wiley

NEWSLETTER

What to Expect in Privacy from a Second Obama Administration

December 2012

With the 2012 elections now history, it is time to look forward to what may happen in privacy law during the early part of the second Obama Administration and the new Congress.

Consumer Privacy

Consumer privacy received substantial attention during the first Obama Administration and in the years before. Most recently, the Obama Administration presented its view on consumer privacy issues last February with the issuance of its "Blueprint for Consumer Privacy," in which it, among other things, advocated a Consumer Privacy Bill of Rights, recommended that Congress enact baseline consumer privacy legislation and urged industry and consumer groups to cooperate in devising binding self-regulatory privacy codes of conduct tailored for different types of technologies. See "White House Announces Consumber Bill of Rights While Internet Companies Agree to 'Do-Not-Track,'" March 2012, *Privacy In Focus*.

With the Administration having so recently pronounced its position on privacy law, the next four years will likely focus on implementation rather than policy development. In an initial effort to implement the Blueprint, the National Telecommunications and Information Administration (NTIA) in July launched a series of "multistakeholder meetings" focusing on transparency in privacy of mobile applications. NTIA hopes that this process will culminate in a privacy self-regulatory code of conduct acceptable to a wide range of stakeholders. Watch to see what results come from the current NTIA multistakeholder process. If a consensus emerges that is acceptable to the wide range of participating stakeholders, then this process may serve as a model for similar initiatives in the future.

Congress has discussed consumer privacy for more than a decade, but no bill has ever made its way through both chambers. That is not likely to change in the upcoming Congress, which returns with the same parties in control of the respective chambers, although with a few new faces, mostly on the Republican side, in both the House and the Senate.

Even with new legislators, however, legislation would seem to face significant obstacles. Congress has for more than a decade struggled with consumer privacy and data protection issues, but seldom has a bill passed either House, much less both. Instead, expect a series of hearings and the introduction of various bills.

Even if a bill were to pass in one chamber, navigating its way through the other would likely prove difficult.

The principal obstacles facing legislation are fundamental disagreements over what approach to take. For years, the Senate has remained unable to resolve whether consumer privacy law should be addressed as a regulatory matter or as a law enforcement matter. And in the House, the leading Republicans on the committee have not seen any need for general consumer privacy legislation at all.

At the same time, however, House Republicans have shown an interest in establishing a national standard that would govern a business's obligations to disclose breaches of data security, in lieu of the more than 45 state laws that currently regulate disclosing such incidents. To date, however, House Democrats have shown little interest in moving a data security bill that does not also address consumer privacy issues, and the Senate would likely also want to address general privacy issues in any data breach legislation.

Given the likely slow movement in Congress, the most likely forum for activity beyond the NTIA's multistakeholder process is the Federal Trade Commission (FTC), which has asserted itself as the leading privacy regulator in the U.S. Expect the FTC, which is generally expected to have a new chairman soon, to continue to bring enforcement actions relating to consumer privacy and data protection. One major FTC responsibility is oversight of its consent decrees with firms such as Google and Facebook. A federal district court in California just approved a consent decree settling charges that Google violated the earlier Google Buzz consent decree by setting cookies on the Safari web browser. In that case, earlier, Google agreed to pay a record $22.5 million civil penalty, the largest fine ever imposed for violating an FTC order.

In addition, the FTC has recently begun to make more use of its jurisdiction over "unfair" trade practices, although its power to do so in the realm of consumer privacy is currently being litigated, and a defeat would constitute a significant setback.

Mobile Devices/Mobile Applications

Privacy in mobile devices and, in particular, in mobile applications, has received significantly increased attention in recent years, spurred by the explosion in the number of GPS-enabled devices and feature-rich smartphones. Unsurprisingly, regulatory interest has followed.

As mentioned above, the NTIA is currently hosting a multistakeholder process that hopes to devise a code of conduct for transparency in mobile app privacy practices. NTIA envisions that businesses would pledge to abide by such a code of conduct, and that this pledge would be enforceable by the FTC under its authority over deceptive trade practices.

Even without such a code of conduct, however, the FTC has staked out a clear role in mobile privacy. It has already exercised its enforcement powers against mobile applications, and will continue to monitor mobile app privacy practices and look for favorable cases that will tend to move industry practices towards more privacy-protective standards.

In addition, a third agency—the Federal Communications Commission (FCC)—in 2012 also began to claim a role in mobile privacy. In May, the agency issued a report on location-based services and mobile network data privacy. It solicited comments on the privacy and data security practices of mobile services providers and the implications of the FCC's regulations regarding customer proprietary network information. While the outcome of this process is uncertain, the agency is likely to remain interested in mobile privacy and data security issues.

International Data Transfers

As for international privacy issues, the Administration likely will continue to work to maintain and promote international data transfers. The U.S. will work to maintain the existing "safe harbor" arrangement with the European Union (EU), and work in cooperation with American business interests to mitigate the worst effects of the proposed new EU privacy regulation. See "Proposed New European Union Data Regulations Raises Significant Issues for U.S. Businesses," February 2012, *Privacy In Focus*. Administration policy prefers less restrictive approaches, such as the arrangement being fashioned through the Asia-Pacific Economic Cooperation process. In late November, the FTC conducted a forum on cross-border codes of conduct to explore recent uses of code-based systems and the role and utility of third-party oversight.

Cybersecurity

Turning to cybersecurity, the Senate's inability to end a filibuster of cybersecurity legislation in November means that any further legislative initiatives will wait until next year. And it is not clear that Congress has come to a sufficient consensus to enable legislation to pass anytime soon.

