PRIVACY AND DATA SECURITY: NEW CHALLENGES OF THE DIGITAL AGE

By Cameron G. Shilling

The digital age has heralded explosive growth in the amount of personal information created, stored and transmitted on computers and mobile devices, over the Internet and broadband, and on popular social media sites. The very same technological advancements that have defined the times also pose serious threats to our personal privacy and information security.

Despite the importance of the interests at stake, no comprehensive or consistent set of rules currently govern privacy and data security in the United States. A patchwork of federal and state statutes and cases govern different industries, various types of conduct, and different kinds of personal information. Frequently complex and confusing, this patchwork often fails to provide clear answers to the most pressing questions.

Though daunting, these new challenges are manageable. To do so, businesses should (1) identify the laws that apply to them, (2) assess the privacy and security risks that may arise in their operations, (3) create and implement data security policies that comply with the applicable laws in light of norms and practices in this area, and (4) adopt information-use policies governing acceptable use of their computer systems and electronic devices. This article aims to help businesses and their legal counsel successfully start this process.

A. Overview of Privacy and Data Security Law

Laws governing privacy and data security first arose to counteract threats of identity theft and theft of financial information, such as the Fair Credit Reporting Act of 1970 (FCRA) and the Gramm-Leach-Bliley Act of 1999 (GLB).3 (See Sections B and C below) Another landmark federal law created protections for health and medical information, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). (See Section D) In 1986, Congress also enacted two important laws prohibiting the interception and unauthorized access and use of information communicated and stored electronically, the Electronic Communications Privacy Act (ECPA) and Stored Communications Act (SCA). (Section F)2

In addition to federal laws, the states have proliferated statutes on data security. Most states, including New Hampshire, require businesses to notify affected individuals and certain government agencies in the event of a data security breach. In addition, Massachusetts, has adopted regulations that go one step further, requiring businesses to implement data security policies designed to avoid breaches. (Section E)

The limited case law in this area has focused primarily on privacy issues, typically arising under the federal Constitution. These cases are particularly instructive with respect to common law protections, such as claims for invasion of privacy. (Section G).

Dispersion and disparity in the law have sparked the recent introduction of a number of bills in Congress, which would create more uniform national rules for privacy and data security. Such legislation is sorely needed to foster certainty and avoid contradiction in an area of the law that is critical to the development of the digital economy. (Section H)

A detailed analysis of all of the federal and state privacy and data security rules is beyond the scope of this article. The most significant statutes and recent United States Supreme Court cases are reviewed, so that businesses and their counsel can become more familiar with this area, and can start the process of becoming compliant with applicable laws.

B. Credit and Consumer Reporting Information

Considered the first privacy law in the United States, the Fair Credit Reporting Act (FCRA) and its counterpart, the Fair and Accurate Credit Transaction Act of 2003 (FACTA), govern privacy and security for credit and consumer reporting information.

Businesses that do not routinely deal with credit matters often assume they are not subject to FCRA or FACTA, or believe they need to comply only if they obtain a consumer report, such as for employment purposes. However, the “Red Flags Rule” under FACTA, which became
effective on June 1, 2010, broadly expanded the number of businesses and types of information subject to privacy and security rules. Many companies need to re-evaluate whether their business practices fall within the Red Flags Rule or other FACTA regulations.

FCRA governs consumer reports prepared by consumer reporting agencies. These terms broadly encompass any business that regularly collects or maintains information bearing on a consumer’s creditworthiness, but the statute also exempts such information if it is compiled solely with respect to transactions between the business and consumer.

FCRA also applies to users of consumer reports. A user is any person or entity that receives a consumer report and evaluates a consumer based on it, whether the report is received directly from a consumer-reporting agency or indirectly through another person or entity.

Because the purpose of FCRA is to protect the privacy of personal financial information, the statute restricts the dissemination and use of consumer reports. A business that would like to obtain a consumer report must either obtain written consent from the consumer, or certify to the consumer reporting agency that the prospective user is requesting the report for a statutorily permitted purpose. Such purposes include an employment decision, a legitimate business need related to a business transaction, and a credit transaction.

FCRA also requires a user of a consumer report to notify the consumer if the user takes any adverse action based on information in the report. An adverse action is any decision “adverse to the interests of the consumer,” like a refusal to hire, any other decision “that adversely affects any current or prospective employee,” a refusal to give credit, a termination or unfavorable change of terms of an account, or a denial or cancellation of insurance.

In enacting FACTA, Congress’ primary purpose was to protect consumers from the growing threat of identity theft. The most significant new regulation under FACTA, the Red Flags Rule, requires all financial institutions and creditors that offer or maintain any covered account to “develop and implement a written Identity Theft Prevention Program . . . designed to detect, prevent, and mitigate identity theft.”

While the meaning of “financial institution” is straightforward, the definition of “creditor” encompasses businesses that may not consider themselves to be creditors. The term includes every business that “advances funds to or on behalf of a person,” including a customer or employee, “based on an obligation of the person to repay the funds.”

“Covered account” has a similarly broad meaning. It includes any account “primarily for personal, family, or household purposes . . . designed to permit multiple payments or transactions,” including things like savings and checking accounts, accounts to pay bills, cell phone and cable television accounts, and other similar accounts. The term also includes a broad catch-all encompassing any account “for which there is a reasonably foreseeable risk to customers . . . from identity theft.”

Given the ramifications of identity theft and the penalties for violating FACTA, one might expect the Red Flags Rule would expressly outline the specific provisions necessary for an identity theft prevention program. The problem is that no such general outline would be appropriate for all businesses, because identity theft threats (like data security matters generally) differ depending on the operations and information gathered by each business.

The Red Flags Rule instead requires businesses covered by the rule to adopt “reasonable policies and procedures” designed to identify patterns, practices and activities that demonstrate the possibility of identity theft (i.e., red flags), detect the red flags when they occur, and respond appropriately. The rule was purposefully created in an open-ended manner, so that businesses must undertake the process necessary to identify the red flags specific to their operations and design a program suited to their needs and capabilities, similar to the process necessary to create and implement a data security plan under other laws. For businesses that face a particularly low risk of identity theft, the Red Flags Rule also permits and provides a more simplistic method to assess the risks and adopt an appropriate program.

