The Forecast is for Continued Controversy and Bold Statements with (Maybe) Some Action:
Privacy, Cybersecurity and Regulatory Trends for 2012

A White Paper

March 8, 2012

Dr. Don Lloyd Cook
Director of Privacy, Lunarline, Inc.
Table of Contents

1 Introduction ................................................................................................................................................. 2

2 US Congress ............................................................................................................................................... 2

3 Federal Departments and Agencies ........................................................................................................... 5

4 The White House ...................................................................................................................................... 8

5 The European Union ................................................................................................................................ 10

6 Conclusion ............................................................................................................................................... 11
1 Introduction

Data surrounds us, we live in a sea of data where almost every action we take will generate additional data about our likes, dislikes, activities, location and innumerable other variables. Increasingly, that data is collected and used in a variety of ways, some of which we may not be aware of. In an era of “big data”, privacy and cybersecurity generate a lot of debate and great deal of interest on the part of government, business, and of course, consumers. A recent study reported that 90% of American adults were concerned about their privacy, particularly online privacy. Legislators and regulators are also active and the continuing growth of the online economy means they have to be cognizant of balance between competing needs. As recent observers noted: “In order to craft a balance between beneficial uses of data and the protection of individual privacy, policymakers must address some of the most fundamental concepts of privacy law, including the definition of ‘personally identifiable information,’ the role of consent and the principles of purpose limitation and data minimization.”\(^1\) The same arguments can also readily be made for cybersecurity as well. Security is necessary for effective privacy and the two are inextricably intertwined. Movement toward the cloud has increased activity among legislators and regulators regarding cybersecurity in particular.

While there is a lot of interest and activity, this will probably not be the year that privacy experts and pundits anoint the upcoming year as a “big year in privacy,” with predictions of sweeping legislation and regulatory change. Because of the largely deadlocked Congress and upcoming elections, we are not likely to see much in the way of sweeping legislation, but that doesn’t mean that there aren't important trends worth watching. Even if nothing much gets done in the way of new legislation, at least in the US, legislative hearings and debate, as well as regulatory and advisory publications from the Executive branch will continue to frame and influence the direction of future privacy and cybersecurity laws.\(^2\) Just as many of the key privacy events of this year will have been triggered by earlier debates and legislation, watching the evolution of thought on privacy through this year will gives us some clues about what will be in store in the future. In turn, we will talk about activities in the US Congress, in Federal agencies such as the Federal Trade Commission (FTC), and in the European Union (EU), and look where these trends may take the privacy profession.


The US Congress

Privacy and cybersecurity have long been areas of interest to Congress, and the 112th Congress has been no exception. However, as noted before, gridlock has meant that few proposals have actually become law and the bills proposed have largely continued the sectoral approach to privacy regulation with bills dealing with specific issues rather than a more global approach. That being the case, there are several bills that are currently active that are worth examining. The list is not exhaustive, but looks at the bills which are showing the most activity.

Location privacy in the context of mobile devices has generated several bills including the Location Privacy Protection Act of 2011, introduced by Senator Franken, and the Geolocation Privacy and Surveillance (GPS) Act, introduced by Senator Wyden and Congressman Chaffetz. While both of these bills are concerned with location privacy, they take very different approaches. Senator Franken's bill focuses on the need to obtain express consent from mobile-device users before their locations are collected and shared with third parties, such as advertisers, but addresses only non-governmental data collections. Governments and police forces would enjoy unlimited data-collection capabilities. The GPS act is “designed to give government agencies, commercial entities and private citizens clear guidelines for when and how geolocation information can be accessed and used.” It covers government and private entities and contains a warrant requirement for obtaining the location information of individuals by law enforcement under the same standards as a wiretap warrant. Given the Supreme Court's recent decision in US v. Jones, where the Court found that placement of GPS tracking device on a vehicle owned by the defendant's wife without a warrant constituted a search under the Fourth Amendment, there may be more impetus to pass statutes that would clarify restrictions on use of GPS or location information, at least for law enforcement. However, it

---


4 S.1223, Location Privacy Protection Act of 2011

5 Geolocation Privacy and Surveillance ("GPS") Act of 2012, full text.


Writing for the Court, Justice Scalia found that it was not necessary to determine whether Jones had a “reasonable expectation of privacy” in the underbody of his Jeep parked on a public street because the search violated the Court’s traditional common-law trespass test. Scalia stated: “It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.”
should be noted that efforts to reform aspects of the antiquated Electronic Communications Privacy Act (ECPA), have not yet been successful in spite of being well received and the widespread agreement that the main federal wiretap statute (written before the existence of the commercial Internet and cell phones) is in serious need of an overhaul and update.\(^7\)

