

# New wave of privacy regulation and enforcement

07.15.2011



By Jay Cline, CIPP

Privacy and marketing professionals should be noticing something in the air. The last 12 months have produced deeper and broader privacy regulation and enforcement across the globe. This wave of activity is the most we've seen since the round of international lawmaking triggered by the 1995 EU Directive on Personal Data and the data breach notification phenomenon that began in 2005.

Technology innovations--many of them used for direct marketing--are generating much of this activity. Recently introduced proposals in the U.S. and EU, as well as actions taken in India and Korea, have signaled greater regulatory interest in smart grid technology, online privacy and location data. Lawmakers and regulators around the globe seem intent on ensuring new technologies incorporate widely accepted fair information practices.

A second driver is bureaucratic momentum. Several regulators tasked with enforcing existing data privacy laws are hitting their stride, launching more investigations and levying greater fines.

## Americas region: More chefs in the privacy kitchen

Both trends are unfolding in the United States. The 2010 Dodd-Frank financial reform act created the Consumer Financial Protection Bureau. As many of the act's provisions take effect this month, the bureau's profile regulating privacy for non-depository financial institutions will increase. The Dodd-Frank Act also increased the powers of the Securities and Exchange Commission, which in April imposed its [first fines](#) for violations of its Regulation S-P Safeguard Rule for data privacy. In February, the Financial Industry Regulatory Authority (FINRA)--which regulates securities firms--imposed its first significant privacy fine, a \$600,000 levy on Lincoln Financial Securities for insufficiently protecting consumer information.

The Federal Communications Commission (FCC), which oversees the [National Do Not Call Registry](#) and regulates telemarketing in general, has also been increasingly asserting itself on data privacy. In recent months, the FCC has been examining the safeguards and implications of location-based services and marketing. At the same time, the U.S. Senate created its first body focused on privacy--the subcommittee on Privacy, Technology and the Law. The subcommittee wasted little time, holding its first hearings on the status of mobile device privacy in May.

The nation's most prominent privacy regulator, the Federal Trade Commission, has also been newly flexing its muscles. In December 2010, the FTC capped a yearlong outreach effort by issuing a landmark [paper](#), "Protecting Consumer Privacy in an Era of Rapid Change." The paper sets out the commission's priorities for the coming several years, including online do-not-track rules and protections for location-based data. In March, the commission--which oversees enforcement of the U.S.-EU Safe Harbor agreement, the Children's Online Privacy Protection Act, CAN-SPAM Act, Gramm-Leach-Bliley Act Safeguard Rule, Health Breach Notification Rule and Red Flags Rule--showed its

resolve to pursue its new set of priorities. The commission reached a [settlement agreement](#) with Google over its Google Buzz product, claiming the company misrepresented that it protected users' confidentiality. The settlement was the first time the FTC enforced substantive noncompliance with the Safe Harbor agreement.

Over the past year, the U.S. Department of Health and Human Services (HHS) has established itself as one of the nation's other leading privacy regulators. Following the implementation of the HITECH health data breach notification rule, the HHS Office for Civil Rights has stepped up its levying of fines-- most notably on the University of California (\$865,500 in July), Cignet (\$4.3 million in February), Massachusetts General Hospital (\$1 million in February) and RiteAid (\$1 million in July 2010).

The Department of Education (DOE) is also jumping into the privacy fray. The department regulates compliance with the Family Educational Rights and Privacy Act (FERPA). Largely because of a 2002 Supreme Court ruling concluding that FERPA does not create enforceable personal rights, the department has not pursued substantive enforcement actions of the act. This may be changing. In April, the DOE released a [Notice of Proposed Rule Making](#) under FERPA that would lay the groundwork for stricter protections and enforcement over student data sharing and use of student data for marketing.

Privacy regulation and enforcement at the U.S. state level has also picked up over the past year. The rise of smart grid technology has prompted several public utility commissions (PUCs) to issue rules on protecting consumer information under their purview. In May, the California Public Utility Commission adopted a [proposal](#) that would require smart grid operators to minimize data collection and only use it for the purposes collected. The Colorado and Minnesota PUCs have been following similar paths.

