


PRIVACY YEAR IN REVIEW

By: Leita Walker[1] and David Merritt[2]

Privacy continued to be big news in 2012, starting with the release of privacy reports by both the White House and the Federal Trade Commission, followed by a state-led crackdown on asking employees for social media passwords, and ending with the first enforcement action under California's Online Privacy Protection Act and amendments to the COPPA rule. In addition, the year was marked by a number of interesting bill proposals and court decisions. We discuss the highlights below.[3]

White House, FTC release privacy reports.

In late February 2012, the White House released its "Consumer Privacy Bill of Rights," aimed at protecting consumers' private information. The document set forth the following globally recognized fair information practice principles as "baseline" protections: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.

The Obama Administration called on Congress to enact the Bill of Rights through federal legislation and to provide the FTC and state Attorneys General with authority to enforce its principles. The Administration also called for creation of a multi-stakeholder process to specify how the principles apply in particular business contexts and for greater interoperability with international privacy frameworks.

The March 2012 FTC privacy report emphasized privacy by design, simplified choice, and greater transparency, and identified five action items: Do-Not-Track, mobile, data brokers, large platform providers, and promoting enforceable self-regulatory codes.

A few weeks later, in March, the FTC released its final report outlining best practices for businesses to protect the privacy of American consumers and to give them greater control over the collection and use of their personal data. Like the White House framework, the FTC's report—titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers"—recommended that Congress consider enacting general privacy legislation, as well as data security, breach notification, and data broker legislation.

The best practices recommended in the FTC's report were organized in a three-part framework:

- **Privacy by Design:** Companies should build in consumers' privacy protections at every stage in developing their products. These include reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy;
- **Simplified Choice for Businesses and Consumers**: Companies should give consumers the option to decide what information is shared about them, and with whom. This should include a Do-Not-Track mechanism that would provide a simple, easy way for consumers to control the tracking of their online activities.
- **Greater Transparency**: Companies should disclose details about their collection and use of consumers' information, and provide consumers access to the data collected about them.

The report also identified the FTC's five main action items: Do-Not-Track, mobile, data brokers, large platform providers, and promoting enforceable self-regulatory codes. While the new report does not itself establish any new laws or regulations, in a dissenting opinion Commissioner Thomas Rosch wrote that companies that fail to comply with the "best practices" may "face the wrath of 'the Commission' or its staff."

States Prohibit Employers From Demanding Social Media Passwords, Otherwise Increase Privacy Protections

In April, Maryland became the first state to ban employers from requesting access to the social media

Continued on page 13

1 Leita Walker is chair-elect of the Media, Privacy and Defamation Committee and editor of the committee's newsletter. She is an associate in the intellectual property group in the Minneapolis Office of *Faegre Baker Daniels LLP*.

2 David Merritt is an associate in the intellectual property group in the Minneapolis Office of *Faegre Baker Daniels LLP*.

3 Given the audience of this publication, we have omitted healthcare-related developments from our summary.

be nearly verbatim reports of statements made by [a source]," but stated that "not every alteration of a quote beyond correcting grammar or syntax by itself proves falsity." Instead, the altered quotation must convey what the source "meant."[26]

This standard does provide some breathing room for journalists who do not quote sources verbatim, but it may also serve as an incentive to participate in some kind of pre-publication review of quotations by sources to ensure that the source's intention was conveyed accurately.

A Source's Withdrawal of Consent to Use Quotes Containing Private Facts Eliminates Consent as a Defense to an Invasion of Privacy Claim

If reporters agree to allow quote approval and revision as a condition of obtaining an interview, they should consider the content of the information conveyed by the source. If the quotes contain "private facts" about the source that could be considered highly offensive and not newsworthy, the source's initial consent to the publication of that information would serve as a defense if the news organization were later sued for the publication. Consent can be express or implied. However, if at any point in the negotiation process between the reporter and the source, the source withdraws consent, it can no longer be used as a defense. Media organizations could also be liable for any private information published beyond the scope of the consent granted by the source.[27]

Takeaways for News Organizations and Their Lawyers

Although the decision to permit quote approval prior to publication is primarily one of journalism ethics, news organizations should nevertheless understand the possible legal ramifications, particularly if a promise is made by a reporter and then overridden by editors, as occurred in *Cohen*. Accordingly, it is advisable that the news organization develop a policy on quote approval, including whether it is permitted at all, under what circumstances, who has authority to make a promise, and whether prior approval from an editor must be obtained before the promise is made. Once adopted, it is essential that all editorial and reporting staff be aware of the policy, and apply it consistently.

