibit adverse action based on other lawful activities, such as an individual's appearance, political affiliations, or other factors. The Minnesota law provides exceptions if a restriction on consumption of lawful consumable products is based on a bona fide occupational requirement or is necessary to avoid a conflict of interest with any responsibilities owed by the employee to the employer. However, employers should act cautiously before taking any action against an applicant or employee on the basis of these narrow exceptions.

Retaliation Laws. Similarly, employers may face legal risk for taking action based on information that could be construed as asserting rights under employment laws. A number of federal and state employment laws (including but not limited to anti-discrimination, wage and hour, leave, and worker's compensation laws) prohibit retaliation against an individual for asserting rights under the law, assisting someone else to assert their rights, or participating in an investigation or legal proceeding. Just as employers may learn of whistleblowing through online sources, employers also may learn of other protected activities that an individual may claim gives rise to anti-retaliation rights. An employer who learns of such activities through online sources must act carefully to avoid engaging in unlawful retaliation.

Applicant Screening Laws

Surveys and informal data suggest that employers are increasingly using the web and social media sites to both identify and recruit desirable job candidates, as well as to weed out less desirable candidates. Just as there are legal limitations to screening applicants through more traditional methods, legal issues are likely to arise when applicants are screened online. The following section summarizes some of the special applicant screening laws that may be triggered by online screening of job applicants.

Negligent Hiring. In Minnesota, an employer can be liable for negligent hiring if it "places a person with known propensities, or propensities which should have been discovered by reasonable investigation, in an employment position in which, because of the circumstances of employment, it should have been foreseeable that the hired individual posed a threat of injury to others." *Ponticas v. Investments*, 331 N.W.2d 907, 911 (Minn. 1983). Employers have a "duty to exercise reasonable care in view of all the circumstances in hiring individuals who, because of the employment, may pose a threat of injury to members of the public." *Ponticas*, 331 N.W.2d at 911. This has come to be known as a sliding scale duty, requiring the employer to decide how much investigation is necessary based on the nature of the position. Because of this potential liability, it is sometimes appropriate for an employer, depending on their business and a particular position's duties, to do a more thorough screening of an applicant's background to try to ensure that the individual does not pose a safety risk or other risks to the business or third parties.

Historically, the doctrine of negligent hiring has resulted in employers considering whether it is appropriate to run a criminal background check on applicants. As social media becomes more common, it is possible, although not yet known, whether the scope of an employer's duty to investigate job applicants for safety risks may extend to conducting social media or other online searches.

Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, et seq., and State Background Check Laws. When an employer conducts a background search on an applicant entirely in-house using only the employer's staff, background check laws generally do not apply. However, when an employer uses an outside entity for a fee to obtain a criminal background check or to otherwise obtain a background report or investigate an applicant's background for employment purposes, the employer must comply with background check laws, including FCRA and any applicable state law. FCRA establishes a number of legal requirements for obtaining a background report, including notice, consent, and various procedural steps that must be followed before acting on background check information to withdraw a job offer. Although the legal landscape of online searches is still evolving, it is likely that an employer who pays an outside entity or uses a fee-based online service to obtain online background information on an applicant must comply with FCRA and any applicable state background check laws.

While background checks arise most often in the hiring context, employers sometimes pay outside entities to obtain criminal background information about or to otherwise investigate a current employee. In these situations, FCRA and state background check laws may still apply. [See discussion of FCRA on pages 10-14.]

Disparate Impact Claims. In recent years, the EEOC announced its E-RACE Initiative ("Eradicating Racism and Colorism in Employment") which is aimed at reducing race discrimination in hiring. The EEOC has sued employers in several high-profile cases for policies and practices that the EEOC believes lead to systemic discrimination in hiring. Although the cases so far have involved employer use of background checks, the EEOC has also announced its intent to pursue employers that require the use of video resumes or other technological application processes. According to the EEOC, these practices lead to "disproportionate exclusion of applicants of color who may not have access to broadband-equipped computers

or video cameras." Given the EEOC's very public statements about technology and disparate impact claims, employers should take care to ensure that their hiring policies and practices in hiring do not result in systemic discrimination.

In 2012, the EEOC issued guidance on employers' use of criminal history information to exclude individuals from employment. [See http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm.] Because persons of color are arrested and convicted at disproportionate rates, excluding individuals from employment based on a criminal record can be unlawful race discrimination under Title VII of the Civil Rights Act of 1964. To be lawful under Title VII, an employment exclusion must be based on proven criminal conduct and must be job-related and consistent with business necessity. In light of the EEOC's new guidance, employers should tread carefully and consult with legal counsel before excluding someone from employment based on criminal history information, including information found online.

In addition to following the above-described guidelines, employers must comply with Minnesota's "Ban the Box" law, which restricts the timing of employer's inquiries into an applicant's criminal past. [See Minn. Stat. §§ 364.021, 364.06, 364.09.] Minnesota law requires employers to wait until a job applicant has been selected for an interview, or a conditional offer of employment has been extended, before inquiring about an applicant's criminal history or conducting a criminal background check.

Employee Privacy Considerations

Where an employer provides employees with technology resources or monitors employees through its own technology, employees may argue that they have a right to privacy in the technology or conduct at issue. Privacy issues may also result from the online conduct of employees outside of the employer's network or technology

resources. Because of the public nature of the web and many social media sites, privacy law may, at first blush, seem inapplicable. However, the law regarding online privacy rights is unsettled, and some of the few cases involving the issue have raised the possibility of legal risks for employers, at least when online data comes from a website with privacy restriction settings. While privacy law is still unsettled and evolving, the following is a summary of some of the legal issues that might arise in the employment context.

Common Law Invasion of Privacy. Minnesota recognizes invasion of an individual's privacy as a tort action. See *Bodah v. Lakeville Motor Express, Inc.*, 663 N.W.2d 550 (Minn. 2003). The most common privacy claims raised by employees against employers are intrusion upon seclusion and publication of private facts. To prove either type of privacy claim, however, the plaintiff must first demonstrate a reasonable expectation of privacy. When information is publicly available on the Internet, it may be difficult for an individual to establish any reasonable expectation of privacy in the information. It is less clear, however, whether individuals might claim some reasonable expectation of privacy in social media sites with some privacy settings, such as Facebook, which allows users to limit access to the site to only individuals that have been approved by the user. In a case involving a restricted MySpace chat room used by employees, the court declined to recognize an invasion of privacy claim where a supervisor accessed a restricted site using a password given by an employee participating in the site. [See *Pietrylo v. Hillstone Restaurant Group*, No. 06-5754, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009).] However, the employer was still found to have violated the Stored Communications Act, [See pages 47 and 69-70.]

In order to establish that employees have no reasonable expectation of privacy in the activity or technology at issue, employer's policies should clearly state that the resources provided to employees are provided for the benefit of the business and that employees do not have any expectation of privacy in the specific conduct. The policy

should also reserve the right to monitor employee's email and other uses of its own technology resources. With these policies in place, employers are much less vulnerable to an invasion of privacy claim.

State Wiretapping Laws. Minnesota statutory law prohibits the interception and disclosure of wire, electronic, or oral communications. Minn. Stat. § 626A.02, Subd. 1. Any interception of these forms of communication will violate the law unless an exemption applies. However, an exemption applies if one of the parties to the communication has given prior consent to such interception. Minn. Stat. §626A.02, Subd. 2(d). [See pages 101-104.]

To assert this exemption to Minnesota's wiretapping law, employers that wish to monitor employee communications with outside parties must be able to demonstrate that the employee in question consented to the monitoring of those communications. To do so, employers should, at a minimum, maintain policies that explicitly state that employees have no expectation of privacy in communications using employer-provided communication technologies. Employers should also document the employees' written consent in the form of an acknowledgement that the employee has received and understands the employer's policy, including that the employer has the right to monitor such communications.

Surveillance and Creating an Impression of Surveillance. Employers may also be liable for an unfair labor practice under Section 8(a)(1) of the NLRA for engaging in the surveillance of, or creating an impression of surveillance of, union activity. In *Magna International, Inc.*, 7-CA-43093(1), 2001 NLRB LEXIS 134 (Mar. 9, 2001), for example, an administrative law judge held that it was a violation of Section 8(a)(1) of the NLRA for a supervisor to tell an employee that he liked a picture of her the day after the photo was posted to a union blog, because this suggested to the employee that her union activities were being monitored. Employers faced with organizing activity should be mindful of this complicated and often surprising body of the labor law.

Special Concerns for Public Employers. In addition to the above privacy laws, public employers are also subject to the Fourth Amendment of the United States Constitution. The Fourth Amendment protects public employees from unreasonable searches and seizures, and this prohibition extends to electronic information. In 2010, the United States Supreme Court decided the case of *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), a case that raised the question of whether law enforcement employees had a reasonable expectation of privacy in text messages sent on employer provided devices. In *Quon*, the employer had a written policy allowing inspection of messages, but in practice did not regularly monitor messages. Although the Supreme Court declined to find that the employees had a reasonable expectation of privacy in the messages, the court held that the search was reasonable under the Fourth Amendment because the search was motivated by a legitimate work-related purpose and was not excessive in scope. Public employers must be mindful of this additional constitutional responsibility.

Federal Laws Applicable To Electronic Communications and Data

In addition to privacy laws, federal electronic communication laws may also be implicated by an employer's search or review of employees' use of technology. These laws include the Electronic Communications Privacy Act, [18 U.S.C. § 2510], et seq. the Stored Communications Act (SCA), and the Computer Fraud and Abuse Act (CFAA). These laws are briefly summarized below and covered in this Guide on page 45.

The Electronic Communications Privacy Act (ECPA or the "Wiretap Act")

The federal Wiretap Act prohibits the unlawful "interception" of an electronic communication contemporaneously with the communication being made. As such, employers that monitor and intercept employee's online communications through social media or other online sources could, depending on the circumstances, be liable under the Act. Most employers do not, however, monitor employee communications in real time as they are occurring. If there is no real-time, contemporaneous "interception" of an electronic communication, the Wiretap Act most likely does not apply. [See discussion of ECPA on pages 46-47.]

The Stored Communications Act (SCA), [18 U.S.C. § 2701, et seq.]

The SCA prohibits the knowing or intentional unauthorized access to "a facility through which an electronic communication service is provided." [18 U.S.C. §§ 2701, 2707.] This includes unauthorized access to a password-protected email account or social networking site. Key exceptions exist, however, if the person accessing the communication is the provider of the service, a user of the service and the communication is from or intended for that user, or has been granted access to the site by an authorized user. [18 U.S.C. § 2701(c)(2).]

At least three notable cases have applied the SCA to electronic communications. In *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), the Ninth Circuit Court of Appeals was confronted with a situation where the employer gained access to the site by submitting an eligible employee's name and creating a password to enter, after accepting terms and conditions that prohibited viewing by management. According to the court, this conduct alleged by the plaintiff was sufficient to bring a claim under the SCA.

In the *Pietrylo* case discussed above (see page 66), the District Court of New Jersey upheld a jury verdict imposing liability against an employer under the SCA. [2009 U.S. Dist. LEXIS 88702.] The Court found sufficient evidence that a company supervisor accessed the password- protected employee chat room with a password provided by an employee coerced into giving access.

Finally, in the *Quon* case mentioned above, the Ninth Circuit Court of Appeals held that the employer and wireless provider violated the SCA by viewing the content of text messages sent by employees through a third-party pager service, even though the employer paid for the service. The Supreme Court declined to hear the wireless provider's challenge to this ruling. [*USA Mobility Wireless, Inc. v. Quon*, 130 S. Ct. 1011 (2009).] [See discussion of SCA on page47.]

The Computer Fraud and Abuse Act (CFAA), [18 U.S.C. § 1030, et seq.]

The CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access." The CFAA provides for both criminal prosecution and civil actions for violations. Although the CFAA may apply against employers in some circumstances, the CFAA is far more often a tool for employers to pursue claims against employees who abuse their access to the employer's computer network. For example, an employer may pursue claims against employees who abuse their access to confidential information in violation of the employer's policies. *See United States v. Rodriguez*, 627 F.3d 1372 (11th Cir. 2010).
[See discussion of CFAA on page 45.]

References and Recommendations

The popular business social networking site LinkedIn.com allows employees to ask their "connections" to provide recommendations for them. Most employers, however, due to defamation, privacy, and other legal considerations, typically provide very limited reference information on former employees. *See, e.g., Randi W. v. Muroc Jt. Unified School Dist.*, 14 Cal. 4th 1066 (1997) (finding liability where an employer provided positive references but failed to disclose complaints of sexual misconduct). Employers should make sure that employees are aware that any limited reference policies that the employer may have in place extend to providing references on social media sites, such as LinkedIn.

Safeguarding Confidential and Proprietary Information

In today's knowledge-based economy, confidential information and electronic systems are often the most valuable resources of a company. Employees who have access to this information or create the employer's electronic systems during the course of their employment can do a great deal of harm to a company if they disclose this information or attempt to take it with them when they leave their employment. Both state and federal laws provide guidelines for employers and employees in this important arena. These laws are summarized below.

Information Security. Employers have a responsibility to keep certain information confidential. For example, employee personnel records often include information that employers must keep confidential, such as employee medical records, drug testing records, social security numbers, and credit reports. Employees may also have access to similar confidential information about customers, clients, or donors that the employer is obligated by contract or law to keep confidential.

Employers should adopt systems and policies to address the security of this confidential information. If employees have access to particularly sensitive information, employers should also consider requiring those employees to sign agreements acknowledging the duty to keep such information secure and providing specific guidelines on appropriate practices for keeping that information secure.

Confidential and Proprietary Information. The Uniform Trade Secrets Act, codified in Minnesota at Minn. Stat. § 325C.01, et seq., prohibits misappropriation of trade secrets, and provides employers with the right to injunctive relief and actual damages in the event of a threatened or actual misappropriation. The law defines a trade secret as information that derives independent economic value from not being generally known by others, so long as the employer makes reasonable efforts to maintain its secrecy.