Health commissioners, insurance commissioners and attorneys general in a growing number of states have been initiating enforcement actions to protect the privacy of consumers in their states. Most recently, the Indiana attorney general imposed a \$100,000 [fine](#) on Wellpoint for a data breach.

More privacy regulation is also developing in Canada and Latin America, although these parts of the Americas region have not yet seen a trend toward the imposition of fines for privacy violations. In December, Canada passed its long-awaited anti-spam law, which comes into effect this summer for companies conducting e-mail marketing in the country. This month, Peru also adopted its first national data protection law. In April 2010, Mexico similarly passed its national data protection law and created one of the most well-financed and staffed data protection authorities (DPAs) in the world. Indeed, an IAPP survey of DPAs worldwide, to be released later this year, will reveal that Mexico tops all other DPAs surveyed with a \$38 million (USD) annual budget, followed by Italy (\$35 million), the UK (\$32 million), Canada (\$25 million) and Spain (\$22 million).

### **Europe: Turning a new page on privacy**

The European Union has encountered over the years two main critiques of its privacy regime: that it hasn't kept pace with technological change and that member state enforcement has been generally light. These critiques have started to lose force over the past year, as Europe enters a new era of data protection oversight.

Last November, the European Commission issued a [proposal](#) for modernizing the 1995 Data Protection Directive. The proposal would usher in a sweeping set of changes, including stricter rules on data retention and breach notification and harmonized enforcement. In May, EU member states also passed the deadline for implementing enhancements to the EU Privacy and Electronic Communications Directive. The enhancements included far-reaching changes to how websites administer and gather

consent for placing cookies on user computers. The UK and the Netherlands were two of the first member states to codify the new restrictions. According to analysts, new EU cookie laws will have a tremendous effect internationally. This development follows a significant decision from the EU Article 29 Working party defining mobile device location data as personal data.

Over the past year, Europe also continued its global leadership on the data protection docket. At the 32<sup>nd</sup> Annual International Conference of Data Protection and Privacy Commissioners in Jerusalem, EU delegates were instrumental in continuing to promote a [global agreement](#) on data privacy.

A handful of EU member states also imposed significant fines over the past year. According to the 2011 IAPP benchmarking survey of data protection authorities to be released at the 33<sup>rd</sup> Annual International Conference of Data Protection and Privacy Commissioners in Mexico City, European DPAs collected more than \$31 million in fees in the past year. Just three member states--Spain, Italy and the UK--accounted for nearly all of this amount, however. In April, the French DPA, CNIL, warned businesses and individuals of its plans to increase compliance inspections and enforcement of cross-border data transfer practices, particularly by companies enrolled in the U.S.-EU Safe Harbor Program.

### **Asia: laying foundations**

The IAPP's landmark paper "[A Call For Agility](#)" identified the Asia-Pacific region as the next frontier awaiting a privacy makeover. The past year may have seen the opening act. In April, India [adopted](#) its first comprehensive privacy framework, the *Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules*. The rules amend the Information Technology Act of 2000 and broadly require prior consent for collection of personal data within the country. In May, Korea published draft regulations of its Personal Information Protection Act (PIPA), scheduled to become effective in September. The country's most far-reaching privacy law to date restricts the collection, use and retention of personal data. The law also ties together previous data protection laws covering telecommunications into a comprehensive framework governing "personal information" and its handlers.

### **Outlook**

What does the rising tide of privacy regulation and enforcement portend for marketing and privacy professionals?

For marketers, there will be a growing premium on those who develop expertise on data privacy regulations and Privacy by Design. They will need this expertise to steer their clients through the maze of acceptable and prohibited uses of personal data. Look for more marketers pursuing the Certified Information Privacy Professional designation.

For privacy professionals, the spread of privacy regulation across new countries and sectors will create new opportunities for specialists with niche experience and expertise. Heightened enforcement actions should increase the overall demand for privacy expertise and, particularly, for experience managing regulatory investigations.

*Jay Cline, CIPP, is president of [Minnesota Privacy Consultants](#), the winner of the 2010 Privacy Innovation Award for Small Organizations.*