C. Financial Information

The Gramm-Leach-Bliley Act arose from efforts to modernize the financial services industry, and to scale back the tendency of some banks to share information with telemarketers. GLB thus permits a financial institution to share non-public personal information about consumers and customers with affiliates, but prohibits such information-sharing with non-affiliated entities, until the financial institution has given notice to consumers and customers of its intent to do so and offered an opportunity to opt out.

Non-public personal information is broadly defined to encompass any information provided by consumers or customers “to obtain a financial product or service” from the financial institution. A consumer is an individual who obtains “financial products or services” from a financial institution “used primarily for personal, family, or household purposes.” A customer, by extension, is a consumer with whom the financial institution has a “continuing relationship.” Financial institutions have greater duties to customers than they do to consumers.

GLB contains both privacy and security protections for non-public personal information held by financial institutions. It is considered the first law in the United States to impose comprehensive security requirements for information, and has served as a model for other state and federal data security laws.

GLB’s “Privacy Rule” requires a financial institution to provide a notification to customers of its privacy practices both at the time it establishes a relationship with customers and at least annually thereafter. A financial institution may provide a simplified notification to consumers who are not customers.

GLB’s “Safeguards Rule” mandates that financial institutions adopt “administrative, technical, and physical safeguards” designed to ensure the security and confidentiality of records that contain nonpublic personal information, protect against any anticipated threats to the security or integrity of such records, and protect against unauthorized access to or use of such records which could result in substantial harm or inconvenience to a consumer or customer.
“comprehensive information security program” should be tailored to the size and complexity of the financial institution, the nature and scope of the institution’s activities, and the sensitivity of the nonpublic personal information maintained by it. 

GLB’s Safeguards Rule outlines the five elements necessary for an appropriate information security program under that law. First, the financial institution must designate an employee or employees to coordinate the program. 

Second, the financial institution must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to manage these risks. At a minimum, such an assessment must consider risks in each area of business operations, including (1) employee training and management, (2) information systems, and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures. 

Third, the financial institution must design and implement safeguards to control the risks identified through the risk assessment, and regularly test or monitor their effectiveness. 

Fourth, the financial institution must oversee service providers that possess its non-public personal information. This obligation includes (1) taking reasonable steps to select and retain vendors capable of maintaining appropriate safeguards, and (2) requiring vendors by contract to implement and maintain such safeguards. 

Fifth, the financial institution must evaluate and adjust its information security program in light of the results of testing and monitoring, changes to operations, and other circumstances that may affect the effectiveness of the program. 

D. Health and Medical Information

The privacy and security of health and medical information are governed by some of the most comprehensive and complex federal statutes, the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health Act of 2010 (HITECH). 

HIPAA and HITECH specify the permissible uses of protected health information (PHI) mandate privacy notices by covered entities, impose requirements for services providers (called “business associates”), and create information security requirements for electronic PHI (ePHI). Covered entities are health plans and clearinghouses, and “health care providers who transmit any health information in electronic form in connection with [certain] transactions.” While employers are not expressly included in the list of covered entities, employers can qualify as covered entities in their roles as sponsors of group health plans. 

HIPAA’s Standard for Privacy of Individually Identifiable Health Information (Privacy Rule) prohibits a covered entity from using or disclosing PHI in any way not expressly permitted by the rule. HIPAA’s Privacy Rule generally allows a covered entity to disclose PHI to the individual, and to use and disclose PHI for treatment of the individual, payment, or “health care operations” of the covered entity. The rule also permits various other uses and disclosures of PHI if the individual authorizes the use or disclosure in writing, or if the covered entity notifies the individual in advance and the individual does not object. 

When HIPAA permits use or disclosure of PHI, its Privacy Rule generally requires covered entities using PHI (or covered entities making or fulfilling a request to disclose PHI) to use “reasonable efforts” to limit the use or disclosure of PHI “to the minimum necessary to accomplish the intended purpose.” To comply with this requirement, covered entities must, “to the extent practicable,” use or disclose PHI from a “limited data set,” which means information from which the covered entity has removed personally identifying information (such as names, addresses, email addresses, phone and facsimile numbers, social security numbers, account numbers, and biometric identifiers). 

HIPAA’s Privacy Rule permits individuals to access, inspect and obtain a copy of their PHI records. An individual also can ask a covered entity to amend or modify his or her PHI; has a right to an explanation if the covered entity decline to do so; and may submit statements disagreeing with any denial of an amendment or modification of his or her PHI. Finally, an individual has a right to obtain an accounting of disclosures of his or her PHI made by a covered entity within the six years before the request is made. 

The Health Insurance Reform Security Standard (Security Rule) under HIPAA creates detailed requirements for the security of ePHI, though it does not cover hard-copy PHI. Like other federal and state data security laws, HIPAA’s Security Rule requires covered entities to adopt reasonable policies and procedures focusing on the administrative, physical and technical measures necessary and appropriate to safeguard information. 

In addition to requiring a data security policy, HITECH mandates that covered entities, as well as entities not covered by HIPAA, provide certain notifications in the event of a breach of unsecured protected health information (unsecured PHI). While many HITECH breach-notification requirements resemble notification requirements under state laws, others are more onerous. For example, HITECH defines “breach” to include not only unauthorized access or acquisition, but also unauthorized use or disclosure, and in some instances, HITECH requires notification to not only affected individuals and government agencies, but also media outlets. 

HITECH also offers safe harbors to covered entities and other businesses dealing with breaches. For example, notification must be given only if the breach “poses a significant risk of financial, reputational or other harm to the affected individual.” In addition, notification need not be given if the covered entity or other business had implemented certain encryption technology and the decryption key was not breached. 

