



Articles

What's Ahead for Privacy and Security in 2009?

By [Kirk J. Nahra](#)

January 2009 | *Privacy In Focus*

With a new Administration, a significantly different Congress and a wide range of new rules and upcoming legislation, privacy and security professionals will continue to have their hands full in 2009 with new developments. Here are a few of the main items we'll be watching in 2009.

Increasing Government Enforcement

Despite the substantial array of privacy and security laws and regulations, at all levels of government, enforcement of privacy and security laws has remained nominal. Some agencies, notably the Federal Trade Commission (FTC), have brought a modest number of high-profile enforcement actions. Other agencies, like the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (for the HIPAA Privacy Rule) and the various federal agencies responsible for Gramm-Leach-Bliley Act enforcement, have done virtually nothing on enforcement.

There are significant reasons to anticipate new enforcement policies in the year ahead. First, even in 2008, some movement towards additional enforcement was apparent. In the health care industry, for example, we saw the first HIPAA penalty, brought against Providence Health Systems. See "The HIPAA Enforcement Era Begins," *Privacy In Focus* (August 2008), Click [here](#) to view this article. Calls for additional enforcement from Congress and a wide range of privacy advocates continue.

In the Obama Administration, enforcement of privacy laws is likely to be a significant priority. Additional enforcement resources for the FTC were a component of the Obama campaign platform. There is a virtual guarantee that the new Administration will take a more aggressive approach on enforcement of the HIPAA rules. Accordingly, we can expect a general increase in enforcement activity in 2009, although this is likely to be a stream rather than a flood.

Key Action Item. Because of the new likelihood of enforcement action, companies should pay particularly close attention to complaints about privacy and security, and should act aggressively to mitigate any security breaches or other potential harms from privacy and security failures. Also, pay close attention to marketing issues—this is a key area of ongoing controversy, and one where privacy advocates are particularly aggressive in pushing for more enforcement.

The FTC's Challenging "Red Flags" Rule

In terms of new regulatory obligations, the FTC's "red flags" rule is far and away the most broadly applicable and challenging additional regulation on the horizon. The red flags rule, one of the last FTC rules to be promulgated under the Fair and Accurate Credit Transactions Act (FACTA), imposes obligations on "financial institutions and creditors" to develop an "identity theft red flags program." While the "financial institution" definition is somewhat technical and therefore very limiting, the concept of "creditors" has potentially broad application; moreover, the FTC has taken a surprisingly broad view of its own rule, such that virtually any company—in any industry—that provides services in advance of payment may face obligations under this rule.

The FTC, despite its scary pronouncements on the scope of the rule, also has acknowledged that its interpretation will impact numerous companies not accustomed to such regulation. Accordingly, the FTC has

moved a November 1, 2008, effective date back to May 1, 2009, to give companies an additional opportunity to meet their compliance obligations on the "identity theft program" aspects of this rule (other components still had a November 1, 2008, compliance date). While the extension is appreciated, many companies will face challenges in meeting this deadline.

Key Action Item. Companies in virtually all industries face the possibility of being identified as creditors subject to the red flags rule. The first step for any company—which needs to be taken immediately—is to determine the situations in which the company issues any kind of credit, interpreted as broadly as providing services in advance of payment. In the FTC's view, these companies are "potentially" covered by the rules. The second step in the analysis is the hard one—does a company have "covered accounts," meaning specific kinds of transaction accounts, or other accounts where there is a credible threat of identity theft? The main task for most companies will be to conduct a risk assessment of their accounts, to determine whether there are credit arrangements that require companies to adopt a full-scale red flags program.

Identity Theft as an Enforcement Priority

The broad scope of the red flags rule reflects an ongoing and growing concern about the problem of identity theft. The enforcement effort directed at fighting identity theft continues to expand. For example, the Department of Justice (DOJ) and the FTC recently released an updated status report on overall efforts directed against identify theft. See "Combating Identity Theft: A Strategic Plan," available by clicking [here](#). In the press release accompanying the status report, the FTC and the DOJ made clear that "Government and the private sector, working together with consumers, must remain vigilant and adaptable as new generations of identity thieves and techniques develop over the coming years."

In addition, we also are seeing an increased focus on a newer form of identity theft—medical identity theft. The HHS Office of the National Coordinator for Health Information Technology and the FTC recently held a "Town Hall" meeting on medical identity theft. The general conclusion of the meeting is that there is ongoing confusion about medical identity theft, and few effective means of fighting identity theft. (A "report and roadmap" from this Town Hall meeting is expected to be published this winter). In addition, the movement towards electronic medical records creates the possibility that problems with medical identity theft will get worse (although there clearly are some who think that electronic medical records can help solve this problem in the health care industry). As a general matter, industry concerns with identity theft, whether medical or otherwise, must remain high, as identity theft is the main potential and concrete "harm" that can be suffered as a result of information security breaches.

Companies need to continue an aggressive fight against identity theft and should broaden their scope of review to include not only credit-related risks but other forms of identity theft as well.

Key Action Item. One of the primary conclusions from recent identity theft cases is that many identity theft schemes result from improper activity by insiders. Accordingly, companies need to focus extra attention on how data access is controlled within companies. Identity theft concerns also reflect a broader set of privacy related problems caused by corporate insiders, such as the well-publicized events affecting the UCLA Medical Center, where dozens of employees reviewed celebrity medical records for improper or inappropriate purposes. So, companies need to focus on reviewing employee access controls on the front end, increasing sanctions and training related to improper actions, and, most importantly, reviewing how best to conduct ongoing auditing and monitoring of employee access, particularly in industries where customer service representatives and others have access to large amounts of customer or employee data.