25 501 U.S. 496.

26 *Masson*, 501 U.S. at 513.

27 *See* Richard E. Kaye, *Invasion of Privacy by Public Disclosure of Private Facts*, 103 Am. Jur. Proof of Facts 3d 159 (Originally published in 2008).

PRIVACY YEAR IN REVIEW

Continued from page 5

accounts of employees and job applicants, followed by adoption of similar laws in California, Delaware, Illinois, Michigan, and New Jersey. Bills proposing such laws remain pending in a number of other states, and in May, numerous Senators and Congresspersons introduced a federal version titled The Password Protection Act of 2012. The state laws have some exceptions. The California law, for example, permits employers to ask an employee to divulge personal social media content that the employer "reasonably believes to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations."

Meanwhile, Vermont and Connecticut joined a growing trend of states by amending their data breach notification laws to encompass reporting to the state Attorneys General or other state authorities. The Connecticut amendments were effective October 1; the Vermont amendments were effective May 8.

And as of March 1, Massachusetts law now requires that organizations sharing personal information about Massachusetts residents with vendors have contracts in place with those vendors that comply with state data privacy and security regulations. Importantly, it does not matter whether a company has a physical presence in Massachusetts: the law requires any company that "owns or licenses" personal information belonging to Massachusetts residents to comply with the new Massachusetts law. Among other things, the law requires companies to (1) encrypt all electronic personal information stored on laptops or portable devices or transmitted wirelessly or across public networks, (2) develop and implement a written information security plan, and (3) ensure that third party service providers that receive personal information agree, in writing, to safeguard the personal information.

California Attorney General Files First Suit Under State's Privacy Law

In early December, a month after notifying scores of mobile application developers and companies

that they were not compliant with the state's Online Privacy Protection Act, the California attorney general announced that she had filed the first legal action under that law, against Delta Airlines.

California's Online Privacy Protection Act—the de facto national law—requires "an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service"—such as a mobile application—to post a privacy policy that contains the elements set out in the act. App owners may be penalized for violating this subdivision if they fail to post a privacy policy within 30 days after being notified of the noncompliance.

Delta was among the companies notified in October that its app, "Fly Delta," needed a privacy policy. According to the complaint, Delta failed to post a policy despite receipt of the notice. The complaint alleged that since 2010 Delta had collected app users' names, telephone numbers, email addresses, frequent flyer numbers and pin codes, photographs, and geo-locations, yet did not have a privacy policy in the app itself, in the platform stores from which the app may be downloaded or on Delta's website. The suit seeks to enjoin Delta from distributing its app without a privacy policy and to apply penalties of up to $2,500 for each violation.

FTC Updates COPPA Rule

In mid-December the FTC adopted final amendments to the Children's Online Privacy Protection Rule that strengthen kids' privacy protections and give parents greater control over the personal information that websites and online services may collect from children under 13.

Among other things, the amendments:

- modify the list of "personal information" that cannot be collected without parental consent (it now includes "geolocation information, as well as photos, videos, and audio files that contain a child's image or voice);
- offer companies a new, voluntary approval process for ways of gaining parental consent;
- close a loophole that allowed kid-directed applications and websites to permit third-parties to collect personal information;
- extend coverage so that in some cases the third-parties collecting information have to comply with COPPA;
- extend coverage to "persistent identifiers" that recognize users across different websites or online services;
- strengthen data security protections by requiring covered websites to release children's personal information only to companies that can keep it secure and confidential;
- require covered website operators adopt procedures for data retention and deletion; and
- strengthen the FTC's oversight of self-regulatory safe harbor programs.

Meanwhile, in early December, the FTC issued a new staff report titled "Mobile Apps for Kids: Disclosures Still Not Making the Grade," which examines the privacy disclosures and practices of apps offered for children in the Google Play and Apple App stores. The report found little progress since 2011 toward giving parents the information they need to determine what data is being collected from their children and who will have access to it. The report urges all entities in the mobile app industry to accelerate transparency, to incorporate privacy "by design," and to give parents easy-to-understand choices about data collection and sharing through kids' apps.