Almost all of the requirements of HIPAA’s Privacy Rule and Security Rule apply, either directly or indirectly, to business associates. A business associate is an entity that performs or assists with any “function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, qual-
ity assurance, billing, benefit management, practice management, pricing, . . . or any other function or activity regulated by” HIPAA. 32 HIPAA’s Privacy Rule requires covered entities to enter agreements with business associates contractually requiring them to comply with certain provisions of the rule. 33 HITECH similarly imposes most of HIPAA’s Security Rule and HITECH’s rules directly on businesses associates, including the mandate to adopt a data security policy. 34

D. State Data Security Laws

Nearly every state in the United States requires notification in the event of a data security breach. New Hampshire’s statute is a typical example. While most breach-notification laws are similar, they are not all the same, and the differences between them often create compliance difficulties when a breach affects individuals in multiple states. Massachusetts law goes further, requiring every business to implement a written information security policy, or “WISP.” In this regard, the Massachusetts regulations are similar to the requirements under GLB and HITECH.

While each state’s data security law defines the “personal information” protected by the law, definitions differ. New Hampshire defines personal information as including the first name (or initial) and last name of the individual, in combination with (1) social security number, (2) driver’s license or other government issued identification number, or (3) account number, or credit or debit card number, with the password or the security or access code necessary to access the account. 35 By contrast, under Massachusetts law, the name of the individual in combination with an account, credit or debit number constitutes personal information, even without the password or the security or access code. 36 Other state statutes include additional types of information that, in combination with the individual’s name, constitute personal information, such as an email address or health information.

The requirements for a “breach” also can differ from state to state. 37 Both New Hampshire and Massachusetts require the breach to pose a certain level of harm to affected individuals before the business experiencing the breach must make notifications. 38 Other states require notification irrespective of whether the breach may harm affected individuals. 39 However, all states laws relieve businesses of the notification requirement if the compromised information was encrypted and the decryption key was not similarly compromised. 40

If a breach occurs, the business that owns or licenses the information must always notify affected individuals, typically must notify the state attorney general, and sometimes must notify other state or federal agencies and consumer reporting agencies. 41 Service providers that experience a breach usually are required to notify and cooperate with the business that owns or licenses the information, which then must notify others. 42 Notice typically may be given in writing, electronically, or (in certain circumstances) by “substitute” means. 43

Though state statutes vary as to the content of the required notice, most require the notice at least to describe the circumstances of the breach, include the date or approximate date of the breach, and specify the type of personal information compromised. 44 Some laws also require that the notice include information about how affected individuals can protect themselves, and even mandate that the business responsible for the breach pay for credit protection services. 45

The business experiencing the breach usually must give notice “as soon as possible” after learning of the breach, though some states set a specific deadline to do so. 46 All states permit notification to be delayed if giving notice would impede a law enforcement investigation. 47

Massachusetts has followed the federal approach by requiring every business that “receives, stores, maintains, processes or otherwise has access to” personal information about Massachusetts residents to “develop, implement, and maintain a comprehensive [written] information security program.” 48 The WISP must include administrative, technical, and physical safeguards properly tailored to the size, scope and type of business, the amount of resources of the business, the amount of stored data, and the need for security and confidentiality of the information. 49

The Massachusetts regulations contain meaningful detail about the measures that businesses must adopt in their WISPs. Mandatory administrative measures include (1) designating one or more employees to maintain the program, (2) identifying and assessing reasonably foreseeable risks, and evaluating and improving existing safeguards, (3) conducting ongoing employee training, ensuring employee compliance, disciplining employees who violate the program, and preventing access by terminated employees, (4) conducting due diligence before retaining service providers, and contractually requiring service providers to comply with the regulations, (5) reviewing and updating the program at least annually, and (6) conducting post-breach reviews.

NEW HAMPSHIRE’S LEADING MEDICAL MALPRACTICE FIRM.

Abramson, Brown & Dugan

The lawyers and staff at Abramson, Brown & Dugan are proud to congratulate Holly B. Haines on her selection as the recipient of the 2011 Robert E. Kirby Award from the New Hampshire Bar Foundation.

The award honors the memory of Bob Kirby, “a young lawyer of great skill, civility and good humor,” and is given annually to a practitioner “55 years old or younger who demonstrates the traits of civility, courtesy, perspective and excellent advocacy.”

Holly has demonstrated these traits on behalf of her clients at Abramson, Brown & Dugan since joining the firm in 2003. Since then Holly has focused her practice on litigating plaintiff’s medical malpractice and personal injury claims. She is the current president of the New Hampshire Women’s Bar Association and has served on the Board of Directors since 2006.

Abramson, Brown & Dugan

ATTORNEYS

1819 Elm Street, Manchester, NH
Ph: 603-627-1819, Fax: 603-666-4227
www.abhd.com

Referral fees honored.

Summer 2011 New Hampshire Bar Journal
and modifying the program accordingly.

Massachusetts’ law also requires technical steps including: (1) user authentication protocols, such as controlling data security passwords, restricting access to active users, blocking access after multiple unsuccessful logon attempts, and using unique identifier technologies (such as biometrics or token devices), (2) secure access control, such as restricting access to information technology employees who need data to perform their job duties, and assigning unique user passwords to them, (3) encrypting information on public and wireless networks, laptops and mobile devices, (4) implementing appropriate firewall, anti-virus, and anti-malware technology, and (5) monitoring for unauthorized access.

E. Electronic Communications Privacy

Electronic communication privacy is the hottest topic in this area, and also the least developed legally. While a myriad of federal and state statutes and common law touch on electronic communication privacy, the most significant rules in this area arise out of the Electronic Communications Privacy Act and Stored Communications Act.

The ECPA amended the federal Wiretap Act by creating civil and criminal penalties for the interception of electronic communications, and the use or disclose of unlawfully intercepted electronic communications. Thus, the ECPA addresses the capture of electronic communications that are in transit, but does not cover the vast amount of electronic communications stored before or after transmission, which is the province of the SCA.

The ECPA contains two exceptions vital to protect the interests of businesses. First, a business may intercept an electronic communication if at least one party consents. Such consent can be express or implied. For example, an employer may establish consent by adopting, distributing, and complying with an appropriate information use policy.