Employers should also consider entering into written agreements with employees to either broaden the scope of protected information or simply to provide more information to employees about what the employer considers to be confidential. Although such agreements cannot stop employees from breaching their obligations by publishing information online, the agreements will at least bolster the employer's case for injunctive relief and damages in the event of such a disclosure.

Employer Policies and Practices

A well-crafted technology and social media policy that balances company needs and concerns against employees' legal rights is an important tool in managing competing legal risks.

Some of the business and legal risks that an employer should address in a technology and social media policy include:

- ***Covered technology and devices***: Employers should consider whether the policy will extend only to employer-paid or provided devices or whether the employer may lawfully and should extend the policy to personally-owned devices used for work purposes. The law is still evolving in this area, and it is not clear whether employers have the legal right in all jurisdictions to search an employee's personal device or personal email account on a company or personally-owned device. However, having a clearly-worded policy can improve an employer's legal position in arguing that it has the right to access any technology devices used by an employee for work purposes.

- ***Privacy considerations***: Due to the privacy issues discussed above, a policy should include an express warning that the employer retains the right to monitor and review the use of and content on any technology and devices covered by the policy. As discussed above, however, there have been court decisions finding employers liable for improperly accessing or using online content, particularly where the content was on a website with restricted privacy settings, such as Facebook.com. As such, employers should take care to ensure they lawfully access online content, and they should consult with counsel as appropriate to ensure compliance.

- ***Permissible and impermissible uses:*** The policy should explain the permissible and impermissible uses of technology and social media. Items to address might include, for example, personal use of technology on work time, employees' obligation not to use technology to engage in unlawful behavior, the need to protect confidential or trade secret information, and the need to respect others' intellectual property rights. An employer may also want to prohibit employees from engaging in any company-related blogging, tweeting or the like without express written permission of the company to engage in such social networking activities on behalf of the business.

- ***Lawfully Protected Employee Activity:*** In setting out any prohibited conduct in a workplace policy, employers must take care to balance the employer's needs against employees' legal rights. As discussed above, a job applicant's or employee's use of technology and online content may be legally protected by discrimination, anti-retaliation, lawful consumable products, lawful activity, labor law, or other laws. As such, an employer should be cautious in rejecting a job candidate or disciplining or terminating an employee for online activity to ensure that adverse action is not taken based on legally-protected activities by the individual.

- ***Photography and Recording***: Smartphones and other mobile devices make it far easier than in the past for employees to secretly record conversations at work or to take unauthorized photographs or videos that might be widely disseminated on the internet and go "viral." Depending on the employer's business and its unique risks, a technology policy might include language prohibiting the use of devices to make recordings or take photographs or videos. Again, however, an employer should consult with counsel to ensure that any such language does not run afoul of individuals' Section 7 labor law rights or other employment law rights.

- ***Return of Company Data***: An employer should make clear that all company data, including any electronic data stored on an employee's personally-owned devices, such as a smartphone, tablet, or personal computer, must be returned to the company upon request or when an employee leaves employment. An employer that has a BYOD (bring your own device) approach to workplace technology should consider including language in a technology policy stating that employees agree to turn over their personal devices to the company to permit the company to wipe any company data from the device. Many companies have the capability to remotely cut off access to company technology and to remotely wipe company-owned or employee-owned devices.

STATE DATA PRIVACY AND SECURITY LAWS

As noted above there is no single comprehensive federal data privacy and security law, so a Minnesota business may need to become familiar not only with the relevant federal laws discussed above and the applicable Minnesota state laws, but also other state laws and even international laws that may apply. In some cases the federal law may preempt the state laws and in other cases the state law may be even more restrictive than the federal law.

With more and more data crossing the border and ecommerce creating global businesses out of Minnesota-based companies, the legal landscape is immense. States have passed laws related to wiretapping and electronic surveillance, use and disclosure of medical and genetic information, identity theft, use of social security numbers, and other laws governing the use of personal information.

This patchwork of laws has become of particular concern when it comes to data breach notification. Almost every state has enacted some form of legislation requiring notification of security breaches involving personal information.

California has been far and away the most active in its efforts to enact laws protecting the privacy of its citizens and to enforce these laws. California's Office of Information Security and Privacy Protection, and the California Attorney General have been aggressive in promoting and protecting the privacy rights of California consumers.

Massachusetts has become known as the state with the strongest data security laws and regulations.

Wisconsin has an Office of Privacy Protection dedicated to educating consumers on how to protect against identity theft and consumer protection. [See also Wisconsin's Fair Information Practices Act, Wisc. Stat. Ann. § 19.62]

The Minnesota legislature has seen several data privacy and security bills introduced including a bill to create a Data Practices and Personal Data Privacy Legislative Commission. This commission would provide legislators with more expertise on privacy issues. Another bill would have required retailers to notify consumers of a data breach within 48 hours of discovery, and offer free credit counseling, as well as a $100 gift card. None of these legislative initiatives passed.

In this section of the Guide we first cover Minnesota laws related to data privacy and security followed by the laws of California and Massachusetts - two states currently with the most expansive data privacy and security laws. Many businesses have implemented data privacy practices and procedures to comply with the laws of these two states.

Minnesota Data Privacy and Security Laws

Current Minnesota data privacy related statutes include the following:

Minn. Stat. § 325M.01 Internet Service Providers

Minn. Stat. § 609.527 Identity Theft

Minn. Stat. § 325E.61 Data Breach Notification

Minn. Stat. § 13.055 Data Breach Notification (Government Agencies)

Minn. Stat. § 13.0 Minnesota Government Data Practices Act

Minn. Stat. § 13.15 Government Websites

Minn. Stat. § 325E.64 Plastic Card Security Act

Minn. Stat. § 325E.59 Social Security Numbers

Minn. Stat. § 626A.02 Wiretap law

Internet Service Providers [Minn. Stat. § 325M.01]

Minnesota imposes confidentiality requirements on internet service providers ("ISPs") with respect to their subscribers. An ISP is required to maintain the confidentiality of its customers' personally identifiable information. According to this Minnesota law, "personally identifiable information" means information that identifies 1) a consumer by physical or electronic address or telephone number; 2) a consumer as having a requested or obtained specific materials or services from an ISP; 3) internet or online sites visited by a consumer; or 4) any of the contents of a consumer's data storage devices.

A consumer who prevails in an action for a violation of this statute is entitled to $500 or actual damages, whichever amount is greater. [Minn. Stat. § 325M.07.] One of the problems under many data privacy laws is the ability to quantify and prove damages.

The full text of the statute appears below.

325M.01 DEFINITIONS.

Subdivision 1. **Scope.**

The terms used in this chapter have the meanings given them in this section.

Subd. 2. **Consumer.**

"Consumer" means a person who agrees to pay a fee to an Internet service provider for access to the Internet for personal, family, or household purposes, and who does not resell access.

Subd. 3. **Internet service provider.**

"Internet service provider" means a business or person who provides consumers authenticated access to, or presence on, the Internet by means of a switched or dedicated telecommunications channel upon which the provider provides transit routing of Internet Protocol (IP) packets for and on behalf of the consumer. Internet service provider does not include the offering, on a common carrier basis, of telecommunications facilities or of telecommunications by means of these facilities.

Subd. 4. **Ordinary course of business.**

"Ordinary course of business" means debt-collection activities, order fulfillment, request processing, or the transfer of ownership.

Subd. 5. **Personally identifiable information.**

"Personally identifiable information" means information that identifies:

(1) a consumer by physical or electronic address or telephone number;

(2) a consumer as having requested or obtained specific materials or services from an Internet service provider;

(3) Internet or online sites visited by a consumer; or

(4) any of the contents of a consumer's data-storage devices.

325M.02 WHEN DISCLOSURE OF PERSONAL INFORMATION PROHIBITED.

Except as provided in sections 325M.03 and 325M.04, an Internet service provider may not knowingly disclose personally identifiable information concerning a consumer of the Internet service provider.

325M.03 WHEN DISCLOSURE OF PERSONAL INFORMATION REQUIRED.

An Internet service provider shall disclose personally identifiable information concerning a consumer:

(1) pursuant to a grand jury subpoena;

(2) to an investigative or law enforcement officer as defined in section 626A.01, subdivision 7, while acting as authorized by law;

(3) pursuant to a court order in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by other means;

(4) to a court in a civil action for conversion commenced by the Internet service provider or in a civil action to enforce collection of unpaid subscription fees or purchase amounts, and then only to the extent necessary to establish the fact of the subscription delinquency or purchase agreement, and with appropriate safeguards against unauthorized disclosure;

(5) to the consumer who is the subject of the information, upon written or electronic request and upon payment of a fee not to exceed the actual cost of retrieving the information;

(6) pursuant to subpoena, including an administrative subpoena, issued under authority of a law of this state or another state or the United States; or

(7) pursuant to a warrant or court order.

325M.04 WHEN DISCLOSURE OF PERSONAL INFORMATION PERMITTED; AUTHORIZATION.

Subdivision 1. **Conditions of disclosure.**

An Internet service provider may disclose personally identifiable information concerning a consumer to:

(1) any person if the disclosure is incident to the ordinary course of business of the Internet service provider;

(2) another Internet service provider for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the Internet service provider; except that the recipient may further disclose the personally identifiable information only as provided by this chapter;

(3) any person with the authorization of the consumer; or

(4) as provided by section 626A.27.

Subd. 2. **Authorization.**

The Internet service provider may obtain the consumer's authorization of the disclosure of personally identifiable information in writing or by electronic means. The request for authorization must reasonably describe the types of persons to whom personally identifiable information may be disclosed and the anticipated uses of the information. In order for an authorization to be effective, a contract between an Internet service provider and the consumer must state either that the authorization will be obtained by an affirmative act of the consumer or that failure of the consumer to object after the request has been made constitutes authorization of disclosure. The provision in the contract must be conspicuous. Authorization may be obtained in a manner consistent with self-regulating guidelines issued by representatives of the Internet service provider or online industries, or in any other manner reasonably designed to comply with this subdivision.

325M.05 SECURITY OF INFORMATION.

The Internet service provider shall take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information. The Internet service provider is not liable for actions that would constitute a violation of section 609.88, 609.89, or 609.891, if the Internet service provider does not participate in, authorize, or approve the actions.

325M.06 EXCLUSION FROM EVIDENCE.

Except for purposes of establishing a violation of this chapter, personally identifiable information obtained in any manner other than as provided in this chapter may not be received in evidence in a civil action.

325M.07 ENFORCEMENT; CIVIL LIABILITY; DEFENSE.

A consumer who prevails or substantially prevails in an action brought under this chapter is entitled to the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded to a party awarded damages for a violation of this section. No class action shall be brought under this chapter.

In an action under this chapter, it is a defense that the defendant has established and implemented reasonable practices and procedures to prevent violations of this chapter.

325M.08 OTHER LAW.

This chapter does not limit any greater protection of the privacy of information under other law, except that:

(1) nothing in this chapter limits the authority under other state or federal law of law enforcement or prosecuting authorities to obtain information; and

(2) if federal law is enacted that regulates the release of personally identifiable information by Internet service providers but does not preempt state law on the subject, the federal law supersedes any conflicting provisions of this chapter.

325M.09 APPLICATION.

This chapter applies to Internet service providers in the provision of services to consumers in this state.

Identity Theft/Phishing
[Minn. Stat. § 609.527, Subd. 2.]

Minnesota makes it a crime to transfer, possess, or use an identity that is not one's own, with the intent to commit, aid, or abet any unlawful activity, as well as the electronic use of a false pretense to obtain another's identity, often referred to as "phishing." [See Minn. Stat. § 609.527, Subd. 5a.]

In a typical phishing scheme, a perpetrator uses fraudulent email messages that appear to come from legitimate businesses. Authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers, passwords, credit card numbers, and social security numbers. It is a crime to use a false pretense in an email or web page to trick a victim into divulging his or her personal information. A "false pretense" is defined as "any false, fictitious, misleading, or fraudulent information or pretense or pretext depicting or including or deceptively similar to the name, logo, website address, email address, postal address, telephone number, or any other identifying information of a for-profit or not-for-profit business or organization or of a government

agency, to which the user has no legitimate claim of right." [See Minn. Stat. § 609.527, subd. 1(c).]

Identity Theft Penalties Under Minnesota Law. The penalties for identity theft range from a misdemeanor to a 20-year felony. The penalties are based upon the amount of loss incurred, the number of direct victims involved, or the related offense. Loss is defined in the Minnesota statute as the value obtained and the expenses incurred as a result of the crime.

The full text of the statute appears below.

609.527 IDENTITY THEFT.

Subdivision 1. **Definitions.**

(a) As used in this section, the following terms have the meanings given them in this subdivision.

(b) "Direct victim" means any person or entity described in section 611A.01, paragraph (b), whose identity has been transferred, used, or possessed in violation of this section.

(c) "False pretense" means any false, fictitious, misleading, or fraudulent information or pretense or pretext depicting or including or deceptively similar to the name, logo, Website address, email address, postal address, telephone number, or any other identifying information of a for-profit or not-for-profit business or organization or of a government agency, to which the user has no legitimate claim of right.

(d) "Identity" means any name, number, or data transmission that may be used, alone or in conjunction with any other information, to identify a specific individual or entity, including any of the following:

(1) a name, Social Security number, date of birth, official government- issued driver's license or identification number, government passport number, or employer or taxpayer identification number;

(2) unique electronic identification number, address, account number, or routing code; or

(3) telecommunication identification information or access device.

(e) "Indirect victim" means any person or entity described in section 611A.01, paragraph (b), other than a direct victim.

(f) "Loss" means value obtained, as defined in section 609.52, subdivision 1, clause (3), and expenses incurred by a direct or indirect victim as a result of a violation of this section.