Congress's inability to act leaves the door open for the President to issue an executive order setting cybersecurity standards for the government. These standards would likely apply to at least some private companies that serve as government contractors, and thus indirectly would begin to reach into the private sector. If the President does, such standards would probably become the minimum for any subsequent legislation.

Email Privacy/ECPA Reform

The scandal involving former CIA Director David Petraeus's relationship with his biographer has brought increased public attention to government surveillance powers in general, and to the ease with which police investigators can access email and other electronic communications without a search warrant. Courts are confused as well, as shown by a divergence of decisions across the nation regarding the appropriate level of protection to be given email.

In general, the Obama Administration has, consistent with its predecessor, supported current law or sought to remove legal obstacles to government investigations, especially in cases where national security or anti-terrorism interests are involved. This has put the Administration at odds with privacy advocates.

On November 29, the Senate Judiciary Committee had approved legislation that would establish a search warrant requirement for most electronic communications. If no bill is enacted by the lame-duck Congress, expect this issue to return next year. Although the Administration has yet to take a formal position on this legislation, it has in the past been deferential to the concerns of law enforcement, which tends to oppose the establishment of search warrant requirements.

Cell Phone Privacy

A cousin of the privacy of electronic communications is location privacy, and, in particular, access to location through GPS-equipped cell phones and other location-aware devices. The Supreme Court this year, in *United States v. Jones*, held that attaching a GPS device to a suspect's automobile constituted a "search" under the Fourth Amendment, but did not address whether location information in the possession of carriers or other mobile services providers is similarly protected. See "Supreme Court Limits GPS Surveillance," February 2012, *Privacy In Focus*.

A number of cases in lower courts have struggled to address the legal standard that law enforcement must meet in order to obtain "live" and "historical" location information from wireless providers. Look for Congress to take an interest in this issue as well, as the question of when law enforcement must have a search warrant in order to obtain location data, whether a record of past locations or in real time, is a question of policy likely to interest legislators.

"Big Data"

The comprehensive collection, retention and analysis of consumer activity, and especially activity online—is now attracting the interest of the FTC as well as Congress. Such "big data" offers both obvious business utility and a clear potential for intrusiveness.

The FTC expressed some concerns about data brokers in its March 2012 report *Protecting Consumer Privacy in an Era of Rapid Change*. *See* "FTC Issues Much-Awaited Consumer Privacy Report," April 2012, *Privacy In Focus*. The FTC held a workshop on December 6, at which it heard from advocates, technologists and business representatives on online consumer data collection, as to what standards should apply and whether the market will provide alternatives. Look for an FTC report on the issue sometime in the second half of 2013, and keep an eye on this potential area of new enforcement activity.

Interest has spread to Capitol Hill, as well. This summer, Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX) sent letters to a number of leading data compilers. More recently, Sen. Jay Rockefeller (D-WV), chairman of the Senate Judiciary Committee, sent letters to nine leading data brokerage firms asking for information about the types of personal data that those firms collect and related business practices. Look for congressional hearings in 2013, followed by some legislative proposals. At this point, however, it is too early to tell what form any such proposals might take.

COPPA

The FTC is winding up a proceeding to amend and extend its regulation implementing the Children's Online Privacy Protection Act (COPPA). See "FTC Eyes Children's Privacy and Telemarketing," November 2012, *Privacy In Focus*, available at www.wileyrein.com/coppa. Its proposal received substantial criticism from online services and related technology companies as being overbroad, counterproductive and possibly unconstitutional. Nonetheless, indications are that the final rules may not vary significantly from the agency's proposal.

If adopted, the new rules may well be challenged in court. Such an appeal would raise potentially important questions of constitutional and administrative procedure. Stay tuned.

Do-Not-Track

The concept of "Do-Not-Track" continues to be contentious. Stoutly opposed by the online advertising community while supported by some privacy advocates and the FTC, the current process of developing a Do-Not-Track standard at the World Wide Web Consortium has become mired due to disputes over exactly what "Do Not Track" means. Major questions of scope (is the standard limited to tracking for marketing purposes, or does it apply to all tracking?) and whether advertising networks must honor default browser settings that are set to "no tracking" have to date been insurmountable. In November, the W3C appointed Professor Peter Swire to try to revive the process.

Professor Swire's appointment may buy the W3C some time, but the FTC does not have unlimited patience. The agency has made clear that it believes that a workable and effective Do-Not-Track approach is desirable, and that if industry cannot work something out, it may try to play a larger role. Just how it would do so is unclear, but businesses in online advertising, along with the publishers and websites that depend upon their services, should pay close heed.

Do-Not-Call and Text Messaging

Although the Do-Not-Call registry is one of the most popular privacy initiatives undertaken by the government, many consumers complain that scofflaws flout the registry at will and that they continue to receive a vast quantity of unwanted commercial calls. In late fall, the FTC invited technologists to try to develop technological solutions that might help to slow the ongoing onslaught of unwanted calls.

The FTC shares Do-Not-Call enforcement responsibility with the FCC. The FCC is expected to have a new chairman in 2013. The new chairman will oversee continued FCC enforcement of the Telephone Consumer Protection Act's (TCPA) telemarketing restrictions.

One of the more contentious issues is text messaging marketing. Although the FCC believes that text messaging is covered by the TCPA, that position is being challenged in a number of cases. In addition, pending now before the FCC are a number of petitions regarding text messaging, as parties urge the FCC to exempt certain types of messages from the current strict prohibition. Keep an eye on developments in this

area.