Second, a business that provides an electronic communications service may intercept communications, and may use and disclose them, if necessary to provide the service or protect the interests of the business. This can justify interception, use and disclosure by businesses of electronic communications by employees and others using systems provided by them. While not entirely clear, a business may not qualify for this exception if it does not actually host the computer system, but instead furnishes it through a third-party provider.

The SCA imposes civil and criminal on any business that accesses a computer used to provide an electronic communications service without authorization or beyond the scope of authorization. Like the ECPA, the SCA permits “the person or entity providing [the] electronic communications service,” including a business and employer, to access, use and disclose stored electronic communications on its systems.

Technological developments in the digital age have pushed the limits of the ECPA and SCA, which were enacted in 1986 — long before many such technologies existed or even could have been contemplated by Congress. Thus, while it is clear that businesses can access email and other electronic communications created, sent, received and stored in their own computer systems, the proliferation of digital age technologies — like text and instant messaging, webmail (Gmail, Yahoo!, etc.), social media (Facebook, MySpace, Flickr, etc.), Twitter and blogs — has created complicated and confusing questions for which there often are no clear answers.

For example, while a business has the right to extract from company-owned electronic devices (servers, computers, laptops, tablets, hand-helds, etc.) data in the residual or deleted spaces of the devices — like screen shots of an employee’s Gmail (and other webmail) or Facebook (and other social media) posts — the business cannot under the SCA use the passwords for the employee’s Gmail and Facebook accounts (which also commonly can be retrieved from residual space) to access those accounts directly. Moreover, businesses may not be permitted to review similar electronic communications that are privileged (such as communications between an employee and his or her attorney, or between an employee and his or her spouse), even if the communications were created and stored on company-owned electronic devices.

Businesses similarly have the right to review their employees’ text and instant messages stored on company-owned electronic devices. But, it may violate the SCA for a service provider to furnish the subscriber-business with copies of those texts or instant messages, depending on how some complicated and confusing terms in the SCA apply to the situation.

Though many issues under the ECPA and SCA remain unclear or unresolved, the United States Supreme Court recently gave businesses and employers some sage advice (and maybe even reliable precedent) when it comes to managing electronic communications privacy issues. The Court recognized that businesses and employers can create and implement information use policies, and that such policies will “shape the reasonable expectations” as to whether electronic communications on their computer systems are private.

F. Recent Supreme Court Privacy Cases

The United States Supreme Court recently decided two cases bearing on privacy rights of individuals: City of Ontario v. Quon and National Aeronautics and Space Administration v. Nelson. Both
cases involve privacy under the federal Constitution, and therefore apply directly to government agencies. The cases also are persuasive authority on common law rights generally, such as invasion of privacy claims, since such common law rights frequently rest on the same expectations of privacy as constitutional rights.

In Quon, the Police Department (Department) for the City of Ontario, California (City) had issued pagers to its SWAT team to facilitate coordination and rapid response in emergencies. Some SWAT team members, including Jeffery Quon (Quon), incurred overages by repeatedly exceeding their monthly data limits. When the Department reviewed Quon’s texts, it discovered numerous sexually explicit messages sent by him and others while on duty.

The Department had adopted and disseminated an appropriate written information use policy concerning use of Department-owned electronic devices, including use of the pagers and exchange of texts. However, the Department also had an unwritten practice of not reviewing texts, even if an officer exceeded his or her data limit, as long as the officer paid the overage. The Department had adhered to that practice, until it decided to review Quon’s texts. When the Department terminated Quon because of the content of his texts, Quon sued the City alleging that it had violated his common law and constitutional rights to privacy.

In denying the City’s summary judgment motion, the District Court Judge stated that he would have agreed with the City’s argument that Quon had no reasonable expectation of privacy in his texts, if all that had occurred was that Quon was informed “that the city considered the use of the pagers to fall within its e-mail policy, and that the city would monitor the use of its pagers. . . . All of this would have put any employee on fair notice that the communications that were transmitted over the pager were, in essence, open to the public for view.”

However, the Judge found that Quon’s expectation of privacy was “fundamentally transformed” by the Department’s “conscious decision not to enforce” its policy. The Department “in effect turned a blind eye to whatever purpose an employee used the pager, thereby vitiating [its] policy of any force or substance.” The judge therefore concluded that the Department “effectively provided employees a reasonable basis to expect privacy in the contents of the text messages they received or sent over their pagers.”

When Quon’s privacy claim went to trial, the jury found for the City, concluding that the Department reviewed Quon’s texts in the course of a legitimate workplace investigation. But the Ninth Circuit disagreed and reinstated Quon’s claim, ruling that it was unreasonable for the Department to review the content of the texts just to determine if the usage limits were sufficient. There “were a host of simpler ways to verify the efficacy” of the limit “without intruding on Quon’s rights,” the panel reasoned.

The United States Supreme Court reversed and granted judgment in favor of the City. Many practitioners expected the Court to issue a seminal decision defining the contours of individual privacy rights in the digital age. The Court declined to do so.

Writing for a unanimous Court, Justice Kennedy explained that courts “must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by [an] employer. The judiciary risks error by elaborating too fully on the implications of emerging technology before its role in society has become clear.”

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . At present, it is uncertain how workplace norms, and the law’s treatment of them, will evolve. [T]he Court would have difficulty predicting how employees’ privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable.

Despite understanding the hazards of wading into a sea of digital privacy issues, Justice Kennedy nonetheless seeded his opinion with helpful hints about some of the most important issues in this area. For example, as noted above, he recognized that an employer’s policies concerning electronic communications in the workplace “will of course shape the reasonable expectations of [its] employees, especially to the extent that such policies are clearly communicated.” In addition, the particular circumstances of each workplace also help define the contours of an employee’s legitimate expectation of privacy.

Rather than squarely address the privacy issue, the Court instead held that, even if Quon had a reasonable expectation of privacy in his texts, the Department’s investigation was nonetheless justified and appropriate. Under existing case law, the government’s warrantless search in the workplace “is reasonable if it is ‘justified at its inception’ and if ‘the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of’ the circum-

Medical Malpractice

Reis Law

With years of experience successfully representing plaintiffs in medical malpractice cases, Randy Reis welcomes the opportunity to assist you and your clients in malpractice and other personal injury matters.