(g) "Unlawful activity" means:

(1) any felony violation of the laws of this state or any felony violation of a similar law of another state or the United States; and

(2) any nonfelony violation of the laws of this state involving theft, theft by swindle, forgery, fraud, or giving false information to a public official, or any nonfelony violation of a similar law of another state or the United States.

(h) "Scanning device" means a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on a computer chip or magnetic strip or stripe of a payment card, driver's license, or state- issued identification card.

(i) "Reencoder" means an electronic device that places encoded information from the computer chip or magnetic strip or stripe of a payment card, driver's license, or state-issued identification card, onto the computer chip or magnetic strip or stripe of a different payment card, driver's license, or state-issued identification card, or any electronic medium that allows an authorized transaction to occur.

(j) "Payment card" means a credit card, charge card, debit card, or any other card that:

(1) is issued to an authorized card user; and

(2) allows the user to obtain, purchase, or receive credit, money, a good, a service, or anything of value.

Subd. 2. **Crime**.

A person who transfers, possesses, or uses an identity that is not the person's own, with the intent to commit, aid, or abet any unlawful activity is guilty of identity theft and may be punished as provided in subdivision 3.

Subd. 3. **Penalties.**

A person who violates subdivision 2 may be sentenced as follows:

(1) if the offense involves a single direct victim and the total, combined loss to the direct victim and any indirect victims is $250 or less, the person may be sentenced as provided in section 609.52, subdivision 3, clause (5);

(2) if the offense involves a single direct victim and the total, combined loss to the direct victim and any indirect victims is more than $250 but not more than $500, the person may be sentenced as provided in section 609.52, subdivision 3, clause (4);

(3) if the offense involves two or three direct victims or the total, combined loss to the direct and indirect victims is more than $500 but not more than $2,500, the person may be sentenced as provided in section 609.52, subdivision 3, clause (3);

(4) if the offense involves more than three but not more than seven direct victims, or if the total combined loss to the direct and indirect victims is more than $2,500, the person may be sentenced as provided in section 609.52, subdivision 3, clause (2); and

(5) if the offense involves eight or more direct victims; or if the total, combined loss to the direct and indirect victims is more than $35,000; or if the offense is related to possession or distribution of pornographic work in violation of section 617.246 or 617.247; the person may be sentenced as provided in section 609.52, subdivision 3, clause (1).

Subd. 4. **Restitution; items provided to victim.**

(a) A direct or indirect victim of an identity theft crime shall be considered a victim for all purposes, including any rights that accrue under chapter 611A and rights to court-ordered restitution.

(b) The court shall order a person convicted of violating subdivision 2 to pay restitution of not less than $1,000 to each direct victim of the offense.

(c) Upon the written request of a direct victim or the prosecutor setting forth with specificity the facts and circumstances of the offense in a proposed order, the court shall provide to the victim, without cost,

a certified copy of the complaint filed in the matter, the judgment of conviction, and an order setting forth the facts and circumstances of the offense.

Subd. 5. **Reporting.**

(a) A person who has learned or reasonably suspects that a person is a direct victim of a crime under subdivision 2 may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction where the person resides, regardless of where the crime may have occurred. The agency must prepare a police report of the matter, provide the complainant with a copy of that report, and may begin an investigation of the facts, or, if the suspected crime was committed in a different jurisdiction, refer the matter to the law enforcement agency where the suspected crime was committed for an investigation of the facts.

(b) If a law enforcement agency refers a report to the law enforcement agency where the crime was committed, it need not include the report as a crime committed in its jurisdiction for purposes of information that the agency is required to provide to the commissioner of public safety pursuant to section 299C.06.

Subd. 5a. **Crime of electronic use of false pretense to obtain identity.**

(a) A person who, with intent to obtain the identity of another, uses a false pretense in an email to another person or in a Web page, electronic communication, advertisement, or any other communication on the Internet, is guilty of a crime.

(b) Whoever commits such offense may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $10,000, or both.

(c) In a prosecution under this subdivision, it is not a defense that:

(1) the person committing the offense did not obtain the identity of another;

(2) the person committing the offense did not use the identity; or

(3) the offense did not result in financial loss or any other loss to any person.

Subd. 5b. **Unlawful possession or use of scanning device or reencoder.**

(a) A person who uses a scanning device or reencoder without permission of the cardholder of the card from which the information is being scanned or reencoded, with the intent to commit, aid, or abet any unlawful activity, is guilty of a crime.

(b) A person who possesses, with the intent to commit, aid, or abet any unlawful activity, any device, apparatus, equipment, software, material, good, property, or supply that is designed or adapted for use as a scanning device or a reencoder is guilty of a crime.

(c) Whoever commits an offense under paragraph (a) or (b) may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $10,000, or both.

Subd. 6. **Venue.**

Notwithstanding anything to the contrary in section 627.01, an offense committed under subdivision 2, 5a, or 5b may be prosecuted in:

(1) the county where the offense occurred;

(2) the county of residence or place of business of the direct victim or indirect victim; or

(3) in the case of a violation of subdivision 5a or 5b, the county of residence of the person whose identity was obtained or sought.

Subd. 7. **Aggregation.**

In any prosecution under subdivision 2, the value of the money or property or services the defendant receives or the number of direct or indirect victims within any six-month period may be aggregated and the defendant charged accordingly in applying the provisions of subdivision 3; provided that when two or more offenses are committed by the same person in two or more counties, the accused may be prosecuted in any county in which one of the offenses was committed for all of the offenses aggregated under this subdivision.

Minnesota Data Breach Notification [Minn. Stat. §§ 325E.61 and 13.055]

Any person or business that maintains data that includes personal information that the person or business does not own must

notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Definition of Personal Information. For Minnesota residents personal information includes first name or first initial and last name plus one or more of the following: social security number, driver's license number or state issued ID card number, account number, credit card number or debit card number combined with any security code, access code, PIN, or password needed to access an account and generally applies to computerized data that includes personal information. It does not include encrypted data.

Definition of Breach. Breach of the "security system" means any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by the person or business.

Content of Notice. There is no specific requirement as to content of the notification.

Timing. The notification requirement is triggered upon discovery or notification of a breach of the security of the system. Notification must be in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

In the event of a breach affecting over 500 people (1,000 for state agencies), consumer reporting agencies (CRA) must be notified within 48 hours and must be informed of the timing, distribution, and content of the notices sent to Minnesota residents.

Penalty. The Minnesota Attorney General may enforce this law by seeking injunctive relief and/or a civil penalty not to exceed $25,000.

Exemptions. An exemption from this notification statute may apply to an entity that is otherwise covered by a federal law such as the GLBA or HIPAA. As noted above, encrypted information is exempt but the Minnesota statute does not define encryption.

The full text of the Minnesota notification statute appears below.

325E.61 DATA WAREHOUSES; NOTICE REQUIRED FOR CERTAIN DISCLOSURES.

Subdivision 1. **Disclosure of personal information; notice required.**

(a) Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

(b) Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section and section 13.055, subdivision 6, may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

(d) For purposes of this section and section 13.055, subdivision 6, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section and section 13.055, subdivision 6, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

(1) Social Security number;

(2) driver's license number or Minnesota identification card number; or

(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section and section 13.055, subdivision 6, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section and section 13.055, subdivision 6, "notice" may be provided by one of the following methods:

(1) written notice to the most recent available address the person or business has in its records;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

(i) email notice when the person or business has an email address for the subject persons;

(ii) conspicuous posting of the notice on the Website page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media.

(h) Notwithstanding paragraph (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section and section 13.055, subdivision 6, shall be deemed to be in compliance with the notification requirements of this section and section 13.055, subdivision 6, if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Subd. 2. **Coordination with consumer reporting agencies.**

If a person discovers circumstances requiring notification under this section and section 13.055, subdivision 6, of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Subd. 3. **Waiver prohibited**.

Any waiver of the provisions of this section and section 13.055, subdivision 6, is contrary to public policy and is void and unenforceable.

Subd. 4. **Exemption**.

This section and section 13.055, subdivision 6, do not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).

Subd. 5.

[Renumbered 13.055, Subd. 6]

Subd. 6. **Remedies and enforcement.**

The attorney general shall enforce this section and section 13.055, subdivision 6, under section 8.31.

Government Agencies. The following statutes apply to Minnesota State government agencies:

13.055 STATE AGENCIES; DISCLOSURE OF BREACH IN SECURITY.

Subdivision 1. **Definitions.**

For purposes of this section, the following terms have the meanings given to them.

(a) "Breach of the security of the data" means unauthorized acquisition of data maintained by a state agency that compromises the security and classification of the data. Good faith acquisition of government data by an employee, contractor, or agent of a state agency for the purposes of the state agency is not a breach of the security of the data, if the government data is not provided to an unauthorized person.

(b) "Contact information" means either name and mailing address or name and email address for each individual who is the subject of data maintained by the state agency.

(c) "Unauthorized acquisition" means that a person has obtained government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

(d) "Unauthorized person" means any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data.

Subd. 2. **Notice to individuals.**

A state agency that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach.

Notification must be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency as provided in subdivision 3; or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

Subd. 3. **Delayed notice.**

The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede an active criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

Subd. 4. **Method of notice.**

Notice under this section may be provided by one of the following methods:

(a) written notice by first class mail to each affected individual;

(b) electronic notice to each affected individual, if the notice provided is consistent with the provisions regarding electronic records and signatures as set forth in United States Code, title 15, section 7001; or

(c) substitute notice, if the state agency demonstrates that the cost of providing the written notice required by paragraph (a) would exceed $250,000, or that the affected class of individuals to be notified exceeds 500,000, or the state agency does not have sufficient contact information. Substitute notice consists of all of the following:

(i) email notice if the state agency has an email address for the affected individuals;

(ii) conspicuous posting of the notice on the Website page of the state agency, if the state agency maintains a Website; and

(iii) notification to major media outlets that reach the general public.

Subd. 5. **Coordination with consumer reporting agencies.**

If the state agency discovers circumstances requiring notification under this section of more than 1,000 individuals at one time, the state agency

must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Subd. 6. **Security assessments.**

Each government entity shall conduct a comprehensive security assessment of any personal information maintained by the government entity. For the purposes of this subdivision, personal information is defined under section 325E.61, subdivision 1, paragraphs (e) and (f).

The following statute is known as the **Minnesota Government Practices Act**:

13.01 GOVERNMENT DATA.

Subdivision 1. **Applicability.**

All government entities shall be governed by this chapter.

Subd. 2. **Citation.**

This chapter may be cited as the "Minnesota Government Data Practices Act."

Subd. 3. **Scope.**

This chapter regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

Subd. 4. **Headnotes.**

The headnotes printed in boldface type before paragraphs in this chapter are mere catchwords to indicate the content of a paragraph and are not part of the statute.

Subd. 5. **Provisions coded in other chapters.**

(a) The sections referenced in this chapter that are codified outside this

chapter classify government data as other than public, place restrictions on access to government data, or involve data sharing.

(b) Those sections are governed by the definitions and general provisions in sections 13.01 to 13.07 and the remedies and penalties provided in sections 13.08 and 13.09, except:

(1) for records of the judiciary, as provided in section 13.90; or

(2) as specifically provided otherwise by law.

The following statute applies to government websites:

13.15 COMPUTER DATA.

Subdivision 1. **Definitions**.

As used in this section, the following terms have the meanings given.

(a) "Electronic access data" means data created, collected, or maintained about a person's access to a government entity's computer for the purpose of:

(1) gaining access to data or information;

(2) transferring data or information; or

(3) using government services.

(b) "Cookie" means any data that a government-operated computer electronically places on the computer of a person who has gained access to a government computer.

Subd. 2. **Classification of data.**

Electronic access data are private data on individuals or nonpublic data.

Subd. 3. **Notice; refusal to accept cookie.**

(a) A government entity that creates, collects, or maintains electronic access data or uses its computer to install a cookie on a person's computer must inform persons gaining access to the entity's computer of the creation, collection, or maintenance of electronic access data or the entity's use of cookies before requiring the person to provide any data about the person to the government entity. As part of that notice, the government entity must inform the person how the data

will be used and disseminated, including the uses and disseminations in subdivision 4.

(b) Notwithstanding a person's refusal to accept a cookie on the person's computer, a government entity must allow the person to gain access to data or information, transfer data or information, or use government services by the government entity's computer.

Subd. 4. **Use of electronic access data.**

Electronic access data may be disseminated:

(1) to the commissioner for the purpose of evaluating electronic government services;

(2) to another government entity to prevent unlawful intrusions into government electronic systems; or

(3) as otherwise provided by law.

Subd. 5. **Exception.**

This section does not apply to a cookie temporarily installed by a government entity on a person's computer during a single session on or visit to a government entity's Website if the cookie is installed only in a computer's memory and is deleted from the memory when the Website browser or Website application is closed.

Plastic Card Security Act [Minn. Stat. § 325E.64]

In 2007 Minnesota became the first state to incorporate a portion of the PCI-DSS into their state data security or data breach laws. [See discussion of PCI-DSS on page 14]

Known as the Plastic Card Security Act, the Minnesota law was passed largely in response to the massive data breach at TJX Companies when card issuers were required to reissue millions of debit and credit cards. [See discussion of FTC action In Re TJX on page 25.] The Minnesota law prohibits anyone conducting business in Minnesota from storing sensitive information from credit and debit cards after the transaction has been authorized. The law also makes noncompliant entities liable for financial institutions costs

related to cancelling and replacing credit cards compromised in a security breach. As a result, any business that is breached and is found to have been storing "prohibited" cardholder data (e.g., magnetic stripe, CCV codes, tracking data, etc.) are required to reimburse banks and other entities for costs associated with blocking and reissuing cards. This law also opens up the business to the potential of private lawsuits.

This law applies to any "person or entity conducting business in Minnesota" that accepts credit cards, debit cards, stored value cards, or similar cards issued by financial institutions.