Federal Legislators Introduce Privacy Legislation on Various Topics

On the federal legislative front, a number of lawmakers introduced bills to protect consumers' privacy. In early September, Rep. Ed Markey proposed the Mobile Device Privacy Act. Among other things, this bill would require mobile phone makers, network providers, and mobile app developers to disclose to customers any monitoring software installed on their devices, would require companies that collect personal information through mobile devices to adopt policies to ensure the security of that information, and would allow the FTC, Federal Communications Commission, and state attorneys general to bring enforcement actions.

Along similar lines, An Act Regarding the Protection of Geolocation Information, introduced in October, would codify standard practice of obtaining opt-in consent before collecting precise, real-time location information by making it illegal to collect, disclose, or use geolocation information unless, among other things, the user gains prior consent. The bill does make exceptions for use by law enforcement for an emergency situation or when a warrant has been issued or national security is threatened.

And earlier in the year, in another effort to create a national data breach notification standard, Sen. Pat Toomey introduced the Data Security and Breach Notification Act of 2012. Under the Toomey Bill, if a covered entity "reasonably believes [a security breach] has caused or will cause identity theft or other financial harm" then it must notify all affected individuals "as expeditiously as practicable and without unreasonable delay." The FTC would be charged with enforcing compliance with the Toomey Bill, but in instances where a breach affects 10,000 individuals or more, a covered entity would also be required to report the breach to the Secret Service or the FBI.

Supreme Court Decides Privacy-Related Cases

On January 23, the Supreme Court decided *United States v. Jones*, 132 S.Ct. 945 (2012), holding that the government's use of a GPS device to track the movements of an individual's vehicle constitutes a search within the meaning of the Fourth Amendment. The government had installed a GPS tracking device on Jones's vehicle and consequently used evidence gained from the GPS to prosecute Jones for conspiracy to distribute cocaine.

The Court reasoned that because an automobile is indisputably an "effect" protected under the Fourth Amendment, and the installation was an intrusion into that effect, a "search" within the meaning of the Fourth Amendment had occurred. The Court added that the well-known "reasonable expectation of privacy" test derived from *Katz v. United States*, 389 U.S. 347 (1967), added to, but did not substitute for, the common-law trespassory test. In two separate concurrences, however, five Justices seemed to suggest that GPS usage under the facts of this case violated an individual's reasonable expectation of privacy.

A couple of months later, on March 28 the Supreme Court decided *Federal Aviation Administration v. Cooper*, 132 S.Ct. 1441 (2012), holding that the Privacy Act of 1974 does not waive the federal government's immunity from liability for claims of mental or emotional distress arising from violations of the Privacy Act.

Cooper, a private pilot, withheld information about his diagnosis of HIV from the FAA. When the FAA learned of his diagnosis and shared it with the DOT and SSA, Cooper brought a claim for violation of the Privacy Act for exchanging his records. The Court concluded that the Privacy Act "does not unequivocally authorize an award of damages for mental or emotional distress. Accordingly, the Act does not waive the Federal Government's sovereign immunity from liability for such harms.

A Sneak Peak at 2013…Anticipating a Supreme Court FOIA decision

Journalists and companies that sell public records are hopeful that the U.S. Supreme Court will find the residents-only restriction of Virginia's Freedom of Information Act unconstitutional. The Supreme Court agreed to hear the case, *McBurney v. Young*, in early October.

Virginia is among at least seven states with a law that limits FOIA access to state residents. While the Virginia law has exceptions for "representatives of newspapers and magazines with circulation" in Virginia and television and radio broadcasts that reach Virginia's airwaves, it excludes media outlets that have an Internet-only presence. Proponents of greater governmental transparency are hopeful that the Court will deem the residents-only restrictions unconstitutional, leaving state records open wide to FOIA requests regardless where they originate.

Conclusion

The sensitivity of consumers, legislators, and regulators to privacy concerns shows no sign of waning. Thus, although federal privacy legislation has proven difficult to enact, savvy companies will stay abreast of the ever-evolving field of privacy law in 2013. This is especially true for those expanding their social and mobile presences and for those engaging in online tracking and interest-based advertising. Although the White House and FTC privacy reports are not currently binding, failure to follow the principles they espouse may have real consequences in the future and companies would be well-served by adopting those principles sooner rather than later. ⚖