603-792-0800 or 800-210-0605

66 Hanover St. Suite 203
Manchester, NH 03101
Ph: 603-792-0800

Summer 2011 New Hampshire Bar Journal
stances giving rise to the search.”

The Court found that the search in Quon was justified at its inception because “there were reasonable grounds for suspecting that the search was necessary for a non-investigatory work-related purpose,” namely, whether the character limit on the City’s contract was sufficient to meet its business needs. Similarly, the scope of the investigation was reasonable “because it was an efficient and expedient way to determine whether Quon’s overages were the result of work-related messaging or personal use.” The Court rejected the reasoning of the Ninth Circuit in this regard, stating that the Court “has repeatedly refused to declare that only the ‘least intrusive’ search practicable is reasonable.”

While there are several morals to the Quon story, one of the most important is that, even if employees or individuals have (or claim to have) a reasonable expectation of privacy with respect to electronic communications or other personal information, businesses and employers generally have the right to access and obtain information necessary to investigate workplace matters and other matters in which they have a legitimate business interest. This theme reoccurred in a similar context, with other types of personal information, in another recent privacy case, *National Aeronautics and Space Administration v Nelson*.

* Nelson* arose out of the federal government’s decision to require all contractors working at NASA’s Jet Propulsion Laboratory to undergo background checks, even though they had not been required to do so before. One question on the form given to each contractor asked whether he or she had used, possessed, supplied or manufactured illegal drugs within the last year, and (if so) to provide details about such conduct, including information about any “treatment or counseling” the contractor received. Once the contractor completed that form, the government sent out forms to former employers, landlords, and references. Some of the questions on that form asked whether those individuals had any reason to question the contractor’s honesty or trustworthiness, and whether they had any information about the contractor’s violation of the law, financial integrity, abuse of alcohol or drugs, mental or emotional stability, or other matters that might bear on the contractor’s suitability for government employment.

Several contractors refused to submit to the background checks and sued to challenge the government’s decision, alleging that the information sought violated their “right to informational privacy” under the federal Constitution. The District Court refused to enjoin the government’s conduct, but the Ninth Circuit reversed, holding that the question concerning “treatment and counseling,” and the questions on the forms sent to former employers, landlords and references, likely violated the contractors’ rights to informational privacy.

When the Supreme Court granted certiorari, practitioners again assumed that the Court did so either to reject any constitutional right to information privacy, or to establish clear and limited boundaries around the right. However, as in Quon, the Court declined to render a decision that could have provided significant guidance with respect to privacy law.

The Court instead assumed without deciding that a right to informational privacy exists under the Constitution, and held that the government nonetheless was justified in obtaining the information at issue in the background checks. Justice Alito, writing for a unanimous Court, recognized that “the Government has a much freer hand in dealing with citizen employees than it does when it brings its sovereign power to bear on citizens at large.” With this principle in mind, the Justices concluded that the forms “consist of reasonable, employment-related inquiries that further the Government’s interests in managing its internal operations.” The justices also rejected the notion, as they had in Quon, that the government must demonstrate that the requested information was “the least restrictive means of furthering its interest.”

Just as important (if not more important) to the Court were the “substantial protections against disclosure to the public” of the information collected by the government in the background checks. Specifically, the federal Privacy Act prohibits the government from disclosing any such information without authorization from the contractor, and imposes criminal penalties for the willful violation of its nondisclosure provisions.

The decisions in Quon and Nelson share two principles—one perpetuates the privacy issues businesses will face, while the other helps businesses manage them. First, because the Court did not decide whether the privacy rights at issue actually exist, individuals and litigants are free to assert such rights in the future, resulting in a continued divergence of lower court decisions. Second, the Court found that, even if privacy rights exist, businesses may access the information at issue if they (1) are pursuing a legitimate interest and have a need for the information, (2) do not exceed the scope of their interest or need, and (3) take appropriate precautions to protect the information from improper or unauthorized use or disclosure.

H. Recent Federal Legislation

Congress has in the past considered, but not enacted, federal legislation to govern privacy and data security generally. Several recent high-profile data security breaches, as well as widespread international
data privacy efforts, have led to the introduction of a number of credible new bills, which would broadly govern privacy and data security. 4

Given the non-partisan political support for a data security law, the relative similarity of the legislative proposals, and the need for a national law (rather than numerous different state laws), a federal data security law seems imminent. The existing proposals essentially assimilate the breach notification requirements of state and federal statutes with the requirements of GLB, HITECH and Massachusetts law for a written data security policy. 5

The existing privacy bills have been subject to less Congressional consideration and have far broader implications, thus, a national privacy law seems less imminent. 6 However, given the bipartisan sponsorship of a comprehensive and credible bill by Senator John Kerry and Senator John McCain and the high-profile nature of privacy in the digital age, such legislation surely will receive serious consideration and has a real potential to become law in the future.

G. Conclusion: Businesses Can Rise to the New Challenges

The federal and state statutes governing privacy and data security can be complicated, confusing, conflicting and unclear; and existing case law has not yet defined the boundaries of privacy rights. Amidst all of this uncertainty lies a path for businesses to follow to rise to these new challenges. To do so, businesses need to:

• identify the laws that apply to them;

• assess the security risks that arise in their operations;

• and implement data security policies that will comply with applicable law;

• and establish a forward looking security structure.

Businesses also need to assess potential privacy issues, decide how they choose (or how they must) address those issues, and implement an information use policy that complies with applicable consent laws and appropriately instructs employees about workplace expectations.

ENDNOTES

1 Cameron G. Shilling is a partner at McLane, Graf, Raulerson & Middleton, where he leads the firm’s Privacy and Data Security Group. His background is handling complex technology and business litigation, and employment matters. Cam’s experience in data security includes managing security audits, preparing and implementing written data security policies, addressing day-to-day data security issues, and investigating and remediating data security breaches. His experience in privacy matters includes creating and implementing information use policies, advising employers with respect to workplace privacy, counseling clients with respect to social media issues, addressing customer and consumer privacy, and handling claims against companies for invasion of privacy.