Failure to comply with the law may result in the reimbursement to the card-issuing financial institutions for the "costs of reasonable actions" to both protect its cardholders' information and to continue to provide services to its cardholders after the breach. Costs may be related to the notification, cancellation and reissuance, closing and reopening of accounts, stop payments, and refunds for unauthorized transactions. The financial institution may also bring an action itself to recover the costs of damages it pays to cardholders resulting from the breach.

Target and other businesses hit with massive data security breach incidents are likely to see this law used by credit card companies trying to recover the costs incurred to replace credit cards of affected customers.

The full text of the Plastic Card Security Act appears below.

325E.64 ACCESS DEVICES; BREACH OF SECURITY.

Subdivision 1. **Definitions.**

(a) For purposes of this section, the terms defined in this subdivision have the meanings given them.

(b) "Access device" means a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for

storage of information which includes, but is not limited to, a credit card, debit card, or stored value card.

(c) "Breach of the security of the system" has the meaning given in section 325E.61, subdivision 1, paragraph (d).

(d) "Card security code" means the three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device which is used to validate access device information during the authorization process.

(e) "Financial institution" means any office of a bank, bank and trust, trust company with banking powers, savings bank, industrial loan company, savings association, credit union, or regulated lender.

(f) "Microprocessor chip data" means the data contained in the microprocessor chip of an access device.

(g) "Magnetic stripe data" means the data contained in the magnetic stripe of an access device.

(h) "PIN" means a personal identification code that identifies the cardholder.

(i) "PIN verification code number" means the data used to verify cardholder identity when a PIN is used in a transaction.

(j) "Service provider" means a person or entity that stores, processes, or transmits access device data on behalf of another person or entity.

Subd. 2. **Security or identification information; retention prohibited.**

No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

Subd. 3. **Liability.**

Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service

provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:

(1) the cancellation or reissuance of any access device affected by the breach;

(2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;

(3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;

(4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and

(5) the notification of cardholders affected by the breach.

The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Use of Social Security Numbers [Minn. Stat. § 325E.59]

The following Minnesota statute governs the use of social security numbers in Minnesota.

325E.59 USE OF SOCIAL SECURITY NUMBERS.

Subdivision 1. **Generally.**

(a) A person or entity, not including a government entity, may not do any of the following:

(1) publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display"

means to intentionally communicate or otherwise make available to the general public;

(2) print an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity;

(3) require an individual to transmit the individual's Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted, except as required by titles XVIII and XIX of the Social Security Act and by Code of Federal Regulations, title 42, section 483.20;

(4) require an individual to use the individual's Social Security number to access an Internet Website, unless a password or unique personal identification number or other authentication device is also required to access the Internet Website;

(5) print a number that the person or entity knows to be an individual's Social Security number on any materials that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed. If, in connection with a transaction involving or otherwise relating to an individual, a person or entity receives a number from a third party, that person or entity is under no duty to inquire or otherwise determine whether the number is or includes that individual's Social Security number and may print that number on materials mailed to the individual, unless the person or entity receiving the number has actual knowledge that the number is or includes the individual's Social Security number;

(6) assign or use a number as the primary account identifier that is identical to or incorporates an individual's complete Social Security number, except in conjunction with an employee or member retirement or benefit plan or human resource or payroll administration; or

(7) sell Social Security numbers obtained from individuals in the course of business.

(b) For purposes of paragraph (a), clause (7), "sell" does not include the release of an individual's Social Security number if the release of the Social Security number is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a

legitimate business purpose. The release of a Social Security number for the purpose of marketing is not a legitimate business purpose under this paragraph.

(c) Notwithstanding paragraph (a), clauses (1) to (5), Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the Social Security number. Nothing in this paragraph authorizes inclusion of a Social Security number on the outside of a mailing or in the bulk mailing of a credit card solicitation offer.

(d) A person or entity, not including a government entity, must restrict access to individual Social Security numbers it holds so that only its employees, agents, or contractors who require access to records containing the numbers in order to perform their job duties have access to the numbers, except as required by titles XVIII and XIX of the Social Security Act and by Code of Federal Regulations, title 42, section 483.20.

(e) This section applies only to the use of Social Security numbers on or after July 1, 2008.

Subd. 2.[Repealed, 2007 c 129 s 58]

Subd. 3. **Coordination with other law.**

This section does not prevent:

(1) the collection, use, or release of a Social Security number as required by state or federal law;

(2) the collection, use, or release of a Social Security number for a purpose specifically authorized or specifically allowed by a state or federal law that includes restrictions on the use and release of information on individuals that would apply to Social Security numbers; or

(3) the use of a Social Security number for internal verification or administrative purposes.

Subd. 4. **Public records.**

This section does not apply to documents that are recorded or required to be open to the public under chapter 13 or by other law.

Recording Communications
[Minn. Stat. § 626A.02 Wiretap law]

The following Minnesota statute is nearly identical to the federal wiretapping statute [18 U.S.C. § 2511 (1)] [See pages 46-47] and generally provides that it is legal for a person to record a wire, oral, or electronic communication if that person is a party to the communication, or if one of the parties has consented to the recording- so long as no criminal or tortious intent accompanies the recording.

626A.02 INTERCEPTION AND DISCLOSURE OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS PROHIBITED.

Subdivision 1. **Offenses.**

Except as otherwise specifically provided in this chapter any person who:

(1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication;

(2) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication;

(3) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; or

(4) intentionally uses, or endeavors to use, the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision;

shall be punished as provided in subdivision 4, or shall be subject to suit as provided in subdivision 5.

Subd. 2. **Exemptions.**

(a) It is not unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(b) It is not unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It is not unlawful under this chapter for a person acting under color of law to intercept a wire, electronic, or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It is not unlawful under this chapter for a person not acting under color of law to intercept a wire, electronic, or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state.

(e) It is not a violation of this chapter for a person:

(1) to intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public;

(2) to intercept any radio communication that is transmitted:

(i) by a station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(ii) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(iii) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(iv) by a marine or aeronautical communications system;

(3) to engage in any conduct which:

(i) is prohibited by section 553 of title 47 of the United States Code; or

(ii) is excepted from the application of section 605(a) of title 47 of the United States Code by section 605(b) of that title;

(4) to intercept a wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(5) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if the communication is not scrambled or encrypted.

(f) It is not unlawful under this chapter:

(1) to use a pen register or a trap and trace device as those terms are defined by section 626A.39; or

(2) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of the service.

(g) It is not unlawful under this chapter for a person not acting under color of law to intercept the radio portion of a cordless

telephone communication that is transmitted between the cordless telephone handset and the base unit if the initial interception of the communication was obtained inadvertently.

Subd. 3. **Disclosing communications.**

(a) Except as provided in paragraph (b), a person or entity providing an electronic communications service to the public must not intentionally divulge the contents of any communication other than one to the person or entity, or an agent of the person or entity, while in transmission on that service to a person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of a communication:

(1) as otherwise authorized in subdivision 2, paragraph (a), and section 626A.09;

(2) with the lawful consent of the originator or any addressee or intended recipient of the communication;

(3) to a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or

(4) that were inadvertently obtained by the service provider in the normal course of business if there is reason to believe that the communication pertains to the commission of a crime, if divulgence is made to a law enforcement agency.

Subd. 4. **Penalties.**

(a) Except as provided in paragraph (b) or in subdivision 5, whoever violates subdivision 1 shall be fined not more than $20,000 or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then:

(1) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service

communication, a cordless telephone communication transmitted between the cordless telephone handset and the base unit, or a paging service communication, and the conduct is not that described in subdivision 5, the offender shall be fined not more than $3,000 or imprisoned not more than one year, or both; and

(2) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication, a cordless telephone communication transmitted between the cordless telephone handset and the base unit, or a paging service communication, the offender shall be fined not more than $500.

(c) Conduct otherwise an offense under this subdivision that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted:

(1) to a broadcasting station for purposes of retransmission to the general public; or

(2) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is
not an offense under this subdivision unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

Subd. 5. **Civil action.**

(a)(1) If the communication is:

(i) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(ii) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of title 47 of the Code of Federal Regulations and that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct is subject to suit by the county or city attorney in whose jurisdiction the violation occurs.

(2) In an action under this subdivision:

(i) if the violation of this chapter is a first offense for the person under subdivision 4, paragraph (a), and the person has not been found liable in a civil action under section 626A.13, the city or county attorney is entitled to seek appropriate injunctive relief; and

(ii) if the violation of this chapter is a second or subsequent offense under subdivision 4, paragraph (a), or the person has been found liable in a prior civil action under section 626A.13, the person is subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (a), clause (2)(i), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

California

California has been the most active state in the privacy field. As a result, many Minnesota based businesses will simply draft their website privacy policies and other privacy practices to make sure that their practices and procedures comply with California law.

The California state constitution provides that: *"All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and privacy."* Ca. Const. art I, § 1.

California's Office of Privacy Protection governs the state's wide array of privacy laws, including data security. In California, "[a] business that owns or licenses personal information about a California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." [California

Civil Code 1798.81.5(b)] Such security procedures include administrative, technical, and physical safeguards. Businesses should establish a written data security policy to inform employees what is required. Businesses that own or license such personal data must also contractually require third parties dealing with the data to protect personal information.

California's Online Privacy Protection Act (Cal.OPPA) became the first state law in the nation to require operators of commercial websites or online services to post a privacy policy.

The Far Reach of Cal.OPPA. Cal.OPPA extends beyond California borders and requires a Minnesota business that operates a website that collects personally identifiable information from California consumers to post a conspicuous privacy policy on its website as well as mobile apps and mobile devices. Cal.OPPA essentially operates as a national law as it has potential impact on virtually every website or mobile app that collects personally identifiable information from consumers.

The California Attorney General has been aggressive at enforcing Cal.OPPA including going after businesses with corporate offices outside California. Delta Airlines was found non-compliant by not having a conspicuous privacy policy on its mobile app called "Fly Delta." The California Attorney General has also reached an agreement with major app platforms requiring apps delivered through their platforms to have clear privacy policies.

Do Not Track. Cal.OPPA now includes the first state law to address Do Not Track (DNT) signals sent from web browsers. The law does not require advertisers or website operators to honor those signals but does require operators of websites and online services, including mobile applications, to notify users about how they handle DNT signals.

Data Breach Notification. A business that possesses data of California residents is required to disclose a breach of a user's online account information. California Civil Code Section 1798.82 specifically requires that the business disclose the breach of "[a] user name or email address in combination with a password or security question and answer that would permit access to an online account." This law makes such disclosures of the breach mandatory and creates specific requirements for the notification.

The Right to Be Forgotten - Eraser Law. Effective January 1, 2015, the so-called California Eraser law Cal. Bus. & Prof. Code §§ 22580-22582) requires website and mobile app operators to provide minors (California residents under 18) with 1) the ability to remove or request removal of content that the minor has posted on the website or mobile app, 2) notice and clear instruction on how to remove the data, and 3) notice that such removal may not remove all evidence of the posting. The law includes certain exceptions and offers methods for businesses to comply with the removal requirements. The law also imposes restrictions on targeted advertising to minors and prohibits operators of websites or mobile apps from 1) marketing or advertising certain products to minors based upon information unique to that minor, e.g., activities, interests, profile, address, and 2) using, disclosing, or compiling personal information of a minor, knowing it will be used for marketing or advertising certain restricted products such as alcohol, guns, tobacco, drug paraphernalia, etc. The removal requirements apply to any website or mobile app that is "directed to minors" (as opposed to general audiences) or if the operator has actual knowledge that a user is a minor. The law does not require the operator of the website to collect or maintain age information. It may therefore be advisable for a website operator to not collect age information as part of a general audience website or mobile app.

Massachusetts

Massachusetts has widely been regarded as the gold standard for data security laws. Massachusetts requires any company that owns or licenses personal information from residents of the state to develop, implement, and maintain a comprehensive written policy that creates proper administrative, technical, and physical safeguards for consumer information. Massachusetts follows a "sliding scale" approach, allowing a smaller business with limited customer information to develop a policy that works to protect their data, but does not require costly investments in software or other technical safeguards. The regulations require encryption of any data relating to a Massachusetts resident transmitted across a public network, as well as encryption (not just password protection) of any customer data on a portable device. The State of Massachusetts makes available a "Compliance Checklist" that guides a business through the process of creating and implementing a comprehensive Written Information Security Program (WISP).

Massachusetts data privacy laws and regulations require all persons that own or license personal information of Massachusetts residents to:

> [D]evelop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope, and type of business of the person obligated to safeguard the personal information... (b) the amount of resources available to such person, (c) the amount of stored data, and (d) the need for security and confidentiality of both consumer and employee information.

[201 Mass. Code Regs 17.03(1)]

These Massachusetts regulations require policies that include training of employees, identifying media and records that contain personal information, monitoring, and verifying and requiring that third party service providers comply with the Massachusetts regulations.

Specific technical safeguards are identified such as secure authentication protocols, secure access control measures, and encryption of personal information stored on laptops and mobile devices or any files or records that contain personal information and that may be transmitted across a public network.

A Minnesota business may have to pay attention to these Massachusetts data security laws and regulations if they collect any personal information of a Massachusetts resident.

Other State Privacy and Breach Notification Laws

Following extensive fears of identity theft and highly publicized data security breaches, most states, including Minnesota, passed laws requiring consumer notification when a security breach involving private information occurs. While there continues to be discussion about the need for a comprehensive federal law that would preempt the patchwork of state laws and create a uniform standard, as of the publication of this Guide, there was no such federal breach notification statute. [See discussion of proposed federal legislation on pages 53-56.] A Minnesota business is therefore still required to comply with multiple state laws in the event of a data breach that involves the personal information of residents of other states.

State Breach Notification Laws

Minnesota and most other states have enacted laws that require notification to individuals in the event of a security breach of sensitive or personal information. These laws usually cover any

businesses that conduct business in the state and own, license, or maintain information covered by the statute (usually defined as the person's name, combined with their social security number, driver's license number, or credit and banking account information), regardless of the size of the business.

