Before the
Department of Commerce
Internet Policy Task Force

In the Matter of the Request for	)	
Comments on Information Privacy and	)	**Docket No. 100402174-0175-01**
Innovation in the Internet Economy	)	

COMMENTS OF THE STATE PRIVACY & SECURITY COALITION

Jim Halpert
Adrian Copiz
DLA Piper
500 Eighth Street, NW
Washington, DC 20004
(202) 799-4000

June 16, 2010

June 16, 2010

FILED ELECTRONICALLY

National Telecommunications and Information Administration
US Department of Commerce

In the Matter of the Request for Comments on
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174-0175-01

Comments of the State Privacy & Security Coalition on Information Privacy and Innovation in the Internet Economy

I. INTRODUCTION

The State Privacy and Security Coalition very much appreciates both the Department's undertaking this NoI and this opportunity to submit comments.

A. Description of State Privacy & Security Coalition

State Privacy & Security Coalition ("the State Coalition") members include a broad cross-section of the US technology and media industries – companies and trade associations who are vitally concerned with barriers to innovation posed by conflicting state privacy, security and e-commerce regulation: Amazon.com, AOL, AT&T, Cisco, Comcast, HP/EDS, Facebook, Fox Interactive, Google, Monster.com, Reed Elsevier, Skype, TimeWarner Cable, Verizon, and Yahoo!, the Entertainment Software Association, Internet Alliance, the NA*i,* NetChoice, Technology Association of America, and TechNet.

Our Coalition has a wealth of experience in the issues raised in the State portion of the NOI. Its focus is on state privacy, security and e-commerce proposed laws and regulations that would create barriers to doing business on a nationwide basis.

At the same time, most of its members do business internationally and are strongly supportive of the Department's efforts to reduce barriers to innovation posed by conflicting international regulation.

The State Coalition was formed in the wake of passage of a sweeping California opt-in spam law with $1,000 per message class action exposure and an overbroad Utah "anti-spyware" law that imposed broad notice and consent download restrictions on a wide array of routine, beneficial software programs that are not spyware, including parental controls software. The

first law was preempted by Congress through the CAN-SPAM Act[1], before it could take effect. The second was enjoined by a Utah state court on First Amendment and Dormant Commerce Clause grounds.[2] However, both these narrow misses highlighted the threat to Internet innovation and growth posed by disparate and overbroad state privacy and security regulation. These laws underscored the need for technology and media companies and trade associations to join forces to work proactively to manage these significant risks to innovation.

A white paper from the Department or the White House explaining potential barriers to innovation caused by disparate state privacy and data security regulation would be very helpful. State policymakers, many of whom are part-time legislators, are well intentioned, but often make law in a climate of suspicion of new technologies and without full information about the often complex issues raised by new technologies.

B. The Significant Threat to Innovation Posed by State Regulation -- The Large Volume of State Regulation and Near Misses

In recent years, state legislatures have enacted over 100 state privacy and data security-related laws. This includes security breach laws in 46 states plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, 10 data security laws for the protection of personal information, data disposal laws in 19 states, RFID privacy laws in 13 states (with multiple laws passed in Washington, California and New Hampshire), phishing laws in 22 states, spyware laws in 15 states, 37 spam laws, 24 online sexual predator laws, 2 recent credit history privacy laws, and 3 online privacy laws.

The NOI asks only about laws. It is important to recognize that every year, but for the efforts of affected stakeholders, including the technology industry, privacy advocates, and civil libertarians, there would be dozens of additional state privacy and security laws that would make it exceedingly difficult (if not impossible) to operate in the Internet environment and provide commensurate levels of privacy and data security to all users. State barriers to innovation are a significant threat. Policymakers at the state level are actively seeking to regulate in this area, even if relatively few laws are ultimately enacted.

For example, In 2004, Utah enacted a "spyware control act," H.B. 323,[3] which imposed detailed notice, consent and uninstall requirements for any software that triggered an advertising based upon user activity if that advertisement obscured any part of a webpage or advertising on a webpage. Trademark owners, website owners, and advertisers could all sue under the law for $10,000 statutory damages per advertisement displayed, plus attorneys' fees. The law was phrased sufficiently broadly that it reached a wide variety of other software downloads that presented advertising when a user's browser was open, exposing software distributors to lawsuits for significant statutory damages

[1] 15 U.S.C. § 7707(b).
[2] *WhenU v. State of Utah*, (June 22, 2004), transcript available at http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf.
[3] Available at http://www.benedelman.org/spyware/utah-mar04/bill.html.