Litigation Developments Expected

We also can expect continued efforts by plaintiffs' attorneys to poke holes in the existing cases that preclude liability absent a showing of actual harm. In a wide range of cases across the country, the threat of potential loss has not been found sufficient to permit a case to go forward. A lack of actual damages—even in the face of clear security breaches—is now the primary hurdle in most privacy and security cases.

Despite this strong line of precedent, the continuing spread of security breaches, particularly on a large scale, is making multiple class action filings almost commonplace when breaches are publicly disclosed. Moreover, many of the new laws (including some pending proposals) incorporate a private cause of action and/or statutory damages as means of increasing the use of these private enforcement tools.

What can we expect on the litigation front? First, we likely will see an increased use of "negligence" theories to bring cases, relying on existing regulatory or industry standards. We have seen a series of cases in recent years where a common law negligence approach has been used to start a case—by developing the framework for a cause of action.

Beyond the negligence theory, the key issue is still damages. While the negligence theory allows a complaint to be brought, there hasn't been any clear evidence (yet) that this theory is enough to overcome the damages hurdle. Moreover, the few published cases to date typically have involved "single injury" situations, where one individual (or a small number of individuals) has been the potential victim of a privacy or security breach.

Accordingly, many uphill challenges remain to bringing successful privacy/security suits (or, conversely, lots of defenses still exist, even when companies have not behaved well). But, as the number of breach cases continues to grow, plaintiffs are continuing to push the envelope on creative theories concerning how these compliance failures translate to consumer injuries.

Key Action Item. Watch for the breakout case, which could open the litigation floodgates. The critical cases to watch will be those that combine a negligence approach with a credible damages argument, on a class-wide scale. And pay special attention to any laws that include statutory damages—eliminating the need to prove actual damages. While Congress "fixed" the problem with statutory damages in the FACTA credit card "expiration date" disclosure suits, we can't expect this kind of action in the future. The increasing likelihood of privacy and security claims that can survive initial motions in court also means that it is critically important for companies to document their ongoing compliance efforts, so that they can demonstrate their actions to meet the variety of relevant requirements.

Expanding Data Security Obligations

The last critical issue for 2009 will involve ongoing developments related to the protection of customer and employee information—the "security" side of the privacy and security field. Clearly, there is a substantial crossover between privacy and security. Some areas—like the various marketing rules—fall obviously onto the privacy side. Other issues—mainly related to breaches—could be considered either privacy or security issues. But, it is clear that the regulatory obligations related to security are growing and that, for many companies, these security obligations will be both more burdensome and more broadly applicable. Accordingly, analyzing and updating information security programs needs to be key considerations for any company.

For many years, a reasonable and appropriate information security program has been a requirement for any company that maintains personal information -- essentially, every company. See "Effective Security Practices Now a National Requirement," *Privacy In Focus* (June 2005), Click [here](#) to view this article.

Beyond this "general" obligation, we have seen the implementation of specific security requirements on an industry-specific basis (such as the HIPAA Security Rule and the Gramm-Leach-Bliley safeguards rule). Next, we saw the development of a nationwide matrix of "security breach notification laws"—requiring consumer notification in the event of certain security breaches. While these laws did not, by themselves, impose specific security mandates, they did create obligations—for all businesses—in the event of a security failure. Now, two key developments are imposing specific security details on most companies. First, the "Payment Card Industry" (PCI) security standards apply broadly to any company that takes credit cards as a means of payment. The PCI security principles are not new, but are becoming increasingly detailed and are being followed and monitored on an increasingly aggressive basis. Click [here](#) to view a wide variety of materials about the PCI standards (including the recently released October 1, 2008, guidelines).

Most recently, we have seen various new state laws that impose specific and detailed security obligations. For example, a new Nevada obligation, effective October 1, 2008, requires that "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." This law could require many companies to alter their behavior, particularly in connection with email transmissions.

A new Massachusetts law imposes even broader obligations. In fact, Massachusetts has now introduced the most substantial set of security practice obligations applicable to businesses in all sectors. This law was scheduled to take effect on January 1, 2009, but this deadline recently was extended until May 1, 2009. Because the Massachusetts law has broad applicability, virtually any company that does business with a Massachusetts resident needs to be concerned about these requirements. While some of the requirements are straightforward (and consistent with the FTC's earlier views on a reasonable and appropriate program), other requirements (such as specific encryption obligations and physical access restrictions) likely will require many companies to develop new security solutions.

Key Action Item. These new obligations require an overall review of a company's information security practices. At a minimum, if you haven't re-assessed your security program in the last two years, you need to do so now. Also, unless your business is restricted to a single state or a small region, make sure you understand the full set of obligations that you face under these laws. Then, focus attention on the primary areas of risk—make sure your employees are trained well, and that your information is protected as best as one reasonably can. Remember, the biggest risk is not violating these rules in the abstract, it's the additional risk in the event of a breach if you haven't met a required standard.

For more information, please contact [Kirk J. Nahra](mailto:Kirk.J.Nahra) at 202.719.7335 or knahra@wileyrein.com.