BNA

Daily Report for Executives

Privacy

Data security and consumer privacy issues are gaining traction in Washington and the interest may yield a new regulatory framework, write Francine Friedman, Jamie Tucker, Jo-Ellyn Sakowitz Klein, and Kris Ekdahl of Akin Gump Strauss Hauer & Feld LLP. More than a dozen bills have been introduced this year, and the Federal Trade Commission and Department of Commerce have published their own recommendations. Covered entities should establish privacy and security policies, assess risks and assign oversight, and prepare workforces for future changes.

High-Profile Breaches Spur Congressional Activity on Privacy, Data Security Policy

BY FRANCINE FRIEDMAN, JAMIE TUCKER, JO-ELLYN SAKOWITZ KLEIN, AND KRIS EKDAHL

With a Republican-controlled House opposite a Democratic-controlled Senate, and presidential and congressional elections looming in less than sixteen months, few proposals of significance are capable of advancing to become law. Data security and consumer privacy, however, are hot-button issues that are gaining traction and may yield consensus for a new regulatory framework. Bipartisan and bicameral support exists in Congress for updated data security and privacy laws, and the Obama administration is actively engaged. New regulations could directly impact any entity that collects, stores, or shares data on a large scale. Data brokers, online marketers, advertising agencies, ad networks, retailers, banks and other financial services companies, media and publishing companies, automobile manufacturers, mobile application developers, companies selling consumer packaged goods, law enforcement, web browsers, large employers, website operators, credit reporting agencies, and nonprofit organizations (including universities) need to be aware of these policy debates and prepare for the possibility of new regulation in the near future.

A string of high-profile incidents has accelerated the drumbeat in Washington for increased regulation. Major corporations and even government entities have fallen victim to large-scale data breaches, and many mobile devices have been discovered to allow tracking and recording of users' locations (97 DER A-28, 5/19/11). Names, birth dates, Social Security numbers, e-mail addresses, passwords, locations, and even credit or debit card numbers increasingly seem at risk, fueling the anger of privacy watchdogs and galvanizing policymakers (85 DER A-3, 5/3/11).

 ISSN 0148-8155

Congress, Administration Respond to Breaches

Congress and federal agencies have scrambled to respond to privacy advocates' outcry for increased regulation. More than a dozen bills have been introduced this year, and the Federal Trade Commission (FTC) and Department of Commerce have published their own recommendations.

The proposals pertain to three areas that often overlap: online and point-of-sale privacy, mobile device privacy, and data security and breach notification. The scope of the various proposals is sufficiently broad that if enacted in part or in full, entities across the spectrum would be impacted.

With so much at stake, this is a critical moment for covered entities to educate themselves and consider adding their voices to the policy debate in Washington, D.C. Moreover, now is an ideal time for these groups to assess their privacy and security procedures to ensure compliance with legal and industry best practices frameworks currently in place on both the national and state levels.

This article will help covered entities navigate the evolving consumer privacy debate. An analysis is set forth of key pending regulatory proposals in Congress and the federal agencies, the practical implications of proposed regulations, how these proposals might interact with existing law, and what companies and nonprofit organizations should do today to comply with the complicated patchwork of privacy regulations currently in place.

Bills on Consumer Privacy, Data Security

Recent proposals pertain to three general topics.

First, consumer privacy bills seek to help consumers control what personal information is collected, used, stored, or shared based on their online and point-of-sale behavior. Second, mobile privacy bills seek to help consumers take control of what information is collected, used, stored, or shared based on their mobile device usage and their geolocation footprint. Third, data security and breach notification bills seek to implement new protocols for protecting data and to create a national standard for notifying affected individuals and government agencies when a breach has occurred. Some of the proposals under discussion by policymakers span more than one of these categories.

Various Approaches to Privacy Issues

Six bills have been introduced this year that pertain primarily to online and point-of-sale privacy. By browsing the internet or making purchases at a store, consumers reveal valuable information that is used to build user profiles based on their location, their tastes and interests, their contact information, and perhaps even their debit or credit card numbers. This data can be very valuable for behavioral marketers, which is why the practice of collecting and selling consumer data has grown so rapidly.