In 2007, both North Carolina and Connecticut came very close to enacting unworkable age verification mandates for a broad range of websites that bills in these states defined as social networking sites. Neither bill passed, and a Berkman Center Report on child protection issued the following year highlighted privacy and security flaws in the age verification approach, which had been advocated by several vendors.[4] This year, a California bill, S.B. 1361,[5] would prohibit including an address and phone number field in online profiles of users known to be under the age of 18.

In 2009, Maine passed a teenage marketing law, L.D. 1183[6], that had the effect of extendeing the federal Children's Online Privacy Protection Act (COPPA) to 17 year-olds and to offline collection of either personal information or de-identified health information. The law also barred any transfer of personal information or de-identified health information about a minor to any other party, even if transferred with parental consent. Third, the law barred any use of personal information or de-identified health information about a minor to recommend any course of conduct with regard to a product or service (including health or safety recall warnings or advice about the safe use of medicine). The law made no reference to activities in Maine and purported to apply nationwide; there was no feasible way to identify and segment Maine minors on the Internet, unless (ironically enough) companies collected and retained more personal information about individuals. Several coalition members, represented by DLA Piper, sued and obtained a consent order that raised serious questions about the law's constitutionality. As a result of the consent order, the Maine legislature repealed the law this spring.

Both Massachusetts' and New Jersey's security breach laws gave state regulators the authority to impose data security regulations. Both states initially proposed technology mandates that required the use of encryption, and only encryption, as a data security solution. The New Jersey regulations went further, mandating a long list of specific information security measures appropriate for medium-sized business. Both these technology-mandate approaches were withdrawn.

Law enforcement-related mandates are an equally serious threat. In particular, several states (including Nevada, Colorado and, last year, Maine) have come very close to imposing IP address data retention mandates on ISPs and other Internet companies. In a less dramatic but similar vein, Minnesota imposes a hard deadline for complying with any law enforcement subpoena from that State. Other states (New Jersey and Wisconsin) have considered rigid, short deadlines for compliance with all law enforcement subpoenas from their states that would create inevitable conflicts with federal and other state law enforcement priorities. In the end, these bills were changed to remove the hard deadline.

Even state breach notice bills, for which state-by-state compliance is in principle workable, typically pose significant compliance problems as introduced. For example,

---

[4] John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (2008), available at http://cyber.law.harvard.edu/pubrelease/isttf/.

[5] http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1351-1400/sb_1361_bill_20100419_amended_sen_v97.html.

[6] Pub. Law c. 230, codified at 10 MRSA c. 1055, § 9551 *et seq.*

Mississippi this year became the 46th State to enact a breach notice law.[7] Despite having 45 other states to follow, the Senate sponsor proposed a series of different requirements that contained several unworkable features that would have:

- required double notice to state residents by both the data owner and the vendor when a vendor suffered a security breach;
- required notice whenever an employee accessed a database containing personal information in good faith for legitimate work purposes that nevertheless exceed the employee's authorization;
- prohibited electronic breach notice by Internet companies to state residents even if their only communications with these state residents were by electronic means, unless the Internet company had obtained E-SIGN compliant consent for electronic notice; and
- required consultation with federal, state *and* local law enforcement whenever a company determined that a breach did not pose a risk to State residents in the event of a breach.

The Attorney General's office strongly supported the Senate approach. Only in a House-Senate conference on the bill were these outlier provisions removed.

C. Potential Solutions Where State Barriers Arise

1. Preemption

Preemption can be an extremely valuable tool in curbing state barriers to innovation. For example, the preemption provision in the CAN-SPAM Act was critical to preserving the viability of non-deceptive commercial email advertising following passage in 2003 of California S.B. 186.[8] That law created $1,000 per email message statutory damage class action liability against advertisers, senders, and list providers for each commercial email message sent to or from California without opt-in consent. Congress passed the CAN-SPAM Act shortly before the effective date of the California law, averting a huge chilling effect on the use of email as a means of advertising and averting a rash of lawsuits under S.B. 186.