A third bill affecting location privacy, but more broadly addressing mobile privacy in general is the \textit{Mobile Device Privacy Act}\(^8\) proposed by Congressman Edward Markey and currently being circulated as a discussion draft. This bill requires notification of consumers whenever mobile tracking software is installed on a phone, including what data is being collected, how it will be used and, critically, who will get it. Express consent must be obtained from consumers to track and share their information. An additional requirement is that third parties who receive this data must file agreements with the Federal Trade Commission and the Federal Communications Commission (FCC).\(^9\)

The use of tracking techniques by behavioral advertisers has been an ongoing issue ever since the contentious NebuAd hearings\(^10\) in 2009 and 2010 and there are several bills dealing with online tracking. There are three bills currently focused on this issue, with one of them specifically addressing the issues of collecting information from children. H.R. 654, the \textit{Do Not Track Me Online} bill proposed by Rep. Jackie Speier would require the FTC to regulate online tracking or individuals for purposes of collecting or using their information. The Senate corollary is S. 913, proposed by Senator Rockefeller. The third bill, proposed by Rep. Markey, is HR 1895, the \textit{Do Not Track Kids Online Act}, focusing on the online tracking and collection of information from children and would amend the \textit{Children's Online Privacy Protection Act} (COPPA).

There are also several other bills with a variety of goals. H.R. 1389: \textit{Global Online Freedom Act} of 2011 (Rep. Christopher Smith) is aimed at preventing US businesses from assisting repressive governments into “transforming the Internet into a tool of censorship and surveillance.” A later version of this bill was filed as H.R. 3605, also entitled \textit{Global Online Freedom Act}. Other bills concern the desire to keep the Internet free and open and universally available (S. 74 \textit{Internet Freedom, Broadband Promotion and Consumer Protection Act}, by Sen. Cantwell), to promote information openness by the Government (H.R. \textit{Public Online

\(^7\) Gibbs, Mark (2011), While we wait for cold fusion, let’s update the ECPA, Network World, October 24.


\(^9\) Craig Blaha (2012), Mobile Device Privacy Act: The Good the Bad, and the Ugly

Information Act, by Rep. Israel, with a companion Senate bill, S. 717, with the same title by Sen. Tester) and two bills governing online intellectual property which had strong privacy implication and that were strongly opposed and are now considered dead for at least this session, S. 968, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP) by Sen. Leahy and on the House side, H.R. 3261, the Stop Online Piracy Act by Rep. Lamar Smith. As a final note, there are reports that Senate Majority Leader Harry Reid is preparing a bill that would establish a federal data breach notification statute that would replace the current patchwork of 48 state breach notification laws that now exist. Neither a definitive timetable nor a discussion draft had been released at the time of this writing.

On the cybersecurity side, it looks more likely that Congress may move past gridlock to move cybersecurity legislation forward, something that both parties appear to agree is needed. This rare display of unity may break down as the bills move through the legislative process and individual sections of the bills are debated. This has been the case with the Cybersecurity Act of 2012, proposed by Senator Leiberman and co-sponsored by Sen. Collins, which has drawn criticism both over its content and legislative process, with several Senate committees demanding a hand in crafting the bill. Combining previously introduced cybersecurity bills, the Cybersecurity Act would give the Department of Homeland Security (DHS) the power to establish security standards for designated critical infrastructure systems. A self-certification regime would also allow DHS to seek civil penalties for non-compliance with the standards. The previous controversial provision giving the President emergency powers to disconnect some portions of the critical infrastructure from the Internet has been dropped, as has the requirement for a White House Cybersecurity Office (although it does create a White House Office of Cyberspace Policy). The Act would also include Federal Information Security Management Act (FISMA) reform which would “provide a comprehensive framework for ensuring the effectiveness of information security controls” and “a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than overly prescriptive manual reporting.” The Act, which would give DHS FISMA oversight defines, “continuous monitoring” as “the ongoing real-time or near real-time process used to determine if the complete set of planned, required and deployed security controls within an information system continue to be effective over time in light of rapidly changing information technology and threat development.” The bill is still very comprehensive in that DHS would be given the authority to monitor all government system traffic once it is certified that security needs justify access.

On the House side, it appears that Congressmen will wait to see where the Senate bill goes, but will probably introduce their own comprehensive cybersecurity bill during the session. H.R. 3674 the Promoting and Enhancing Cybersecurity Act introduced by Reps. Lundgren and
King is aimed at facilitating information exchange between the private sector and government to improve cybersecurity. A similar purpose is ascribed to *The Cybersecurity Information Sharing Act*, S. 2101 introduced by Senator Feinstein separately from the comprehensive *Cybersecurity Act*. S. 2101 takes the additional step of attempting to facilitate information sharing between private companies for cybersecurity purposes as well as sharing with the government.