Privacy bills seek to change how consumer information is collected, stored, used, and shared, and what consumers are told about these practices. Bills regarding data *collection* call for opt-out or opt-in mechanisms that require express consent from the consumer before any personal information can be collected. Bills addressing data *storage* place new limits on the scope and duration of data retention and also impose new security procedures to safeguard information. Bills regarding data *use* and data *sharing* impose limits on the purposes for which data may be used, restrict with whom a data collector (e.g., a retailer) can share information, and set new standards for whether consumer consent or notification is necessary before information can be used in certain ways or shared with a third party.

Each of the privacy-focused bills differs slightly, but the above themes generally characterize this group of proposals. Key privacy proposals include:

- Rep. Jackie Speier (D-Calif.): Do Not Track Me Online Act of 2011 (H.R. 654). This bill would require opt-out mechanisms for the collection or use of online and personal data (30 DER A-6, 2/14/11).
- Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.): Commercial Privacy Bill of Rights Act of 2011 (S. 799). This bill would require opt-out mechanisms for data use or sharing, as well as opt-in consent for the collection, storage, or sharing of sensitive personal information (126 DER A-15, 6/30/11).
- Rep. Bobby Rush (D-Ill.): BEST PRACTICES Act (H.R. 611). This bill is similar in structure to the Kerry-McCain proposal. It calls for opt-out mechanisms for data collection and storage, as well as opt-in consent for certain third-party information sharing.
- Rep. Cliff Stearns (R-Fla.): Consumer Privacy Protection Act of 2011 (H.R. 1528). This bill would allow consumers to opt out of having their personally identifiable information shared with third parties (94 DER A-2, 5/16/11).
- Sen. John D. Rockefeller IV (D-W.Va.): Do-Not-Track Online Act of 2011 (S. 913). As Chairman of the Senate Commerce Committee, Senator Rockefeller will play a central role in shaping Senate proposals on privacy and data security (90 DER A-15, 5/10/11). His bill would give consumers the ability to opt out of having their online data tracked and stored. Rockefeller's proposal would go one step further than the aforementioned privacy bills by also imposing limits on data collection from mobile devices.
- Reps. Ed Markey (D-Mass.) and Joe Barton (R-Texas): Do-Not-Track-Kids Act (H.R. 1895). Markey and Barton are co-chairmen of the Bipartisan Congressional Privacy Caucus. Their proposal would forbid online companies from using personal information for targeted marketing to children, would empower parents to delete their children's digital footprint, and would require parental consent for any data tracking online or on mobile devices (94 DER A-12, 5/16/11).

Mobile Device Privacy Getting Attention

While the Rockefeller and Barton-Markey proposals touch on many aspects of consumer privacy, including mobile privacy, a separate group of bills focuses solely on mobile devices. When users access GPS-enabled applications on their cell phones, smartphones, and tablet devices, they leave a valuable virtual trail of bread crumbs that can be used to reveal their present or past locations.

  DER ISSN 0148-8155

Proposals in this area seek to restrict the collection and sharing of geolocation data. The key proposals include:

- Sen. Ron Wyden (D-Ore.) and Rep. Jason Chaffetz (R-Utah): Geolocation and Privacy Surveillance (GPS) Act (S. 1212, H.R. 2168). Released as companion bills in the Senate and House, these bills would prohibit companies from collecting or sharing geolocation information without the user's express consent (116 DER A-26, 6/16/11).
- Sens. Al Franken (D-Minn.) and Richard Blumenthal (D-Conn.): Location Privacy Protection Act of 2011 (S. 1223). This bill would require any covered entity to offer upfront notice and receive informed consent from users to track their geolocation information (116 DER A-16, 6/16/11).
- Sen. Patrick Leahy (D-Vt.): Electronic Communications Privacy Act (ECPA) Amendments Act of 2011 (S. 1011). Senator Leahy is the Chairman of the Judiciary Committee and has been active in many aspects of the privacy debate. Enacted in 1986, the ECPA restricts third-party access to private electronic communications, such as online activity and e-mails. Because the ECPA does not cover GPS-based information, Leahy proposed this update to add geolocation information as a new class of private communications subject to the protections of the ECPA (96 DER A-22, 5/18/11).