2 “Privacy” and “security” are confusingly similar and oftentimes overlapping concepts. Privacy typically signifies the expectation an individual has that information about the individual will not be used by or disclosed to others, unless the individual consents. Security is usually understood to mean the measures that should or must be taken to ensure information about an individual is not disclosed to those who do not have authority to access the information.

3 Congress also has enacted other statutes governing different industries, conduct, and types of information. For example, the Children’s Online Privacy Protection Act of 1998 (COPPA) prohibits unfair and deceptive acts and practices related to the collection, use and disclosure of personal information from and about children on the Internet. 15 U.S.C. §6501 et seq. The Family Education Rights and Privacy Act of 1974 (FERPA) provides an extensive array of information privacy rights to students (and their parents) who attend educational institutions that receive public funds. 20 U.S.C. §1232g et seq. The Driver’s Privacy Protection Act of 1994 regulates access to and use and disclosure of personal information contained in driver’s license and motor vehicle records. 18 U.S.C. §2721 et seq. The Control the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) is the most important law governing the transmission of commercial email, and requires online marketers to provide recipients with a method to opt out of receiving future unsolicited email. 15 U.S.C. §7701 et seq.

4 A “consumer report” is “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is intended or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized” by FCRA. 15 U.S.C. §681d(1). A “consumer reporting agency” is “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” 15 U.S.C. § 1681a(f).


6 Id. §1681b(a)(3)(A)-(C) and (F). If obtained for employment purposes, the user must disclose in writing to the consumer that it intends to obtain the consumer report and secure the consumer’s written consent to do so. Id. §1681b(b). The Federal Trade Commission (FTC) has interpreted the “legitimate business need” provision narrowly, such that the circumstances under which a legitimate business need justifies obtaining a consumer report almost always requires a pre-existing business relationship between the user and consumer, or (if there is no such relationship) a transaction initiated by the consumer.

7 Id. §1681m(a)(1). If an adverse action is taken in employment, the user also must give a copy of the report to the consumer, and notify the consumer in writing of his or her rights under FCRA. Id. §1681b(b)(3)(A).

8 Id. §1681a(k)(1)(B).

9 FACTA created the now commonly known right to obtain a free credit report once a year from each of the national consumer reporting agencies, id. §1681g(a), and the right to place a fraud alert on certain accounts. Id. §1681g(d)(2). FACTA also created the requirement to truncate credit

David S. Osman, Esq.

• MEDIATION

• ARBITRATION

• NEUTRAL EVALUATION

Martin, Lord & Osman, P.A.

Alternative Dispute Resolution

www.mlolaw.com Phone: 603.527.9154 Email: dso@mlolaw.com
and debit card numbers on receipts, id. §181b(c), guidelines for the proper disposal of consumer report information, id. §168w and 16 C.F.R. §682, and complex rules restrict the sharing of consumer report information for marketing purposes. See 16 C.F.R. §680.

10 16 C.F.R. §681.1(d)(1).

11 A “financial institution” is a “State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a certain type of transaction account.” 15 U.S.C. §1681a(a). A “creditor” is “any person who regularly extends, renew, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.” Id. §1681a(e)(5) and §1691a(e).


14 Id. §681.1(b)(3)(ii). When assessing whether an account falls within this catch-all identity fraud provision, the business should consider the following factors: “(1) The types of covered accounts it offers or maintains; (2) The methods it provides to open its covered accounts; (3) The methods it provides to access its covered accounts; and (4) Its previous experiences with identity theft.” Id. §681, Appendix A, §III(a).

15 Id. §681(d)(2). The Red Flags Rule also imposes requirements with respect to the administration of an identity theft prevention program, including assigning responsibility for the program, preparing annual reports, training relevant personnel, and periodically re-evaluating and updating the program. Id. §681, Appendix A, §IV(a) and (b). For businesses that rely on vendors with respect to covered accounts, the businesses must take steps to ensure that the vendors comply with the Red Flag Rules, including conducting appropriate due diligence, routine monitoring, and requiring compliance by contract. Id. Appendix A, §V(c).

16 The Red Flags Rule provides some helpful examples for businesses creating an identity theft prevention program. Some examples of means for detecting red flags include: (1) obtaining identifying information about and verifying the identity of a person opening a covered account, and (2) in the case of existing covered accounts, authenticating customers, monitoring transactions, and verifying the validity of change of address requests. Id. §681, Appendix A, §III(i)(a) and (b). Some examples of means for responding to red flag include: (1) monitoring a covered account for evidence of identity theft; (2) contacting the customer; (3) changing any passwords, security codes, or other security devices that permit access to a covered account; (4) re-opening a covered account with a new account number; (5) not opening a new covered account; (6) closing an existing covered account; (7) not attempting to collect on a covered account or not selling a covered account to a debt collector; (8) notifying law enforcement; and (9) determining that no response is warranted under the circumstances. Id. §681, Appendix A, §IV(a)(i).

17 The FTC promulgated a template that guides businesses through the assessment process, and helps businesses select methods to detect and respond to risks, resulting in a document that will suffice under the Red Flags Rule. While the rule does not specify which businesses may use this process, the factors to consider are whether the business knows its customers personally, provides services at customers’ homes, has had experience in the past with identity theft, and is in a business where identity theft is uncommon. See Complying with the Red Flags Rule: A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft, http://www.ftc.gov/bcp/edu/microsites/redflagrule/dy-template.shtml.

18 15 U.S.C. §6801 and §6802. A financial institution is “any institution the business of which is engaging in financial activities.” Id. §6809(3). The FTC’s regulations limit this definition to entities “significantly engaged” in financial activities. 16 C.F.R. §313.3(k)(1). Yet, the definition still includes a broad swath of different types of businesses, including businesses that engage in (1) lending, exchanging, transferring, investing for others, or safeguarding money or securities, (2) insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, (3) providing financial, investment, or economic advisory services, (4) underwriting, dealing in, or making a market in securities; and (5) activities closely related to banking. 15 U.S.C. §6809(3).