In general, most state laws require that companies disclose a data breach to affected residents of the state. Some statutes also require notification of law enforcement, consumer protection boards, or credit agencies. Most breach notification laws set forth notification guidelines as to how soon a company is required to inform customers of a data breach (e.g., without unreasonable delay); the existence of civil or criminal penalties for failure to notify; the existence of a private right of action, if any, against the company; and any exemptions that apply to certain businesses or certain breaches. Some state laws distinguish between material and nonmaterial breaches.

State Laws Not Uniform. Most state laws, including Minnesota's, provide a notification scheme and require notice to individuals after a "breach of the security system." (See Minn. Stat. 325E.61 on pages 87-88). But these state laws are not identical and include their own subtle distinctions and provisions. For example, some laws only require notice when there is a "material" or "significant" risk of harm from the security breach. Note that in Minnesota social security or account numbers alone may not trigger notification as they must be coupled with another identifier such as a name. Some state security breach notification laws (such as Wisconsin) are triggered even if just account numbers or related access codes are compromised. Some states also have specific requirements for what must be included in the breach notification. **Minnesota does not have a specific content requirement.** Timing of the notice is vague in most states and is required to be done within a "reasonable" time frame. (Wisconsin requires notice within 45 days). Some states allow for a private right of action. **Minnesota actions may be brought by the Minnesota Attorney General**. One bill introduced

in the Minnesota legislature would have required notification of a consumer within 48 hours of discovery of the data breach. The variety in state laws is one of the most compelling justifications for a comprehensive federal breach notification law.

State Data Protection and Security Laws

As discussed above there are several industry-specific data privacy related laws at the federal level. Many states have now enacted their own industry- neutral laws which regulate the use, transmission, storage, and dissemination of personal information. Such laws generally contain components regulating the use of social security numbers, notification for breaches of personal information, affirmative obligations to safeguard personal information, and the destruction of records containing personal information.

A business must be certain that its requirements and policies regarding the collection, sharing, and use of personal information comply with the laws applicable to where it conducts business. Personal information subject to these state laws and regulations may include a government identification card or license, social security numbers, residential addresses, birthdates, credit worthiness, employment information, personal references, criminal indictments or convictions, civil litigation, or other dispute resolution and regulatory proceedings.

State Laws-Social Security Numbers. Many states, including Minnesota, have enacted laws governing the use of social security numbers. [See pages 98-101.] Such laws generally prohibit the public posting or displaying of an individual's social security number, the printing of a social security number on anything sent through the mail, prohibiting the sending of a social security number over the internet without encryption, and/or using a person's social security number on any other cards, such as student ID cards.

GLOBAL PRIVACY AND DATA SECURITY LAW

There are two approaches to legally protect the privacy rights of individuals. The United States has primarily taken a sectoral approach with the use and disclosure of personal information regulated by specific industries or sectors. There is no single omnibus privacy law in the United States. In Europe and most countries outside of the United States a more comprehensive approach is followed with one omnibus law or set of regulations covering all industries and sectors.

If a Minnesota business is considering expanding its business outside of the United States, it should consider what foreign laws might apply. An analysis of the proposed activities and whether or not the jurisdiction of any particular country is implicated will help guide the business on what compliance activities may be required relative to data privacy. For example, if any personal information of residents outside of the United States (including employees) is transferred for use by a business situated in the United States, the relevant laws of that foreign jurisdiction will apply.

It is impossible for this Guide to cover all of the foreign data privacy and security laws and their nuances. We will, however, try to provide a basic overview of some key issues for a Minnesota business to consider with a focus on the European Union (EU). The data privacy practices, laws, and regulations of the EU have been the basis of much of law and best practices followed in the rest of the world.

EU-USA Privacy Law Compared. Privacy laws in the EU and the rest of the world are quite different from those in the United States. In fact, the United States is considered by the EU as being so lax in its privacy laws that the transfer of personal data from the EU to the United States is not permitted without the business taking extra steps to assure that it adheres to the same privacy principles that exist in Europe. [See Safe Harbor (no longer valid), Privacy Shield, Model Contracts, and Binding Corporate Rules discussed on pages 121-124]

The European Parliament and the Council of the European Union started from the principle that privacy is a fundamental right that must be protected whenever personal data is processed. In the United States privacy rights are less clear and, as discussed in this Guide, are covered by a patchwork of federal and state laws. Information and data is considered more like a property right (e.g., who owns the data?) in the United States with the idea that a business can generally use the information or data as they desire unless otherwise prevented by a specific law or regulation. Specific informed consent from the individual who is the subject of the data is not always a legal requirement.

In the United States the primary method of obtaining consent to use personal information is for a person to "opt- out" by signifying that they are not interested in participating or receiving any further communications. In Europe personal consent is primarily obtained through an "opt in" by the individual and requires an affirmative acknowledgement and consent by the person for the information to be collected and used.

EU 1995 Data Directive

The privacy model developed by the EU is formally expressed in the 1995 EU Data Directive (95/46/EC3). Under the EU Data Directive each EU member state establishes, implements, and enforces its

own regulatory structure consistent with the guidance provided by the EU Directive. The EU Data Directive is, however, not in itself a law applicable to all private citizens. It must be read only as a guide to the general content of the national laws that are adopted by each member state.

Each of the 27 members of the EU is responsible for adopting and enforcing their own privacy or data protection laws. Countries that are not members of the EU, such as Norway, Iceland, and Switzerland, have adopted EU compliant laws as part of their integrated trade policies. A Minnesota business must therefore consider the data privacy laws and regulations of the country where it does business. **This EU Directive remains in effect until 2018 when it will be replaced by the General Data Protection Regulation (GDPR) discussed below**.

The EU Data Directive has five principles that are set forth in Article 6 of the Directive as follows:

Article 6

1. Member States shall provide that personal data must be:

(a) **processed fairly** and lawfully;

(b) **collected for specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) **adequate, relevant and not excessive** in relation to the purposes for which they are collected and/or further processed;

(d) **accurate and, where necessary, kept up to date;** every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. **[emphasis added]**

Data Controller or Processor? The EU Data Directive establishes the concepts of a "controller" and "processor" and creates specific legal obligations applicable to the data controllers. A controller determines the purposes and means of the processing of personal data. The controller decides how the data is collected, stored, used, altered and disclosed. The processor is a person (other than an employee of the controller) who processes personal data on behalf of the controller. The distinction between controller and processor becomes important as it determines who is responsible for compliance with the relevant data protection laws and the enforcement authorities.

Data processing is broadly defined in the EU Data Directive and includes any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organization, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Notification to the Data Protection Authority in Advance. One of the first things a Minnesota business may need to do when setting up an office or operation in Europe is to notify the relevant Data Protection Authorities (DPAs) that the business intends on processing personal information as a data controller within the relevant jurisdiction. This can be as simple as processing personal data of just a few employees to pay their salaries or the processing of significant amounts of customer data maintained in databases in multiple locations.

A unique and key part of the EU Data Directive is the requirement for notification to the appropriate DPA by the data controller before processing may commence. The purpose of such notification is to allow the DPA to assess the risk posed to the rights and freedoms of the data subjects by the proposed processing, and to post such information in a national register accessible to all. This notification requirement is the part of the EU Data Directive with which a Minnesota business will likely have the most contact.

Data processing by the Minnesota business is not supposed to start until this notification is complete. Data Protection Authorities differ however in when this notice is deemed effective. In some cases notice is complete when the fee is paid or it may not be effective until a receipt and notice is actually received from the DPA. Failure to notify a DPA prior to commencing the data processing activities may, in some cases, constitute a criminal offense.

New General Data Protection Regulation (GDPR) Replaces EU Data Directive. In January 2012, the European Commission first announced proposed revisions to the EU Data Directive. Following years of negotiations the European Parliament and Council on December 17, 2015 announced that agreement had been reached on the text of a brand-new General Data Protection Regulation (GDPR). This draft document (over 200 pages) follows years of intense lobbying and represents a landmark moment in data protection and privacy both in Europe and around the world.

The final version still needs to be ratified and voted on by the full Parliament which is likely to take place in the spring or summer of 2016.

Effective Date The GDPR will not take effect until two years after approval so it will likely have an effective date some time in 2018.

Current Law. The EU Data Directive remains in effect until the GDPR replaces it in 2018. Businesses however, should have already begun to prepare for compliance with the GDPR.

Highlights of GDPR. Some of the major provisions of the GPDR include:

> **Expansion of Scope.** The GDPR applies to many more businesses than the EU Data Directive, including any controller or processor of EU citizen data, regardless of where the controller or processer is located. New obligations are imposed on data processors and on controllers who are required to impose contractual obligations on their data processors.
>
> **Data Breach Notification.** Notification to a privacy regulator of a data breach may be required within 72 hours of discovery of the breach.
>
> **Fines for Noncompliance and Right to Sue.** Violations of certain provisions, such as consent requirements or cross border data transfer restrictions, can trigger fines up to the greater of 20,000,000 EUR or four percent of a company's annual revenue. Individuals are also allowed right to sue and obtain compensation from a noncompliant controller or processor.
>
> **Data Protection Officers.** Data protection officers may need to be hired where data processing is a "core" activity and where sensitive data is processed on a "large" scale.
>
> **Consent Requirements.** Consent will be required in more circumstances than under the EU Directive and it must be either by a statement or a clear affirmative action. Consent has to be demonstrable upon demand, able to be retracted at any time , and will not be considered valid if a data subject has to

give consent to processing for the provision of a service where the processing is not necessary to the actual performance of the contract.

Member States. Intent of GDPR is to harmonize data protection law within EU however each member state may enact its own laws to implement the new regulation.

Children. When an online service is required to obtain consent, the consent must be obtained from the parent or guardian if the concerned individual is under 16 (unless the member state passes a law to lower this age, age cannot be lower than 13).

Sensitive Data. More stringent requirements apply to sensitive data than under the EU Directive, including genetic, biometric, health, racial, and political data.

Enhanced Notice and Information Obligations. Controllers must provide any information they hold about a data subject, free of charge, and within one month of request. More details may need to be disclosed to data subjects, both initially (e.g in a privacy policy) and in response to access requests. Controllers may be required to allow individuals to obtain a full copy of their data in a standard format and possibly facilitate transfer of data to others.

Right to be forgotten. A "right to erasure" requires controllers to delete personal data in a variety of cases, including if the data was collected when the data subject was still a child in need of parental consent, or if the data is sensitive. (This is similar to the "right to be forgotten" discussed on page 152 in the Guide).

Cross Border Transfers Still Restricted. As provided in the EU Data Directive the transfer of personal data to a location outside the EU remains restricted. The EU-US Safe Harbor (pages 121-

124) is no longer available, but the Privacy Shield may be a new option for businesses, along with Model Contracts and Binding Corporate Rules (discussed on page 124 of the Guide).

While many privacy advocates have praised the GDPR as a reasonable compromise of multiple interests, some have expressed concern over the potential sanctions for non-compliance, such as the fines based on company revenue and fear that investors in Europe may move technology ventures to Asia or elsewhere to avoid potential fines.

In any case, businesses with significant global operations must continue to comply with the EU Data Directive while, at the same time, preparing for the GDPR.

Transfer of Personal Data Outside Of The European Union

A major concern of the EU Data Directive, as well as the GDPR, is the protection of personal data that may be transferred outside the EU and the jurisdiction of the DPA over a country (such as the USA) that does not adhere to the same privacy principles set forth in the EU Data Directive and the GDPR. According to EU privacy law personal data may only be transferred outside the EU where it is afforded an adequate level of protection. Such transfers are particularly easy with respect to personal information transmitted via the internet. **The United States is one of the countries recognized by the EU as not having an adequate level of data privacy protection.**

For over 15 years a Minnesota business could qualify to transfer personal data from EU countries provided that it participated in the EU-US Safe Harbor Program. This Safe Harbor Program is no longer available.

On October 6, 2015, the European Court of Justice invalidated the EU-U.S. Safe Harbor Agreement that allowed the storage and processing of personal data of EU citizens so long as the business self-certified compliance with certain privacy policies and procedures. The so-called Privacy Shield may now be available along with Model Contracts, Binding Corporate Rules, consent, and some other exceptions discussed below.

Privacy Shield. On February 2, 2016 the European Commission and U.S. Department of Commerce announced a new data transfer framework, the EU-U.S. Privacy Shield, to replace the invalidated Safe Harbor Agreement. The Privacy Shield includes a new Federal ombudsman to oversee intelligence access to EU citizen data, a multi-step complaint resolution process for EU citizens, and a number of other new provisions. The Privacy Shield is more stringent than the Safe Harbor relative to enforcement, remedies, onward transfer restrictions, certification, and notice and choice obligations. The EU must adopt the Privacy Shield framework (expected in the summer of 2016). Once approved, the United States Department of Commerce will publish the proposed new rules in the Federal Register.

Prior US-EU Safe Harbor

In 2000 the EU and the U.S. Department of Commerce reached an agreement on certain Safe Harbor Principles that allowed a Minnesota business to self-certify adherence to the EU privacy principles. The EU-U.S. Safe Harbor agreement — a cooperative agreement between U.S. government agencies and the European Commission allowed a Minnesota business to store and process data belonging to European citizens if the business demonstrated that they met European data protection principles described in the Safe Harbor. **AS NOTED ABOVE THIS SAFE HARBOR WAS INVALIDATED BY THE EUROPEAN COURT OF JUSTICE IN OCTOBER 2015.**

Self-Certification Under Safe Harbor. A Minnesota business that sought protection under the former safe harbor could do so by self-certifying compliance with certain privacy practices and having a privacy policy that embodied the Safe Harbor Privacy Principles including Notice, Choice, Transfer to Third Parties, Security, Data Integrity, Access, and Enforcement. The privacy policy had to be made public and specifically state that the business adhered to the Safe Harbor Principles. These representations attesting to the Safe Harbor Principles are frequently found in website privacy policies.