Data Security, Breach Notification

Five proposals that primarily focus on data security and breach notification have been introduced in the 112th Congress. The aim of these bills is to require entities that collect or store data to take steps to prevent nefarious actors from accessing personal information and to create a standard for notifying government agencies and consumers if an organization's data is breached. Like some of the privacy bills discussed earlier, these proposals usually incorporate limits on the scope and duration of data storage, under the theory that if less data is stored, less data is at risk. However, security and notification bills impose additional regulations. First, they mandate security policies to prevent unauthorized third-party access to data. Second, they lay out procedures and time frames to alert affected individuals and government agencies when a data breach has occurred. Third, many of these bills require third-party data brokers to allow consumers to view their information and correct any errors.

The key bills in this area include:

- Sens. Rockefeller and Mark Pryor (D-Ark.): Data Security and Breach Notification Act of 2011 (S. 1207). This bill requires businesses and nonprofit organizations that store personal information to implement reasonable security measures and alert consumers when their data has been compromised; in the event of a breach, affected individuals would be entitled to free credit monitoring services for two years (116 DER A-23, 6/16/11).
- Leahy: Personal Data Privacy and Security Act (S. 1151). This bill is similar to bills Leahy has introduced in previous Congresses. His proposal calls for businesses to enact security procedures to protect sensitive data, and it would create a federal standard for notifying appropriate parties of a breach (111 DER A-7, 6/9/11).
- Bono Mack (R-Calif.): SAFE Data Act draft proposal. As chair of the Commerce, Manufacturing, and Trade Subcommittee, Bono Mack is one of the key leaders in the House. Her proposal requires businesses to notify consumers and the FTC within 48 hours of containing and assessing a breach. It also calls for data minimization, stronger security, and, like the Rockefeller-Pryor proposal, would entitle affected individuals to free credit monitoring services for two years (114 DER A-15, 6/14/11).
- Rush: Data Accountability and Trust Act (H.R. 1707). This bill mandates stricter data security policies and creates a national standard for breach notification (89 DER A-2, 5/9/11).
- Stearns: DATA Act of 2011 (H.R. 1841). Stearns' data security and breach bill is similar to Rep. Rush's in its call for tighter protections of data storage systems, in addition to setting a standard for notifying affected individuals and government authorities in the event of a breach (94 DER A-2, 5/16/11).

Administration May Push Forward

Given the plethora of bills and hearings on the topics of privacy and data security, Congress has clearly indicated its interest in passing new legislation this year. The sheer number of competing proposals and the potential for jurisdictional battles in Congress, however, complicates the path to overhauling privacy and data security laws. The legislative process is unpredictable and can be significantly influenced by external events, including data breaches and coverage of new and expanded uses of data. It is more likely that privacy advocates and industry can coalesce around a data breach notification proposal than agree on how to regulate the collection, use, and sharing of consumer information. It is noteworthy that business leaders recently testified before Bono Mack's subcommittee that they would support reasonable federal breach notification regulations.

The Obama administration is preparing its own blueprint for consumer privacy and data security in the event that Congress is unable to pass a meaningful bill. A White House cybersecurity proposal has been the subject of several hearings on Capitol Hill. While the administration's cybersecurity proposal primarily pertains to securing critical infrastructure against cyber attacks, it also calls for a national standard for breach notification.

Additionally, the FTC and the Department of Commerce have issued their own recommendations addressing online and point-of-sale privacy, mobile device privacy, data security, and breach notification. Core goals of the comprehensive FTC and Commerce plans include limits on what information can be collected and how long it can be stored, privacy policies that are shorter and simpler, persistent do-not-track preferences that follow a user from website to website, more transparency on the part of data collectors, and requiring companies to build security and privacy measures into products rather than layering on features as an afterthought. In the absence of meaningful congressional action on these points, it is possible that one or both agencies may utilize regulatory tools under their exist-

ing authority, such as rulemaking, enforcement actions, and issuing guidance. Action along these lines could be undertaken without an act of Congress.