19 16 C.F.R. §313.3(k)(1)). Examples include the following: (1) information on an application to obtain a loan, credit card, or other financial product or service; (2) account balance information, payment history, overdraft history, and credit or debit card purchase information; (3) the fact that an individual or has or has been a customer or has obtained a financial product or service from the financial institution; and (4) information provided by a consumer in connection with collecting or servicing a credit account. Id. §313.3(c)(2).

20 15 U.S.C. §6808(b); 16 C.F.R. §313.3(e)(1).

21 16 C.F.R. §313.3(h) and (i)(1). Individuals include individuals who (1) have a credit or investment account, (2) receive a loan, (3) purchase insurance, (4) have an investment, (5) enter into an agreement for the financial institution to arrange or broker a home loan or credit to purchase a vehicle, (6) enter into a lease of personal property on a non-operating basis, (7) receive financial, investment, or economic advisory services for a fee; (8) receive tax preparation or credit counseling services, (9) receive career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company, (10) receive real estate settlement services, and (11) have a loan serviced by the financial institution. Id. §313.3(j)(2)(A-L).

22 Id. §313.4(a)(1) and §313.5(a)(1). The notice must include, inter alia, the following: (1) the types of nonpublic personal information that the financial institution collects about consumers and customers; (2) the types and examples of nonpublic personal information that the financial institution discloses to non-affiliated entities; (3) the affiliated and non-affiliated entities with whom the financial institution shares such information; (4) an explanation of the rights to opt out and the manner for doing so; and (5) the financial institution’s policies and practices concerning privacy and security of nonpublic personal information. Id. §313.6(a). See Facts for Business: How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act (July 2002), http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus67.shtm.

23 16 C.F.R. §313.6(d)(1). The short form notice must state that the financial institution’s privacy policy is available on request, and provide a reasonable means for the consumer to obtain it. 16 C.F.R. §313.6(d)(2).

24 15 U.S.C. §6801(b). This rule applies to all nonpublic personal information possessed by the financial institution regardless of whether the information relates to consumers or customers of that financial institution or another institution from which it received the information. Id. §314.1(b).

25 Id. §314.3(a).

26 Id. §314.4(a).

27 Id. §314.4(b).

28 The FTC has provided the following recommendations for the training and management of employees: (1) verify references and conduct background checks; (2) contractually require employees to comply; (3) limit access to nonpublic personal information to only those employees with a need to use it for their jobs; (4) require employees to use “strong” passwords; (5) use locking screen savers; (6) develop procedures governing the security of laptops and mobile devices; (7) train employees to recognize and report suspicious behavior; (8) adopt telecommuting policies; (9) impose discipline for violations of the program; and (10) disable access by terminated employees. See Facts for Business: Financial Institutions and Customer Information: Complying with the Safeguards Rule (April 2006) (Safeguards Guidelines), http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus54.shtm.

29 The FTC has provided the following recommendations for information security: (1) store records and data in locked, secure physical facilities; (2) maintain backup media securely; (3) adopt encryption technology and procedures; and (4) maintain an inventory of electronic equipment. See Safeguards Guidelines.

30 The FTC has provided the following recommendations for detecting and managing system failures: (1) monitor emerging threats and distribute information about them to employees; (2) update software routinely, and maintain appropriate anti-virus, anti-spyware, and firewall technology; (3) use computer logs, intrusion detection software, and dummy accounts to detect improper conduct; and (4) in the event of a breach, employ security professionals as needed to assess the breach, immediately secure compromised information, preserve information about how the breach may have occurred, comply with applicable breach notification laws, and notify law enforcement, consumer reporting agencies and other appropriate entities about the breach. See Safeguards Guidelines.

31 16 C.F.R. §314.6(c).

32 Id. §314.4(d).

33 Id. §314.4(e).

34 HIPAA and HITECH do not preempt state health privacy laws that provide greater protections than the federal statutes. 42 U.S.C. §1320d-5. A number of states have such laws. Businesses thus must assess whether they have operations or customers that may be subject to non-preempted state health privacy laws, and if so comply with both HIPAA and HITECH as well as the more restrictive provisions of the state laws.

35 In addition to HIPAA and HITECH, the Genetic Information Nondiscrimination Act of 2008 (GINA) affords certain protection for a specific type of PHI, “genetic information.” Genetic information is information about an individual’s genetic tests, genetic tests of family members of such individual, and the manifestation of a disease or disorder in family members of such individual. GINA §201. GINA prohibits health plans from adjusting premium or contribution amounts based on genetic information, requesting or requiring genetic testing, or collecting genetic information for underwriting before enrollment. Id. §101(a)(2). GINA also prohibits employers from (1) requiring, requesting or purchasing genetic information about employees, and (2) using genetic information to refuse to hire an employee, discharge or retaliate against an employee, discriminate against an employee with respect to compensation, terms or conditions of employment, or limit, segregate or classify an employee in a way that would deprive the employee of any opportunity or affect the
status of employment. Id. §202 and §207(l).

PHI means "individually identifiable health information," whether maintained or transmitted in "electronic form or in "any other form or medium," but does not include "employment records held by a covered entity in its role as employer." 45 C.F.R. §160.103. To fall within this definition, either the information must identify the individual, or there must be "a reasonable basis to believe the information can be used to identify the individual." Id.

42 U.S.C. §1320d-1(a)(1)-(3). The types of "transactions" that subject a business to regulation are submission of health claims, enrollment or disenrollment, eligibility determinations, payments for care, premium payments, referrals, and first reports of injury under workers' compensation laws. Id. §1320d-2(a)(2).

45 C.F.R. §164.502. HIPAA does permit limited use and disclosure of PHI without authorization, including (1) public health activities, (2) disclosure to a governmental authority where the covered entity believes the individual has been the victim of abuse, neglect or domestic violence, (3) in response to certain judicial, administrative or law enforcement requests, (4) for research purposes, and (5) for workers' compensation. Id. §164.512(b)(h).