3 Federal Departments and Agencies

The Federal Trade Commission and the Federal Communications Commission are among the federal agencies with significant responsibilities for privacy and cybersecurity issues. The FTC is the federal government’s chief enforcer for privacy, but has also acted against numerous companies whose privacy breaches were security related. The FTC has authority under Section 5 of the *FTC Act* to challenge unfair or deceptive acts or practices in or affecting commerce. Under the unfairness doctrine it has prosecuted companies who failed to maintain reasonable security around personally identifiable information (PII) as well as pursuing actions against companies that claimed to have reasonable security but actually did not for deceptive practices. The FTC has signaled that although it is still pushing self-regulatory efforts where possible, that it will take an aggressive approach to privacy (and cybersecurity) enforcement. One area of concern that has been specifically mentioned by FTC Chairman Jon Leibowitz is the increasing use of facial recognition technologies.\(^{1}\) Additionally, the FTC is maintaining its support of “Do Not Track” solution with respect to behavioral advertising. The FTC has maintained several high profile actions against Google and Facebook (social media also being a priority issue at the FTC) for changes to their privacy policies that it felt might be detrimental to consumers. The FTC also issues a yearly report which details its enforcement activities which gives great insight into the enforcement priorities of the Commission.

Besides the activities of the FTC, the FCC also has its own niche as a privacy and cybersecurity enforcer; include enforcing the privacy provisions of the *Cable Act* and other telecommunications legislation providing guidance and information in a variety of areas. The FCC’s Privacy and Online Security web page details its efforts directed toward individual consumers and small businesses. It also has jurisdiction over the use of CPNI (Consumer Proprietary Network Information) and the privacy and security practices of common carriers. The Commerce Department has also become increasingly active around privacy issues, although

quite respectful of the FTC’s traditional role as privacy enforcer. The Commerce Department is set to release it report containing a new framework for businesses to create a self-regulatory regime (the FTC is also issuing a similar report) sometime in the next few months. While the recommendation will not be binding, they are expected to be influential as privacy regulation continues to develop.

While the FTC and FCC handle many of the government’s initiatives with respect to privacy and cybersecurity in the private sector, within the government it is often the National Institute for Standards and Technology (NIST) that influences what happens within government. Even non-binding guidelines emerging from NIST are treated with great deference inside and outside of the government. NIST has been very active on both privacy and cybersecurity issues and has issued a number of reports and guidelines. Among the most prominent of the many NIST initiatives on privacy and social security are NIST 800-144, Guidelines on Security and Privacy in Public Cloud Computing and an updated fourth draft of NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The guidelines were created with the goal of encouraging entities to carefully plan the security and privacy aspects of cloud computing solutions before implementing them and to understand the public cloud computing environment offered by the cloud provider. The guidelines also direct entities to ensure that a cloud computing solution—both cloud resources and cloud-based applications—satisfy organizational security and privacy requirements and finally to maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments. NIST 800-53 addresses the “Risk Management Framework security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. This includes selecting an initial set of baseline security controls based on a FIPS 199 worst-case impact analysis, tailoring the baseline security controls, and supplementing the security controls based on an organizational assessment of risk. The security rules cover 17 areas including access control, incident response, business continuity, and disaster recoverability.” Focus areas of the fourth draft include privacy, insider threats, supply-chain security, and social networks and mobile devices.

At the Office of Civil Rights, one of the Department of Justice offices tasked with enforcing the Health Insurance Portability and Accountability Act 12, better known as HIPAA, indications are that enforcement actions will continue to increase in 2012. Since HIPAA includes both a Privacy Rule and a Security Rule, there may be considerable activity in both areas. Peter Fleischer, the global privacy counsel for Google recently said in his personal blog that “[t]here

\[\text{http://www.legalarchiver.org/hipaa.htm}\]
will be blood...the healthcare industry is well advised to wake up and smell the data breaches...2012 will be the year of enforcement.” 13 To implement its mandate under the Health Information Technology for Economic and Clinical Health Act (HITECH) to provide for periodic audits for covered entities and business associations. “OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance. Audits conducted during the pilot phase will begin November 2011 and conclude by December 2012.” 14 In addition the Center for Medicare and Medicaid Services (CMS) at the Department of Health and Human Services (HHS) will begin enforcement of the new electronic data transmission requirements under the New Health Care Electronic Transactions Standards Versions 5010, D.0, and 3.0, 15 although the effective date for enforcement has been delayed 90 days from the original January 1, 2012 deadline. In addition HHS published its interim final rule for standards for health care electronic funds transfers (EFTs) and remittance advice in the Federal Register on January 10, 2012, opening it for comments.