Possible Impact of Increased Regulation

Congress and the administration are debating wide-ranging changes, and consequently the effects could touch nearly every consumer, business, and nonprofit organization in the country, either directly or indirectly. For instance, data privacy regulations, as currently envisioned in ''do not track'' and geolocation proposals, would significantly change operations for entities that purchase consumer information for behavioral marketing purposes. Third-party purchasers would be affected by stricter privacy regulations because they rely on the personal data that point-of-contact entities collect. New standards could change the advertising landscape online, on mobile phones, and on the ground because data privacy and geolocation bills could curtail data-driven, targeted marketing. Under many of the proposals, retailers, strategic advertising companies, and websites that host personalized ads would likely have a diminished ability to tailor and target their outreach to potential customers.

Practical Implications Could Be Far-Reaching

The true breadth of the new proposals is revealed by looking at the wide range of covered entities that could be affected.

The list includes browsers, ad networks, retailers, content websites, consumer research groups and data brokers, mobile network providers, mobile application developers, financial institutions, universities, nonprofit organizations, employers, and any other entity that collects and stores large amounts of personal information. If proposed online or point-of-sale privacy and geolocation regulations are adopted, this diverse group of covered entities would be limited in its ability to collect, store, use, or share consumer information. If data security and breach notification proposals are adopted, covered entities would be compelled to adhere to specific methods for storing consumer information and responding to breaches.

Practically speaking, new privacy regulations would create significant hurdles to sharing information, which would cause a substantial reduction in the information trade. With stricter privacy or geolocation restrictions, data collectors (e.g., a newspaper website or a mobile ''app'' provider):

- would collect less useful information about consumer preferences and interests;
- would be permitted to retain that information for a shorter duration than ever before; and
- may no longer be able to share the more relevant information with outside entities.

As a result, third parties will be less inclined to pay such a high premium for less robust consumer data files.

For example, advertisers strive to place their promotions in front of only those people who fit their profile of a likely customer. It can be more profitable to target 10 likely buyers than to broadcast to a random cross-section of 1,000 people. The information profiles that data collectors build and sell are what enable such targeted, high-yield, efficient marketing. If consumer profiles are no longer robust and insightful, they are no longer valuable.

The end result may lead to less data collector revenue from data sales, an impersonal user experience for consumers, lower yields on each advertising dollar spent, and ultimately a shift in the behavioral advertising business model. Web services that were sustained by advertising revenue may either go out of business or begin charging users for previously-gratis services. Free mobile ''apps'' that collected valuable GPS information may no longer be available. And Internet users will still see the same quantity of advertisements (if not more), but those ads will be less relevant to users' interests or needs.

Moreover, new breach notification regulations could have implications for consumer confidence, the reputations of breached entities, and internal investigations. If new rules lower the threshold at which a breach must be reported (in terms of the size or sensitivity of the data compromised), more breaches should be disclosed. Consumers who receive too many breach notifications that do not affect them may be lulled into complacency and not take proper action when a true risk is identified.

Possible Impact on Industry, Consumers

An increase in breach reporting can also undermine consumer confidence in institutions that store sensitive information, as a group. Whether or not a particular organization suffered a breach, the mere fact that a similar organization suffered one breach can have a corrosive effect on the universe as a whole. And for the entities that actually fall victim to a breach, the impact of negative publicity can be devastating. In either scenario, it is plausible that growing numbers of people would avoid sharing personal information with any outside entity. In the case of nonprofit organizations, that would mean fewer people contributing. In the case of businesses, that would mean fewer customers.

Regarding internal investigations after a breach, a quick notification deadline would give the breached entity very little time to conduct an internal review before the firestorm of journalists, government investigators, and angry customers make such a review infinitely more complicated. As a result, the organization may not be able to spot its vulnerabilities as quickly, leaving it susceptible to repeated attacks.

If implemented, these proposals would also translate into increased compliance costs and technical hurdles for both businesses and nonprofit organizations. Implementing new security features can be expensive and may necessitate an overhaul of computer systems, including migrating massive amounts of data from one platform to another. Not only that, but detailed security requirements may perversely increase the threat of breaches by providing would-be hackers with a road map of network security features. Potential complications arise with the privacy and geolocation proposals, as well. Deleting consumer data logs poses technical challenges if that data is stored on a ''cloud'' or on multiple networks. Adding opt-out or opt-in consents into every application would be cumbersome for data collectors, and such requirements would certainly reduce the number of consumers sharing their information.