Enforcement. The enforcement principle required the business to have an independent third party to which individuals could turn for the investigation of unresolved complaints. Many businesses selected organizations such as TRUSTe, Council of Better Business Bureaus, the American Arbitration Association, or JAMS, to serve in this role. These organizations and others also offered assistance in the development of Safe Harbor compliance programs.

Annual Renewal of Safe Harbor Mandatory. Upon submission by the Minnesota business of the self-certification form to the U.S. Department of Commerce, the materials were reviewed for completeness before the business was posted on the list of Safe Harbor companies. Self-certification was required annually for continued compliance with the Safe Harbor Principles.

FTC Enforcement of Safe Harbor. In the wake of revelations by Edward Snowden about the National Security Agency (NSA) and U.S. government surveillance and the perceived lack of enforcement activities regarding the Safe Harbor, European lawmakers and data privacy officials repeatedly questioned the efficacy of the EU-U.S. Safe Harbor agreement. Critics called for suspension or termination of the program. There was also concern as to whether businesses on the list actually adhered to the Safe Harbor principles. The FTC responded to these European concerns and allegations by taking a more proactive and aggressive approach to enforcement.

At least 13 American businesses (including several NFL teams) agreed to settle FTC charges that they falsely claimed compliance with the EU-U.S. Safe Harbor program. These actions were brought under Section 5 of the FTC Act (See page 21).

In February 2014, the FTC settled a case *In re Fantage.com Inc.* (FTC File No. 1423026) involving Fantage.com, the maker of multiplayer online role playing games aimed at children. The company claimed to be certified under the Safe Harbor program but had let its certification lapse and failed to maintain current status as a participant in the Safe Harbor Program. The FTC alleged that statements made on the Fantage website about Safe Harbor participation were therefore false and misleading for the period of time such certification had lapsed. Under the settlement with the FTC, Fantage is prohibited from misrepresenting the extent to which it participates in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization. The settlement agreement also obligates Fantage to report to the FTC no later than 30 days prior to any changes affecting Fantage's ability to comply with the terms of the settlement. The order terminates in 20 years.

ALL OF THESE CONCERNS WITH THE SAFE HARBOR CULMINATED IN THE INVALIDATION OF THE SAFE HARBOR FRAMEWORK BY THE EUROPEAN COURT OF JUSTICE IN OCTOBER 2015

Despite the loss of some legal protections afforded by the Safe Harbor framework, businesses may still derive benefits and continued legal protections from actions they may have taken as necessary to comply with the Safe Harbor requirements. All of these activities demonstrate that a business takes privacy seriously and might be used as evidence to support a defense against any claims or government investigation as to lax privacy and data security practices. This will however not be the case where a business who certified compliance with the Safe Harbor framework did not actually implement the required actions.

Model Contracts

The EU Data Directive allows for the use of so-called "model contracts." A business that uses certain standard clauses that have been approved by the European Commission in their agreements concerning the transfer of personal data to countries outside of the EU may be deemed to have adequate data privacy safeguards. Some member states require that such model contracts be deposited with the DPA of the relevant member state. [For more information on how to use these "model contracts" see http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.] **Model contracts remain a viable option despite loss of the Safe Harbor.**

Binding Corporate Rules

The EU developed the concept of Binding Corporate Rules (BCR's) to allow multinational corporations to make intra-organizational transfers of personal data across borders and still be in compliance with EU data protection law. The BCR is essentially a global code of conduct based upon European privacy principles, prepared by a business and approved by the relevant regulator. BCR's can be used instead of the Safe Harbor or model contract clauses as a way to meet the "adequacy" test imposed by the EU. As the Safe Harbor came under strong EU criticism and was ultimately invalidated, the use of model contracts and BCR's by American businesses for compliance has increased.

BCR's remain a viable option despite loss of the Safe Harbor.

The E-Privacy Directive and EU Cookie Law. A cookie is a simple text file that is stored on a user's computer or mobile device when visiting certain websites. It allows the website to remember the user's actions or preferences over a period of time. They are used to identify users, remember preferences, and complete shopping tasks without having to re-enter information. They can

also be used for online behavioral target advertising. The use of cookies has become ubiquitous to ecommerce.

The Directive on Privacy and Electronic Communications (E-Privacy Directive) [Directive 2002/58/EC (2002) (Amendments 2009)] was enacted to protect "the right to privacy in the electronic communication sector" and seeks to harmonize the regulations in member states. It permits the use of cookies if the user is provided with clear and comprehensive information about the purpose of the cookie and the user is given a chance to opt-out.

The 2009 amendments to the E-Privacy Directive forbid the placing of cookies without consent of the user. There has been much discussion about whether implied or express consent is required under the E-Privacy Directive or any of the member state laws governing cookies. As a result, some European websites have added a pop-up statement specific to cookies and requesting expressed consent or an "opt-in" from the user.

In June 2012, European data protection authorities (as part of the Article 29 Working Party,-composed of representatives of the DPA's, the European Data Protection Supervisor, and the European commission) issued an opinion clarifying that consent might not be required in cases where cookies were only used to track user input when completing a shopping cart online (also known as session- id cookies) and that first party analytics were not likely to create a privacy risk if the website provided clear information about the cookies and their use with an easy opportunity to opt-out by the user. [See Article 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption 00879/12/EN (adopted June 7, 2012).]

Each EU member state can, however, enact its own cookie law and there has been some variation in the consent requirements required. For example in some countries consent can be obtained via browser settings while others may require the express consent for use of cookies.

There has been lax enforcement of these cookie restrictions and some have criticized these efforts as misguided and of little value to data privacy.

Article 29 Working Party. The Article 29 Working Party is a special group formed in the EU for the expressed purpose of overseeing specific issues such as workplace privacy and handling of employee data. The group is composed of representatives of the DPA's, the European Data Protection Supervisor, and the European commission. The Working Party issues opinions and offers guidance on data privacy to the member states. In addition to the opinion on "cookies" mentioned above they have issued the following recent opinions regarding consent and cloud computing:

Article 29 Data Protection Working Party Opinion 15/2011 on Definition of Consent, 01197/11/EN (July 13, 2011) provides that valid consent requires affirmative indication of consent such as a signature or checking a box.

Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing 01037/12/EN (July 1, 2012) describes potential data protection risks, focusing on both individuals lack of control over their personal data and insufficient information about how the data is used.

CANADA

Personal Information Protection and Electronic Documents Act (PIPEDA)

Many American businesses have crafted their privacy policies to comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) [SC 2000, C5], knowing that PIPEDA fulfilled the requirements for self-certification under the now invalidated US-EU Safe Harbor program administered by the U.S. Department of Commerce. Compliance with PIPEDA will also

satisfy most of the requirements for the privacy laws of any of the member states of the EU.

Canada moved quickly to adopt legislation that complied with the 1995 EU Data Directive in order to both promote ecommerce and trade with the EU. PIPEDA adopts ten privacy principles:

Principle 1 — Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 — Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principle 6 — Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 — Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 — Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

There is little difference between the privacy principles of the EU and Canada.

Canada Anti-Spam Law [SC 2010,C23]

Effective July 1, 2014, Canada enacted one of the strictest laws intended to discourage unsolicited emails from businesses. The Canada Anti-Spam Law (CASL) broadly prohibits the sending of any electronic message that encourages participation in a commercial activity. CASL includes an opt-in regime that has serious ramifications for any business that promotes their products or services in Canadian markets. The definition of "electronic message" includes emails, text messages, phone calls, instant messaging, and social media. There are some exceptions for express or implied consent. Commercial electronic messages must include certain information including an unsubscribe mechanism. Penalties

are severe – up to Cdn$1,000,000 for individual offenders and up to Cdn$10,000,000 for a corporate offender.

The first enforcement action under CASL was on March 5, 2015 and included a fine of C$1.1 million (US$800,000) against Compu.finder Inc. based upon the sending of commercial electronic messages to individuals without their consent and without a functional unsubscribe mechanism. This action was followed, on March 25, 2015 with a settlement with Plentyoffish Media, Inc. for Cdn$48,000 (US$ 34,800) for sending commercial electronic messages to registered users and failing to prominently display the unsubscribe mechanism.

It is important to note that the above actions were taken by the government through the Canadian Radio-Television and Telecommunications Commission (CRTC). **A private right of action for CASL will go into effect July 1, 2017.**

Minnesota businesses should be looking at their promotional emails, texts, newsletters, and other electronic communications that are sent to Canadian residents to see if they fit within the exemptions under CASL, or make sure that appropriate consent has been obtained. When reviewing customer and contact lists, it is also necessary to keep records showing consent. [For more information on CASL see, http://www.ic.gc.ca/eic/site/030.nsf/eng/h_00039.html.]

BEST PRACTICES

As you read through this Guide you may be overwhelmed by the sheer number of laws and regulations. How can a business possibly comply with so many laws and regulations? Is it even possible for a business to limit the potential risks? A good place to start is to first determine what you are already doing relative to the collection, storage, and use of personal information. There may be some basic preventive actions and steps you can take before a data breach or other incident arises. In this section, we suggest basic activities that should help a business be more prepared in the event of a data privacy breach or other security incident.

Key Questions Every Business Should Ask Related To Data Privacy and Security

The following are some basic questions that general counsel, senior management, and corporate directors should be asking themselves and their companies about data privacy and security:

- Why should my business be concerned?
- What personal information do we collect and what do we use it for?
- What personal information do we share with others?
- Why do we share this information?
- How does data flow through our company?
- Where is it stored?

- What steps do we take to protect personal information that we collect?
- What corporate data privacy and security policies and procedures are in place?
- Do we have a social media policy?
- Do we use social media as a business tool?
- What does our website privacy policy say and is it consistent with actual business practice?
- When were the privacy policies and procedures, including the website policy and social media policy , last updated?
- Do we have a technology use policy? What does it say and when was it last updated?
- What business operations are tied directly to computer networks?
- What business records are accessible via the network?
- How, in layperson language with no technospeak, is our data secure?
- Who in the business is responsible for the security and integrity of our system and data?
- Who would want to target us?
- Is a data breach likely to come from within or outside the business?
- Are we confident that our security is current and up to date?
- Do we have a person responsible for data privacy and security? Do we need one?
- What outside professionals do we use for data privacy and security consultation ?
- How do we authorize and control access to our data?
- Is the level of access appropriate for the job title and responsibility?

- How is access terminated?
- How do we learn of a breach or unauthorized access to our network?
- How do we prevent unauthorized users from accessing our system and data?
- What internal controls are used to detect employee abuses and are they adequate?
- Are we vulnerable to outside attacks or the introduction of malware, worms or viruses that may be introduced? What about employees introducing the same to our network or system?
- Have we trained our employees on ways to avoid introducing malware, worms or viruses? What about training on so-called "phishing " attacks as ways to gain entry to the system and data?
- Do we encourage employees to share their concerns about outside intrusions and vulnerabilities?
- Have our internal controls for information security been reviewed by an independent third party or approved by an outside auditor?
- Have we tested our systems for vulnerabilities? When? How?
- Have we engaged someone to try and hack into our system to identify its weaknesses?
- Do we have a response plan in place in the event of a breach, unauthorized access, interruption of service, or other incident?
- Who do we turn to for assistance in the event of a data breach incident that can help us not only to protect and secure our network, but also to recover from such unauthorized access?
- Do we have a secure backup system, offsite data vault, or redundant servers and how long until we are up and running after a serious breach?

- What costs are we likely to incur in the event of a data breach?
- What insurance do we currently have to cover a data breach? Is insurance adequate?
- What federal, state, and international laws apply to our business relative to data privacy and security and what obligations do we have to notify and disclose a data breach?
- Do we transfer personal data from outside the USA (such as employee data) and if so do we participate in the US-EU Safe Harbor program? Model Contracts? Binding Corporate Rules?
- What must be included in a data breach notice and when and to whom must it be disclosed?
- What are the risks to our business for noncompliance with any obligations we might have to notify of a data breach?
- Have we made proper disclosures to investors regarding the risks of a data breach?
- What are potential damages, risks, fees and penalties to management, the board of directors, shareholders, and the business in the event of a data breach?
- What role can state or federal investigators play in the event of a data breach or other incident where our system is accessed by an unauthorized party?
- How would we work with the FBI or other law enforcement on data breach ?
- How would we work with outside legal counsel?
- How would we handle public relations in the event of a data breach?

Establish a Compliance Program

Customized Program

The questions above can be the prelude to a more systematic internal audit of data privacy and security practices of the business followed by implementation of a privacy compliance program.

There is no one-size-fits-all privacy compliance program.

If little or no customer information is collected by the business, and customer privacy is not generally considered part of the service, the compliance program and training would be far different than it would be for a business that collects, uses, and shares personal data as a key part of its business and related services.

All businesses, however, should have adequate safeguards and security systems in place to protect personal data in their possession and a process to systematically handle any data breaches that might arise.

Frequent and targeted compliance audits provide a way for a business to continually assess weaknesses and measure improvements in data privacy policies, procedures and security. These audits should be conducted at all levels. The key to success is to have involvement from the CEO down to the receptionist when assessing how a company collects and uses personal information and the data they are obligated to maintain for their customers and employees.

Security Incident and Data Breach Plan

Every business should prepare for a potential data breach by creating and implementing a company-wide data breach plan. Not all security incidents are a data breach. This is important because the response to a data breach requires a different set of considerations than a security incident.

In the event of a security incident or data breach, a business should pursue the following simultaneous lines of inquiry:

- Detail the chain of events including an initial determination as to whether an unauthorized disclosure or breach occurred. Note that not every unauthorized disclosure of data constitutes a breach and triggers compliance with notification and other legal obligations.
- What data was obtained?
- Was data encrypted?
- Has the unauthorized disclosure been terminated or is it ongoing? If it is ongoing, how can it be stopped?
- Identify the states where the individuals affected by any breach reside.
- Identify the relevant legal obligations, if any, that the business owes regarding potential notification of breach, and timelines for sending any notices .
- Evaluate insurance coverage and take appropriate steps to file a claim.
- What federal, state, and international laws are implicated by the "breach" or "incident"?
- Should law enforcement be called?
- Should an outside technical or forensics consultant be engaged?
- Should outside legal counsel be called?