Id. §164.508(a)(1)-(ii). "Health care operations" include (1) conducting quality assessment, (2) reviewing competence or qualifications of health care professionals, (3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of insurance or coverage, (4) conducting or arranging for medical reviews, legal services, and auditing functions, (5) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the covered entity, and (6) business management and general administrative activities of the covered entity. Id. §164.501.

Id. §164.508(a)(2) (limiting use of psychotherapy notes without authorization); 45 C.F.R. §164.508(a)(3) (prohibiting use for marketing without authorization, except "face-to-face communication made by a covered entity to an individual" and "a promotional gift of nominal value provided by the covered entity."). The authorization must at least (1) specifically describe the information to be used or disclosed, (2) identify the person(s) authorized to use or disclose it, (3) identify the person(s) to whom the covered entity may make the use or disclosure, (4) describe each purpose for the use or disclosure, (5) state the expiration date or expiration event for the use or disclosure, and (6) obtain the signature of the individual and date. Id. §164.508(c)(1).

Id. §164.502(b)(1).

HITECH §13405(b)(1); 45 C.F.R. §164.514(e)(2).

Id. §164.524(a).

Id. §164.526(b)(d).

HIPAA initially excluded from this accounting requirement disclosures made "to carry out treatment, payment, and health care operations." Id. §164.528(a)(i). However, HITECH eliminated that exclusion, and required accountings of disclosures made for this purpose within three years before the request. HITECH §13405(c).

45 C.F.R. §164.308-164.312. HIPAA's Security Rule contains a complex set of specific administrative, physical, and technical safeguards, some of which are required and some optional, although covered entities that do not adopt all optional measures must implement equivalent alternatives and document the reasons for deciding not to adopt the measures specified in favor of the alternatives. Id. §164.306(d)(3). Examples of administrative measures include designating one or more employees of the covered entity to be responsible for the information security plan, conducting risk assessments of potential vulnerabilities and adopting measures to address them, training employees about security, and creating policies and procedures limiting access to PHI. Id. §164.308. Physical safeguards include facility access controls, workstation and device controls, and secure backup and recovery techniques. Id. §164.310. Technical safeguards include unique and "strong" user names and passwords, audit controls, and transmission security (such as encryption). Id. §164.312.

HITECH §13402.

Id. §13400(1).

Id. §13403.

45 C.F.R. §164.402(i)(i). Similarly, no "breach" occurs where there is an "unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted." Id. §164.402(2)(ii).

Unsecured PHI includes only PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS. 45 C.F.R. §164.402. According to HHS, this standard is satisfied as long as the encryption technology meets the National Institute of Standards and Technology Special Publication 800-111 (for data at rest) or the Federal Information Processing Standard 140-2 (for data in transit). See Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of Breach Notification Requirements Under the HITECH Act, 74 Fed. Reg. 19,010-19,011 (April 27, 2009).
(An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).)
In fact, Justice Kennedy incorporated so many “helpful” comments in his opinion that he drew a rhetorical objection from Justice Scalia, who commented that, “In saying why it is not saying more, the Court says much more than it should.” Id. at 2635. Justice Scalia admonished that “lower courts will likely read the Court’s self-described ‘instructive’ explication[s] … as a heavy-handed hint about how they should proceed. Litigants will do likewise, … bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees’ use of electronic media.” Id. at 2630.

For example, as a “law enforcement officer, [Quon] should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used … [or] to assess the SWAT team’s performance in particular emergency situations.” Id. at 2631.

106 Nelson v. Nat’l Aeronautics and Space Admin., 530 F.3d 865, 879 (9th Cir. 2007).

107 Nelson, 131 S.Ct. at 756-57.

108 Id. at 757-58.

109 Id. at 759. In the Court’s view, the treatment and counseling question had to be “viewed in context.” Id. at 760. “The Government, recognizing that illegal-drug use is both a criminal and a medical issue, seeks to separate out those illegal-drug users who are taking steps to address and overcome their problems. The Government thus uses responses to the ‘treatment or counseling’ question as a mitigating factor in determining whether to grant contract employees long-term access to federal facilities.” Id. “The Court also reasoned that the open-ended questions to former employers, landlords and references were ‘reasonably aimed at identifying capable employees who will faithfully conduct the Government’s business. … The reasonableness of such open-ended questions is illustrated by their pervasiveness in the public and private sectors.’” Id. at 761.

110 Id. at 760.

111 Id. at 761.

112 Id., citing 5 U.S.C. §§ 552a(b) and §552a(i)(1).

113 Commercial Privacy Bill of Rights Act of 2011 (Privacy Bill of Rights); Consumer Privacy Protection Act of 2011 (Privacy Protection Act).

114 Personal Data Privacy and Security Act of 2011 (Data Security Act); Secure and Fortified Data Act (SAFE Data Act); Data Accountability and Trust Act (DATA Act); Data Accountability and Trust Act of 2011 (DATA Act of 2011); White House Legislative Language, Data Breach Notification (White House Proposal).

115 Data Security Act §302 and §311; SAFE Data Act §2 and §3; DATA Act §2 and §3; DATA Act of 2011 §2 and §3. But see White House Proposal §101 (only breach notification). See also Privacy Bill of Rights § 101 (authorizing FTC to promulgate data security regulations), Privacy Protection Act § 8 (containing rudimentary requirements for data security policy). The Data Security Act §304 and §319 would preempt all state and some other federal laws. The other proposals would preempt state but not federal laws. SAFE Data Act §6; DATA Act §6; DATA Act of 2011 §6; Privacy Bill of Rights § 601; White House Proposal, §109.

116 Privacy Bill of Rights § 102 (managerial accountability for adoption of privacy policy), §201 and §202 (notice of privacy policy and opportunity to limit or opt out of disclosures), §301 (requiring retention of minimum amounts of personal information), §302 (limiting permissible disclosure of personal information), and §303 (requiring procedures designed to ensure accuracy of personal information); Privacy Protection Act §5 (adoption of privacy policy), §4 (notice to individuals of privacy policy), and §6 (opportunity to limit or opt out of disclosures).