  DER ISSN 0148-8155

Reasonable Uniform Breach Notification

For all of the implications that may be received negatively by data collectors and third party purchasers, one aspect of data security reform might be embraced by covered entities. Assuming strong state law preemption, a new federal standard would replace a disparate patchwork of state laws governing data security and breach notification. Generally speaking, reasonable uniform compliance requirements would be a welcome development for many organizations operating across state borders. In the realm of data security, a uniform federal standard may be palatable because complying with multiple state laws is untenable. Moreover, many organizations already have a strong self-interest in bolstering their internal security measures; therefore, a single federal security guideline could be welcomed by industry.

Considering Interplay With Existing Laws

One final item that covered entities need to monitor in the ongoing privacy debate is how new regulations might interplay with existing data security and privacy laws. The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA) are some of the key federal privacy laws currently under enforcement.

Not all of the recent proposals mention existing federal statutes, but those that do (e.g., Leahy's data breach bill, Bono Mack's breach draft, and Stearns' privacy bill) indicate that existing statutes will trump the new proposals wherever overlap occurs. That may indicate Congress is likely to leave existing federal regimes like HIPAA and GLBA in place even if broader privacy and security regulations are adopted this year. Even so, entities that are currently covered by industry-specific regulations might still feel an additional regulatory burden if they collect, store, use, or share data for any purposes outside the purview of existing laws.

State privacy laws of similar scope would be preempted by most of the congressional proposals. Forty-seven states have their own breach notification laws, and every state has privacy or data security laws of some sort, which often differ from one state to the next. That patchwork of local laws places a high compliance burden on entities operating across state lines, so federal preemption may be a welcome change for some covered entities.

Speier's privacy bill is an exception, as it would *not* preempt state law if state law offers greater privacy protection than the federal law. The vast majority of congressional proposals, however, would supersede state laws wherever overlap occurs. If Congress passes a comprehensive privacy and data security bill this year, it is likely to reflect that consensus.

In the Meantime, Companies Should Act

In spite of all that is at stake in the ongoing policy debate regarding privacy and data security, the immediate priority for any covered entity should be to evaluate their policies vis-à-vis existing law and industry best practices. If an organization does not meet the standards already in place, adjusting to meet new regulations will be that much more difficult.

Unfortunately, evaluating a company's current position is made more complicated by the fact that no comprehensive federal privacy law governs the collection, use, storage, and sharing of consumer information. Rather, an ever-changing patchwork of sector-specific and data-specific state and federal privacy laws makes such compliance assessments difficult.