Finally, one of the more significant developments came from the Securities and Exchange Commission (SEC). The SEC issues guidelines 16 on October 13, 2011, outlining how and when publicly traded companies should report hacking incidents and cybersecurity risk. Although presented as a guideline, it has been widely interpreted as a distinct warning that should companies fail to disclose significant privacy and cybersecurity incidents on an ongoing basis, that the SEC will issue additional rules making the disclosures mandatory and subject to significant penalties where disclosure is not made.

4 The White House


13Leyva, Carlos (2012) HIPAA Compliance: Is 2012 the year of enforcement (redux)? At LawTechTV.com

14http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html


Privacy Bill of Rights," the Framework bases its Bill of Rights upon the well founded Fair Information Privacy Practices (FIPPs). The basic Rights enumerated are:

1.) **Individual Control:** Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

2.) **Transparency:** Consumers have a right to easily understandable and accessible information about privacy and security practices.

3.) **Respect for Context:** Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

4.) **Security:** Consumers have a right to secure and responsible handling of personal data.

5.) **Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.

6.) **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain.

7.) **Accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The Framework advocates a mix of legislation, industry standards and codes of conduct formed through multistakeholder processes, and stepped up enforcement through the Federal Trade Commission as primary mechanisms to create a climate of privacy that would enhance consumer trust in internet commerce and its enabling institutions. While the idea that regulatory mechanisms may promote consumer trust is not a new one\(^\text{17}\), this formulation represents an important milestone because of the direct involvement of the White House and the Obama Administration. This is the first cohesive privacy proposal to emanate from the Oval

---


Office and as a policy document it is very reminiscent of the Clinton Administration's “A Framework for Global Electronic Commerce”\textsuperscript{18}, which also posited a broad vision for the online world.

The Framework explicitly notes that it is focused entirely on private-sector behaviors and does not address governmental handling of personal information. In addition, although it expresses a preference for Congress to enact and codify significant sections of the Framework, there is an expressed sense of recognition that the current political environment may make extending the current mix of regulation and self-regulatory structures as a more practical alternative. The Framework notes that: “[e]nacting the Consumer Privacy Bill of Rights through Federal legislation would increase legal certainty for companies, strengthen consumer trust, and bolster the United States' ability to lead consumer data privacy engagements without international partners. Even if Congress does not pass legislation, the Consumer Privacy Bill of Rights will serve as a template for privacy protections that increase consumer trust on the Internet and promote innovation.” Notably, one of the primary mechanisms for advancing and enforcing privacy protections mentioned in the Framework is to strengthen FTC enforcement and to grant the FTC greater power and resources to pursue that goal. While granting the FTC greater enforcement powers and resources is primarily the purview of Congress, the Executive and the FTC do not need Congressional approval to put more emphasis on enforcement under the FTC's power to seek redress for actions that are unfair or deceptive with respect to consumers. The FTC has already been vocal about the need for “Do Not Track” mechanisms to provide greater consumer choice governing data collection in Online Behavior Advertising and the Framework echoes those concerns.

The reviews of the Framework were mixed among the regulators, businesses, and advocacy groups, but the overall response was fairly positive, if a bit predictably skewed in the direction of each group's privacy orientation. At privacy advocacy group, the Center for Democracy and Technology, a privacy advocacy group, Justin Brookman, the Director of the Consumer Privacy Project argued that the administration is finally taking privacy seriously. Internet giant Microsoft charted a neutral course with the pronouncement that “[c]onsumer trust is vital to the growth of the Internet, and respect for privacy – putting people first – is essential to earning and maintaining that trust.”\textsuperscript{19} However a cautionary note was sounded by attorney Jeremy D. Mishkin (Montgomery, McCracken) who noted that “[t]he cynics will note

\textsuperscript{18}President William J. Clinton & Vice President Albert Gore, Jr., \textit{A Framework for Global Electronic Commerce} (July 1, 1997) (full-text)

that while the aspirations contained in the Privacy Bill of Rights are noble, Web users are only too familiar with lofty rhetoric that sadly is not matched by action. They've talked the talk, now we have to see if they walk the walk."\(^\text{20}\)

A more nuanced view of the Framework suggests that it is best viewed as a general declaration of intent rather than an actual blueprint for prospective regulation. The White House appears to be very cognizant of the difficulty of passing new legislation in the current environment and equally cautious about taking steps that could potentially inhibit innovation in the online space. The reliance on self-regulatory mechanisms and increased FTC enforcement indicate that the White House sees itself as making use of the “Bully Pulpit” to influence and direct the evolution of privacy thought and the subsequent development of a variety of governmental, quasi-governmental and private regulatory mechanisms. However, there is also a sense of commitment to using existing laws and regulations more forcefully to protect consumer privacy. Observers will be carefully watching the actions of the FTC and other federal regulatory agencies for clues to what approach will ultimately be taken.