Planning for a Security Incident or Data Breach. A response plan should be in place well in advance with details as to exactly how a security incident or an actual data breach will be handled. This plan should be reviewed on a regular basis with appropriate personnel educated on their responsibilities. This comprehensive data breach response and notification plan might be included as part of broader disaster recovery or business continuity plans.

Advance Planning and Preparation. The creation of the response plan should engage multiple business interests including legal, information technology, operations, finance, human resources, communications, and marketing. The involvement of upper management is essential.

The plan should be widely distributed so that appropriate people will react in a timely manner. Who in the business is most likely to first become aware of a security incident or data breach? The plan should ensure that employees at all levels know who to contact. Initial questions should be answered quickly and the information given to the appropriate person as efficiently as possible.

The security incident or data breach may pose harm to customers or individuals affected by the incident. Quick action may be necessary to contain the incident or shut down some portion of the network or system while assessing how the security incident occurred. The plan should identify who to contact and when (e.g., information security consultant? Forensics? Law enforcement?).

Incident Report System. There should be a reporting system in place that allows security incidents and data breaches to be tracked as they happen and records maintained of any investigation and result.

Simulated Breach. Conducting a mock security incident may help the business test the plan, evaluate the incident report system, and make any changes necessary. Like fire drills, these mock incidents or simulated breaches will also better prepare a business in the event of a real security incident or data breach.

First Steps. The top priority is to fix the problem and take all necessary steps to protect the data. Can the fix be accomplished with internal resources? Does the business have a forensics or technical consultant ready to immediately become engaged as necessary to investigate and resolve the incident? Notification requirements

under various state and federal laws need to be reviewed promptly to determine if a breach notice is required, and timing of any notice, the appropriate recipients, and content of such notice.

Communications - Is it a Breach that Requires Notice? ? Is the security incident even a breach that requires notice to consumers or individuals? What about government agencies and the media? If notification letters are necessary, what should they say and when should they be sent? Notification requirements vary by state as does the definition of breach. In some cases a business may decide to send to all consumers affected a notice even if the state where the affected person resides does not require it. Regardless of the legal requirements, the business should have a person experienced in handling data privacy and security responsible for preparing appropriate notification language and other communications. The business should also be ready to respond to potential media inquiries.

A public relations firm might also be engaged that has experience in handling data security breach incidents. Media notification may be required under HIPAA. Even if the data breach is handled with minimal legal risk, the mere reporting of such a breach by the media can be damaging to a business's reputation. A good communications plan is an important step in reassuring consumers about containment of the breach and security going forward. How will all of this be communicated to individual consumers and the public?

Who Is Notified? Depending upon the nature of the security incident and data breach, and the applicable federal, state, or international law, the business may need to notify individuals, regulators, credit reporting agencies, state attorneys general, the media or law enforcement. The business may also have a contractual obligation to report or notify another party or their insurance carrier of a security incident or data breach. A material data security breach may also need to be reported in SEC documents. In some

cases, however, the incident may not need to be reported at all. It is critical that knowledgeable privacy professionals be engaged early in the initial determination of whether a breach has occurred and if a legal notification obligation is triggered by any laws.

Mitigating Risk By Contract

Commercial agreements frequently contain provisions that cover data privacy issues including data ownership, rights to use data, restrictions on use, limitations of liability, and indemnities. Specific language may be required in agreements to comply with HIPAA, GLBA, or other federal and state laws. If personal information or PII is involved, the contract should cover the relevant issues regarding the collection, use, and sharing of such information. If personal information of residents outside of the United States is involved the agreement may need to comply with the EU Data Directive, the GDPR, and other international laws regarding the cross border transfer of data. Do Model Contracts, or Binding Corporate Rules [discussed on page 124] apply? What about the Privacy Shield? Is the vendor used to perform data processing compliant with international laws? The agreement may also need to allocate the risk and responsibility of both parties in the event of a data breach. How and when will a security incident or breach be communicated?

Data privacy and security issues should not be limited to agreements with technology vendors. The 2013 breach of data security at Target was the result of password credentials being shared by a HVAC vendor. Appropriate technical and administrative safeguards should be implemented and followed by outside contractors as well as employees.

Vendor Qualifications and Management. Even the best physical, technical, and administrative safeguards can be called into question when a company allows a third-party vendor to interact with personal data maintained by the company and if the vendor does not have adequate data security protections in place.

When assessing risk posed by third-party vendors, it may help to take a complete inventory of all the vendors currently used by the business. An audit of third party vendor agreements can assess their ability to protect data and assure that contractual provisions are in place to ensure compliance. The same due diligence and contract review should be done with all new vendors. Companies should also detail the type of information being transmitted to or stored by various vendors and assess the security of that transmission. What security firewalls or encryption is provided by the vendor? What else can be done to address any security weaknesses?

Vendor contracts should at a minimum include limitations on any use of the data that is collected to your specific purpose. Security controls should be reasonable and appropriate for the work performed. Incident response and reporting provisions, audit rights, and indemnification and insurance clauses should all be included. Vendors who handle sensitive personal information might be required to carry "cybersecurity insurance" to cover data breaches, data loss, and related damages. In some cases it may be appropriate to have certain vendors regularly complete a data security questionnaire or undergo an audit of their data security practices and facilities. Does the vendor meet standards of SSAE16, SOC II, ISO or have related data security certifications? Comply with NIST?

Insurance

A business can also manage some of its own data privacy risk through insurance. A review of current insurance policies should determine what coverage the business is entitled to relative to business interruption, crisis management, costs related to breach notification, response to government investigations, restoration of computer systems and data recovery, computer fraud and criminal activities. Third party liability coverage such as general business liability policies, professional liability (E&O) policies, and directors and officers liability policies should be reviewed.

Special "niche" cyber liability and other new media policies are increasingly appearing on the market. In some cases insurers make it clear that "electronic data" is not covered by the policy and some courts have found that "electronic data" is not tangible property that can be damaged. Have someone knowledgeable in data privacy and security risks and insurance review your current insurance and any contemplated purchase of additional coverage.

Questions to ask when looking for a policy include: Does the insurance cover costs to respond to government investigations? Breach notifications and related costs? Is the computer network and system of the business covered? What about mobile devices? Laptops? Tablets? The insurance policy should be scrutinized to make sure that it covers all of the business activities and relevant technology. For example, does a software provider of cloud services have insurance coverage for the network under its control as well as the computer networks operated by a third party for which it provides cloud services?

Finally, commercial agreements often include insurance requirements and indemnification obligations. Make sure that these contract provisions cover potential data privacy and security risks such as service interruptions, notification costs, data breach, and data loss.

Physical Safeguards/Office Design

Privacy considerations are not limited to the computer system, network, and related technology. The physical or architectural design of an office or business space can be critical. Staff who have access to sensitive data should maintain locked files and locked office doors. Basic office configuration should not be overlooked. The use of shared printers, copiers and fax machines are potential sources for inadvertent data breaches. A shared printer may allow an employee to unknowingly access sensitive personnel information that they are not authorized to see. When planning office space

consider the type and sensitivity of data and information that might be stored in each location. The use of security cameras and locked storage rooms may also be necessary as part of any office design to make sure that customers and employees are not permitted in restricted areas where personal data is maintained.

Storage And Maintenance Of Electronic Data

Most people think of computer systems and related technology where electronic data is stored as the place where a data breach is likely to occur. A review of information technology, however, involves more than just the placement and storage of the servers and computers that contain that private data. What anti-viral software is used by the business and where is it installed? Are all systems secure, and backed up including the servers, laptops and computers where the data is stored? Is access limited to the right persons? Remote back-up locations may help with disaster recovery and ensure the security of data. What about vendor agreements for any data that is maintained off site? As noted above third party vendor agreements should include appropriate privacy and security obligations. Is personal information stored in a cloud and if so, what security safeguards are in place?

Document Retention - Storage And Maintenance Of Hard Copies

Paper documents that contain sensitive personal information or confidential and proprietary business information also require attention. Hard paper copies of sensitive and confidential data should not be left out on desks, and printers should be in close proximity to the individuals printing and using this data. Paper copies of any documents should remain in locked filing cabinets or locked storage rooms.

Formal document retention and destruction policies should be implemented. These policies cover which documents are stored, for how long, and how such documents will be disposed of after the time has expired. There may be specific laws that apply to the type of information collected and stored such as employment records. Docketing systems and procedures should be put in place to monitor compliance with these laws. One of the largest settlements with the FTC resulted from the disposal of personal information in an unsecured dumpster. [See *In Re CVS Caremark* discussed on page 25.]

Technical Safeguards

When implementing a data privacy and security program include legal, information technology, operational, human resources, and business expertise and follow recognized standards such as those released by the National Institute of Standards and Technology. (NIST) or the International Standards Organization (ISO). [See discussion of NIST on pages 52-53.]

A thorough review and audit of the technology and systems used by the business should be conducted by a firm or person with experience in data security. A penetration or attempted hack of the system can highlight potential weaknesses of a system. A business might consider hiring a firm that also has experience in penetration testing. This test simulates attacks from a malicious source and can evaluate how vulnerable the system is to hackers. Based on this test the vendor can then recommend steps to enhance security.

Advances in security continually become available and businesses need to stay current and ahead of those who might seek to penetrate their systems. Keeping up with the technology can be difficult, but it is essential. Cloud computing and the growing use of mobile devices to conduct business have added another layer of complexity to the ways a business must maintain data security.

An example of this vulnerability was "Heartbleed," a flaw discovered in OpenSSL the open source encryption standard used by many websites to transmit secure data. Because of a programming error in OpenSSL, a Google security researcher found that it would be relatively easy to trick the computer to send data stored in memory that included usernames, passwords, credit card numbers, and encryption keys. Once this flaw was discovered a business using OpenSSL should have immediately changed passwords and upgraded to the new version without the Heartbleed bug. Heartbleed is a prime example of the need to closely monitor what is happening in the technical world of data privacy and security. The NIST Framework discussed above can also be a useful tool for a business developing technical safeguards.

Encryption, Encryption, Encryption

One of the basic steps to mitigate risk under most data privacy and security laws is to encrypt the data. The practice of "encrypting" data to be unreadable by an interceptor has long been an accepted practice of securing data that is transmitted electronically. For example, encrypted data will not be susceptible to a data breach that triggers notification under HIPAA. Certain states (including Minnesota) may not consider the loss of encrypted data to be a data breach or a loss of data that requires notification under the statute. [See Minn. Stat. § 325E.61 on pages 87-88.] One of the first questions asked in any security incident or data breach investigation is therefore whether or not the data was encrypted. Businesses should be sure to encrypt personal data transmitted over unsecured networks or stored on portable devices. Encryption technology is continuously changing so a business should also make sure that they are using the most current encryption technology.

Limit Access

Limiting the number of people that can access certain personal data through a company network or system can make it much easier to determine if or when a breach occurred. Businesses should set up layers of access passwords, keys, and firewalls so that access is limited to only those who have a need to access the data for a specific purpose.

Limit Data Collected

This may seem basic but some businesses collect information that they do not even need. Many businesses continue to collect data because it has "always been done that way." The Minnesota Health Insurance Exchange (MNsure) experienced some early flak after one of the staff accidentally sent an email file to a broker including the social security numbers of 2,400 insurance agents. The file was not encrypted. Social security numbers and some of the other information contained in the transmitted excel spreadsheet were not even necessary to be collected and stored by the agency.

A business should only collect information for which the business has a specific need. For example, why ask for the social security number from a person if you have no need for it? This collection and storage of unnecessary personal information is only an invitation for potential liability.

Remote Access

Cloud computing and the expanded ability for employees to access information remotely through laptops, tablets, smartphones, and other mobile devices requires that more attention be paid to building security walls around data that should not be accessed by every user. More and more businesses are allowing employees to use their own personal devices for both personal and business use. In such cases the business might consider implementing an appropriate Bring Your Own Device (BYOD) policy to make sure that data privacy and security issues are covered.

BYOD refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace and to use those devices to access privileged company information and applications. [See page 74 and the *Legal Guide to Use of Social Media in the Workplace* for more discussion of BYOD and employment related issues.] A challenging but important task for any business who utilizes BYOD is to develop a policy that defines exactly what sensitive business information needs to be protected, which employees should have access to this information, and then to educate all employees on this policy.

What if an employee uses a smartphone to access the company network and then loses that phone? Someone outside the business could retrieve any unsecured data on that phone. Another potential issue is with an employee who leaves and takes the device with them along with proprietary business information and personal and sensitive data.

Administrative Safeguards

Training is an integral part of any privacy program.

Even the most secure systems can still be penetrated or hacked so the focus should not be limited to technical solutions. The failure of an employee to follow appropriate practices when working within a secure system or network can place personal data along with proprietary information at risk.

As noted above, in the case of Target, an HVAC vendor somehow disclosed a secure password to the person responsible for the extensive malware attack and data breach affecting millions of customers. While administrative safeguards are sometimes an afterthought in privacy compliance, these audits, policies, procedures, and training are the backbone of any successful and sustainable data security system and should be given early and proper attention.

Policies and Procedures. Written policies and procedures are the first step in implementing any compliance program and adequate data security safeguards. Having appropriate and well understood technology use, data privacy, and social media policies and procedures may mitigate the risks of non-compliance with privacy laws and regulations. (See pages 72-74)

Training/Employee Communications. A formal written compliance program with extensive policies and procedures is meaningless, unless the employees are trained and familiar with proper practices and procedures. Employees must be educated on data privacy practices and procedures of the business, including the appropriate use of technology, so as not to compromise any security or protection of data. Email and social networking can all be used in ways that may pose risks to the business. Employees should be trained on how data can be transmitted or stored on personal devices. What is the business policy regarding the use of personal devices for business purposes? Does the business supply the device? Is a BYOD Policy necessary? Employees may not realize what responsibilities they have to protect and secure business and customer data. Training should be revisited on a regular basis as policies, procedures, and laws may change. New employees should have data privacy and security training as part of any orientation.