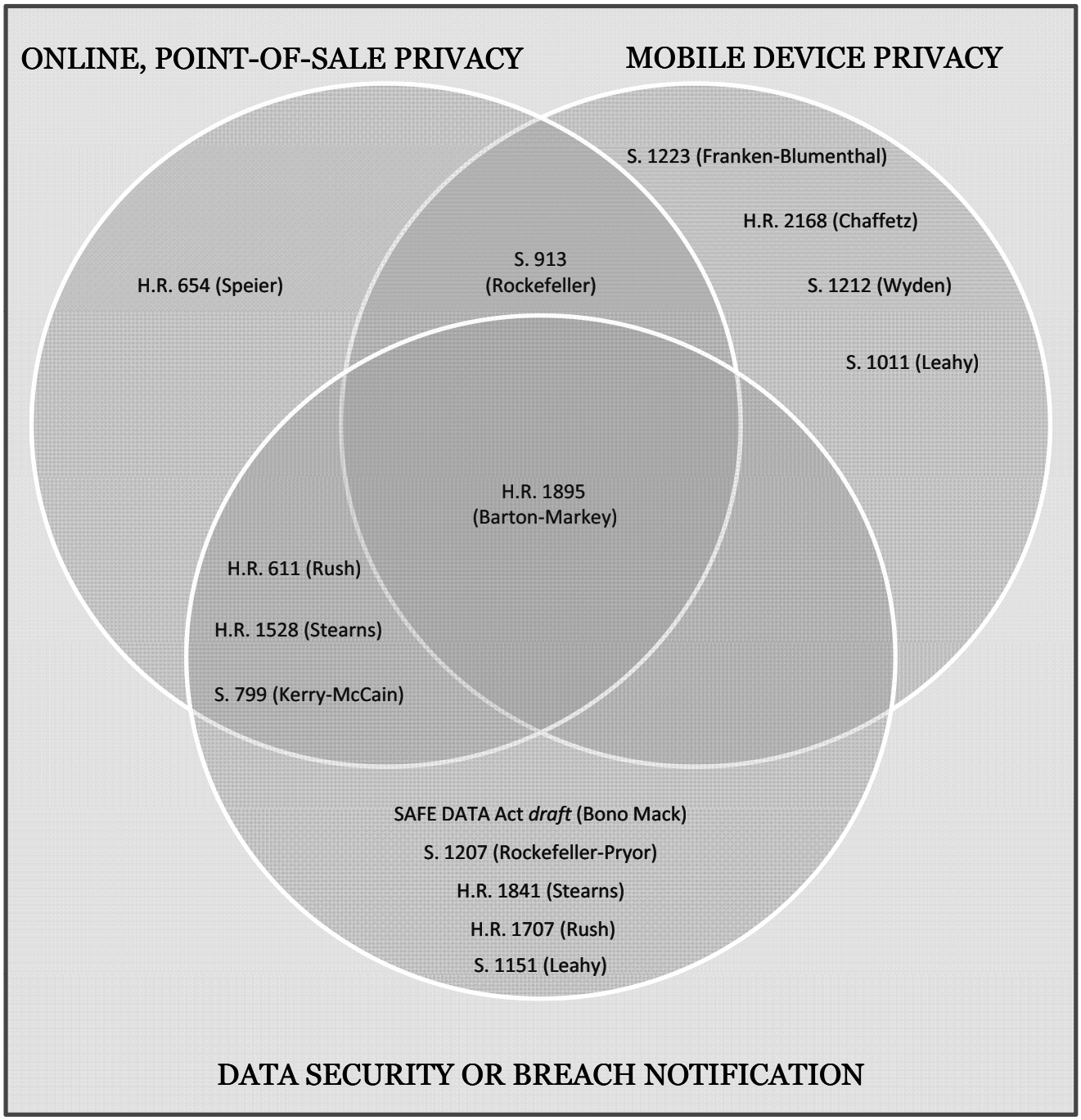
In light of these realities, some organizations may find it helpful to approach the issue from the perspective of attempting to identify steps that can be taken to minimize data privacy and security risks, rather than trying to develop a comprehensive checklist of all possible laws that may apply. While due attention must be paid to specific compliance mandates, privacy issues tend to be less linear, generally warranting a more dynamic approach.

Taking Steps to Minimize Exposure

Covered entities can take several steps to minimize exposure:

- First, companies should not underestimate the value of having reasonable written privacy and security policies. Policies and procedures should be reevaluated at regular intervals, as well as when incidents occur.
- Second, entities should conduct assessments to identify risks specific to their organizations and should be sure to incorporate low-tech and high-tech solutions.
- Third, entities should consider assigning one person responsibility over privacy and security concerns. The position of Chief Privacy Officer is becoming more common in the senior ranks of organizations.
- Finally, companies should train their workforces on privacy matters and ensure that all employees understand the importance of data security and privacy. Many breaches are the result of employee error, rather than external cyber attack.

The prospect for new federal data security and privacy regulations remains in flux. Given the attention that Congress and the administration have already dedicated to these issues, paired with the seeming inevitability of continued high-profile data breaches, it is plausible that a revamped national privacy framework could be agreed upon in the relatively near future. Yet with more than a dozen proposals already released from competing congressional committees, it remains difficult to predict what the final regulations might look like. Looking ahead, it is also important for companies to monitor or become engaged in the policy debate in Washington, D.C., and to better understand how proposals can impact their business. The realm of consumer privacy and data security in the digital era is fast-evolving, and as federal policymakers try to keep pace, much is at stake for all entities—and individuals—involved.



DER ISSN 0148-8155