5 The European Union (EU)

Although the US follows a fundamentally different approach to privacy protection than the EU\(^\text{21}\), the actions of the EU on privacy and security are very influential worldwide, with more countries following the EU approach than the US approach. In addition the fact that the EU is one of the largest trading partners leads to the unsurprising news that the FTC and “EU Member States are working on an overarching privacy framework agreement with the United States. More recently, the Consumer Data Privacy Framework issued by the White House specifically dedicated a section to “Promoting International Interoperability.” Thus it is particularly significant that the EU is introducing a new Data Privacy Directive to replace the 1995 Directive 95/46/EC. The old Directive was written and enacted before the massive expansion of the Internet. Vivian Redding, the EU Justice Commissioner has remarked that “[i]n a world of ever-increasing connectivity, our fundamental right to data protection is in this moment seriously tested. Although the basic principles and objectives of the 1995 Directive remain valid, the rules need to be adapted to new technological challenges.”\(^\text{22}\) Given the influence of the EU,

\(^{20}\) Ibid.

\(^{21}\) Under EU law, privacy is viewed as a fundamental human right governed by the broad-based 1995 Directive 95/46/EC, whereas US law is sectoral in nature, with laws developed to address specific problems and generally based more in property rights.

\(^{22}\) http://www.cnn.com/2012/02/23/opinion/reading-europe/index.html
developments such as this and the new “Right to Be Forgotten,” which allows some actions of internet consumers to disappear or be removed over time, bear close watch.

6 Conclusion

2012 is shaping up to be an important, if not seminal, year in privacy and cybersecurity. Although looking into the crystal ball is fraught with the potential for error, there are a couple of broad themes that we can expect to see over the course of the next year.

- HIPAA/HITECH enforcement will continue
- Mobile will continue to challenge existing privacy and cybersecurity laws. Technology has once again outstripped the regulatory structure and old laws and regulations will be increasingly hard to adapt to the changed environment.
- Geolocation will be a hot issue on both the government and business side and developing technologies such as facial recognition will get additional scrutiny as they become embedded in more applications.
- Social media will be equally praised and castigated. Social Media has been somewhat neglected in this white paper because at this stage of its development, everybody sees issues, but there is no consensus on what the pain points are and which ones should be remediated. Expect this situation to change and evolve throughout the year as social media continues to grow and mature
- Cybersecurity will continue to be a pressing issue for governments and business alike. High profile hacking incidents will continue to motivate calls for cybersecurity legislation.
- There will be at least one new wrinkle in privacy and cybersecurity that all of the prognosticators and pundits will have missed.

What does this mean for business?

For Lunarline partners and others in the business community, the key take-away is that privacy will continue to be a front-burner issues, albeit one that will probably not generate a lot of new legislation. Instead we will see a greater focus on continued and increased enforcement by the FTC and other federal agencies and increased activity on the part of the various State Attorneys' General. The visibility of privacy as an issue will continue to increase and the consequences for
companies caught on the wrong side of the privacy equation (e.g. through breaches or FTC actions) will increase at an even greater rate. The sectoral approach pursued by the US provides a very high degree of uncertainty and the emerging legal practice area of privacy law provides significant opportunities for plaintiff's attorneys to make use of the gaps in existing law. We will see more and more public privacy incidents which will be increasingly tied to public visibility and resulting negative publicity, greater impacts on consumer opinions of companies, higher fines and increasing likelihood of lawsuits from consumers. It is important to remember that the impacts of privacy incidents are typically cumulative, if not multiplicative in nature. For example, a typical FTC enforcement action against a private company will not only involve a fine and a adjudicated commitment to change some type of corporate practice, but also requires several years of monitoring paid for by the company itself. Added on to that is the negative publicity and the resultant potential effect on the brand equity and consumer perception of the company. With the average breach now costing the breaching entity well over $200 per record breached, companies who do not address privacy proactively will pay an increasingly painful price.

---

23 Recently issued Securities and Exchange Commission guidelines strongly advise publicly held companies to make note of significant privacy incidents in certain of their required SEC filings.

24 Cost of a data breach climbs higher, at Ponemon.org. The Ponemon Institute is one of the most prestigious and widely cited privacy think tanks.