Overall awareness in data privacy and security can also be enhanced through regular communications with employees via newsletters, email, or other communications. Frequent communication on data privacy and security related topics will help promote a culture and further understanding of the importance of privacy and data security to the business.

Employee Background and Compliance Checks. Data breaches or security incidents might not be committed by someone from the outside but by employees. The type of customer data stored or the industry in which the business operates may necessitate more comprehensive background checks of employees. [See page 63.]

After an employee has joined the company, periodic compliance checks can be helpful in assessing the effectiveness of certain training programs or the individual employee's ability to follow the procedures and protocols in place for handling sensitive data.

Experienced Privacy Professionals. It would be wise for a business to develop relationships with professionals who have experience handling data privacy and security issues including legal counsel, data privacy and security professionals, public relations, and technology/computer forensics consultants. It will be of some comfort for a business to know they have taken appropriate actions before, during, and after the security incident or data breach.

FINAL THOUGHTS - WHAT IS NEXT?

What is the Harm? When an individual has their personal information disclosed what harm or injury has occurred and what right does that person have to bring a lawsuit for damages or other remedies? On November 2, 2015, the United States Supreme Court heard oral arguments in ***Spokeo v. Robins***, a case that may have a significant impact on privacy litigation. Spokeo operates a commercial website that discloses to the public personally identifiable information, including contact data, marital status, age and wealth. Thomas Robins sued Spokeo for disclosing inaccurate information about him that allegedly harmed his employment prospects and was a violation under the Fair Credit Reporting Act (FCRA). Spokeo initially won dismissal of the case in 2011 based on no "injury-in-fact" with the judge finding Mr. Robin's claims "speculative" and "implausible". Robins did better on appeal where the judge found the FCRA violation sufficient to move the case forward, setting up the current appeal before the Supreme Court. The question at issue before the Court is whether or not a person who has had their personal information disclosed online, with no further harm, has a right to sue? If the Court finds no right to sue it will be a major blow to privacy advocates. If however the Court determines that Mr. Robins has the right to sue, the plaintiff's bar may rejoice as class action lawsuits are filed against companies which handle personal information online.

All Businesses Vulnerable. There is no reason to believe that the volume of data security breaches will decrease in the months and years ahead. Any business, large or small, that holds private data is vulnerable to a data security breach. While large companies may have a team of professionals who deal with data privacy and security, even small- and medium-sized businesses can take some cost effective measures to minimize the risk of a data breach and to ensure compliance with data privacy and security laws.

Social Media. The increasing use of social media as a business tool and by employees has led to unique privacy issues and risks. Many of these issues are covered in the section of this Guide entitled Privacy and the Employment Relationship [See pages 57-74.] Gray Plant Mooty, in collaboration with the State of Minnesota, prepared **A Legal Guide to Use of Social Media in The Workplace**. This **Social Media Guide** covers privacy and other issues related to the use of social media as a business tool. A copy of both the **Social Media Guide** as well as this **Privacy Guide** are available for free from the Minnesota Department of Employment and Economic Development or Gray Plant Mooty. Copies are also available as a download from either http://www.gpmlaw.com or http://mn.gov/deed/newscenter/publications/guidebooks/biz-guidebooks.jsp.

Lessons Learned. Every business faces the risk of a data security breach. The breach will likely be accompanied with operational challenges and unfortunately may include a complicated analysis of legal compliance and appropriate actions. It may also be found that the breach could have been prevented though some of the steps identified in this Guide such as more effective data security policies and procedures, human behavior, or technical safeguards. Unfortunately, the best lessons learned are from real experiences.

Privacy is Good Business Strategy. Providing adequate data privacy and security is simply good business. As customers become more and more aware of the vulnerability of their data, the investment by a business in data privacy is not just an investment in technology and better security. It is an investment in customer service and sales and marketing.

Businesses are already taking a closer look at the security plan and safeguards in place before signing agreements with a party that might be handling their data. Customers may select the business with a stronger track record for security and elect to forgo websites or businesses that offer more limited data privacy and security. Businesses that take data privacy and security seriously may see a competitive advantage over businesses that do not.

Legal Landscape Unpredictable. Federal and state lawmakers continue to grapple with ways to strike a balance between new technology, the free flow of information that has become ubiquitous to e-commerce, the proliferation of social media, and the protection of personal information. The patchwork of state and federal data privacy, especially in the area of breach notification laws, has resulted in many new federal and state legislative proposals.

In 2014 Minnesota became the first state to require that a "kill switch" be installed by cellphone manufacturers. All new cellphones sold in Minnesota after July 2015 must now be enabled with a function that remotely disables the phone.

Federal data privacy and security legislation continues to be discussed but the passage of any comprehensive law is unlikely. [See pages 53-56.] Businesses will still have to contend with the patchwork of state laws and federal acronyms.

The Court of Justice of the European Union decided that search engines like Google® must remove the link between search results and a webpage if it contains information that an individual deems offensive or damaging to his or her reputation. Google has already been flooded with thousands of requests from individuals filing claims to have certain information about them be deleted.

Closer to home, this so- called "right to be forgotten" has also been codified in a new California law that allows anyone under the age of 18 the right to have content they posted online removed or deleted. This law, known as the California Eraser law, became effective January 1, 2015.

Global Compliance. The Safe Harbor Agreement has been replaced with the so-called Privacy Shield and the new GDPR goes into effect in 2018. It is not too soon to be prepared for compliance with these new EU laws. If your company does business in Canada it better become familiar with the new Canadian Anti-Spam law as penalties for non-compliance will be severe.

Data Monetization. Companies are rushing to invest significant resources to collect, analyze, and monetize vast new arrays of transactional, locational, and behavioral data from and about customers, patients, device users, equipment sensors, and other data sources. At the same time the FTC is raising concerns about "data brokers" who may become targets of the FTC. [See FTC report issued May 2014 entitled "A Call for Transparency and Accountability."] Big data and brokers are likely to be a focus of FTC investigations.

It is impossible to predict how the legal landscape relative to data privacy and security will look in the next few months or years to come. We are confident however that there will likely be changes at the state, federal, and global level. We monitor these developments on a daily basis and when significant changes in data privacy and security law occur we will try and update this Guide. We encourage you to periodically check the websites [http://www.gpmlaw.com and http://mn.gov/deed/] for any such updates.

PRIVACY LAW TIMELINE

- **400 B.C.E Hippocratic Oath** duty of medical confidentiality
- **1361 English Justices of the Peace Act** criminalizes eavesdropping/peeping toms
- **1789 United States Constitution**
- **1884** Kodak introduced Brownie camera used by journalists
- **1890** ***The Right to Privacy*** law review article by Warren and Brandeis
- **1928** ***Olmstead v. United States,*** 277 U.S. 438 (1929) wiretapping ok-
- **1948 UN Universal Declaration of Human Rights** includes privacy
- **1950 European Convention on Human Rights** has right to privacy
- **1960** Privacy law review article by torts scholar William Prosser
- **1965** ***Griswold v. Connecticut***, 381 U.S. 479 (1965)- right to contraceptives.
- **1967** ***Katz v. United States***, 389 U.S. 347 (1967)- reasonable expectation of privacy
- **1970 Hesse [German] Data Protection Act** – first comprehensive data privacy law
- **1970 Fair Credit Reporting Act**
- **1973** ***Roe v. Wade***, 410 U.S. 113 (1973) privacy right includes right to abortion

- **1973 Fair Information Practices** privacy principles issued by HEW(former HHS)
- **1974 The Privacy Act** regulates federal government use of data
- **1974 Family Educational Rights and Privacy Act**
- **1977** ***Whalen v. Roe,*** 429 U.S. 589 (1977) right to information privacy
- **1980 OECD Guidelines**- widely adopted fair information principles and practices
- **1986 Electronic Communications Privacy Act**
- **1986 Computer Fraud and Abuse Act**
- **1988 Video Privacy Protection Act**
- **1994 Drivers Privacy Protection Act**
- **1996 HIPAA**
- **1996 EU Data Protection Directive**
- **1998** First FTC actions regarding privacy policies
- **1998 Children's Online Privacy Protection Act**
- **2000 E.U-U.S. Safe Harbor Agreement**
- **2001 PIPEDA** enacted in Canada
- **2003 SB 1386** California enacts first state data breach security notification law
- **2004 FACEBOOK**
- **2004 PCI-DSS debuts**
- **2009 HIPAA/HITECH Act** establishes breach notification for covered entities
- **2011** ***United States v. Jones,*** 132 S.Ct. 945 (2012) installing GPS illegal search
- **2013 Edward Snowden** reveals classified NSA documents to Glen Greenwald

- **2014** ***Riley v. California***, 573 U.S. ____(2014) contents of cellphone protected
- **2014 Right To Be Forgotten** found by Court of Justice of EU
- **2014 Canada Anti-Spam Law** effective July 1, 2014
- **2015 California Eraser law** effective January 1, 2015
- **2015 USA Freedom Act** enacted June 2, 2015 places new limits on bulk collection of telecommunications metadata on US Citizens
- **2015 US-EU Safe Harbor Invalid** October 6, 2015 European Court invalidates.
- **2015 EU General Data Protection Regulation** December 17, 2015 agreement reached on text
- **2015 Cybersecurity Information Sharing Act** ("CISA") enacted December 18, 2015.
- **2016 Privacy Shield** February 2, 2016 agreement in principle reached on new data transfer framework
- **2016 Judicial Redress Act** signed into law by President Obama on February 24, 2016 allows European citizens to sue in US courts in the event their personal information is misused. This law was key to the Privacy Shield moving forward as a replacement to the invalidated Safe Harbor Agreement.

SOURCES OF INFORMATION ON DATA PRIVACY AND SECURITY

There is an abundance of materials available to a business looking for guidance in this area.

One of the most valuable sources of information is the FTC website, http://www.ftc.gov, where you will find materials on most of what we cover in this Guide, including the following:

Federal Trade Commission. "CAN-SPAM Act: A Compliance Guide for Business." Sept. 2009.
https://www.ftc.gov/system/files/documents/plain-language/bus61-can-spam-act-compliance-guide-business.pdf

Federal Trade Commission. "Marketing Your Mobile App: Get it Right From the Start." Apr. 2013.
https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf

Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers." May 2012.
https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

Federal Trade Commission. "Self-Regulatory Principles for Online Behavioral Advertising." Feb. 2009.
https://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral

Federal Trade Commission, "Data Brokers- A Call For Transparency and Accountability." May 2014.

Other government sites and publications that provide privacy related information:

California Office of the Attorney General. Cybersecurity in the Golden State. Feb. 2014.
https://oag.ca.gov/cybersecurity

White House. Consumer Data Privacy in a Networked World. Feb. 2012.
http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

U.S. Department of Commerce, National Telecommunications and Information Administration. Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework. Dec. 2010.

See also:

National Institutes of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Feb. 2014.

Minnesota Department of Employment and Economic Development and Gray Plant Mooty. *A Legal Guide to the Use of Social Media in the Workplace.* July 2013.
http://www.gpmlaw.com/portalresource/A_Legal_Guide_to_the_Use_of_SOCIAL_MEDIA_IN_THE_WORKPLACE.pdf

ASRC. "CARU Safe Harbor Program and Requirements."
http://www.asrcreviews.org/caru-safe-harbor-program-and-requirements/

- The Better Business Bureau Children's Advertising Review Unit Children's Online Privacy Protection Act "Safe Harbor

Program" offers steps to follow to ensure compliance with FTC regulations.

Other Useful Websites:

"Electronic Frontier Foundation."
https://www.eff.org

"EPIC – Electronic Privacy Information Center."
https://www.epic.org

- EPIC is an independent non-profit research center that works to protect privacy, freedom of expression, democratic values, and to promote the public voice in decisions concerning the future of the internet.

"International Association of Privacy Professionals."
https://www.privacyassociation.org

- The International Association of Privacy Professionals (IAAP) is an organization of privacy professionals that offers comprehensive global privacy resources for those who help organizations manage and protect their data.

"Privacy International."
https://www.privacyinternational.org

"Privacy Rights Clearinghouse."
https://www.privacyrights.org

For information on "model contracts" see http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

For information on the Canadian anti-spam law CASL see http://www.ic.gc.ca/eic/site/030.nsf/eng/h_00039.html

Selected Books, Articles and Treatises on Privacy:

Angwin, Julia. Dragnet Nation: *A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, Times Books, 2014.

Breaux, T., Introduction to IT Privacy-A Handbook for Technologists, Portsmouth, NH, IAPP, 2014.

Corporate Counsel's Guide to Privacy. Eagan, MN: West, 2011.

Guidebook to the Freedom of Information and Privacy Acts. Eagan, MN: Thomson Reuters/West, 2013.

Solove, Daniel J. *Nothing to Hide: the False Tradeoff Between Privacy and Security*. New Haven, CT: Yale University Press, 2011.

Solove and Hartzog, FTC and the New Common Law of Privacy, 114 Columb. L. Rev. 583 (2014).

Warren, Samuel and Brandeis, Louis. "The Right to Privacy". 4 Harvard Law Review 193, 1890.

Weikers, Ronald N., and Ronald N. Weikers. *Data Security and Privacy Law.* St. Paul, MN: West, 2011.

Westin, A. *Privacy and Freedom*, New York, New York: Atheneum, 1968.

Wolf, Christopher, and Kristen Matthews. *A Practical Guide to the Red Flag Rules: Identifying and Addressing Identity Theft Risks.* New York: Practicing Law Institute, 2008.

ISBN 1-888404-71-X