Given the very large volume of state legislation and enormous interest among state policymakers in imposing privacy and security regulation on a conflicting, state-by-state basis, when Congress regulates in these areas, it should do so by adopting uniform national standards. While we recognize that some in Congress are reluctant to preclude innovative state approaches to regulation, once an issue ripens to the level that it is addressed in congressional legislation, preemption is necessary to avoid conflicting state and federal standards.

It is important that the Department's report stress that where Congress regulates in a privacy or data security area affecting the Internet or other areas of innovation, Congress do so by establishing a fair, uniform standard, empowering State AGs to enforce that federal standard,

---

[7] Mississippi H.B. 583 available at http://billstatus.ls.state.ms.us/documents/2010/pdf/HB/0500-0599/HB0583SG.pdf.

[8] http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_0151-0200/sb_186_bill_20030924_chaptered.html.

and preempting state law that addresses the same subject matter, while preserving state unfair and deceptive trade practice statutes..

To date, with a few exceptions discussed below, the State Coalition has been successful in opposing state laws that would create inconsistent privacy and data security standards. We are not suggesting that federal legislation is needed in any of the areas discussed in these comments. However, if Congress decides to legislate, it should do so preempting state law.

2. Dormant Commerce Clause/First Amendment:

The Dormant Commerce Clause and First Amendment have served as the other legal bulwarks protecting innovation across state lines. It would be very helpful if the Department's report specifically cited the important limits that the Dormant Commerce Clause places on state regulation of interstate commerce over the Internet and other communications networks. and that the First Amendment places on state restrictions on expression on the Internet by teenagers and adults and on state restrictions on advertising.

For example, a host of decisions have struck down state "harmful to minors laws" that attempted to regulate Internet content.[9] The 2004 UT "spyware contract act" was enjoined on Dormant Commerce grounds.[10] Last year, DLA Piper, counsel to the State Coalition, represented several State Coalition members in a lawsuit that resulted in a consent judgment declaring the Maine teenage marketing law, L.D. 1183[11], discussed above on pp. 2-3, likely unconstitutional on First Amendment grounds (the court did not reach plaintiffs' Dormant Commerce Clause theories).

The Dormant Commerce Clause guards against barriers to interstate or foreign commerce. The Dormant Commerce Clause doctrine flows from a power affirmatively and exclusively granted to the federal government in U.S. Const. Art I., § 8, cl. 3: to regulate interstate commerce. Because the federal power is exclusive, states and localities may not enact laws or impose regulations that impede the free flow of goods and services across state lines.[12] The doctrine prohibits both protectionist laws that discriminate against commerce from other states in favor of the enacting state as well as state regulations that, although facially nondiscriminatory, unduly burden interstate commerce.[13]

States may regulate commerce that occurs solely within their borders, and, to a limited extent, interstate commerce that affects their citizens. However, the Dormant Commerce Clause prohibits state laws or regulations that:

---

[9] *Johnson v. ACLU,* 194 F.3d 1149 (10th Cir. 1999); *PSINET, Inc. v. Chapman,* 362 F.3d 227 (4th Cir. 2004); *American Booksellers Foundation v. Dean*, 342 F.3d 96 (2d Cir. 2003) ("*Dean*"); *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997).

[10] *WhenU v. State of Utah*, (June 22, 2004), transcript available at http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf

[11] Pub. Law c. 230, codified at 10 MRSA c. 1055, § 9551 *et seq.*

[12] *See Lewis v. BT Inv. Managers, Inc.*, 447 U.S. 27, 35 (1980).

[13] *See Kassel v. Cons. Freightways Corp. of Del.*, 450 U.S. 662 (1981).

(1) directly regulate a means of interstate commerce that by its nature demands uniform national treatment[14]; or

(2) have the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction[15];

(3) would risk "inconsistent legislation arising out of the projection of one state['s] regulatory regime into the jurisdiction of another State"[16]; or

(4) regulate interstate commerce only indirectly, but imposes burdens on interstate commerce that are "clearly excessive" in relation to the law's asserted local benefit.[17] A state statute that burdens interstate commerce will be invalidated in this context if the legitimate local purpose "could be promoted as well with a lesser impact on interstate activities."[18]

Most importantly for state Internet regulation, a string of cases addressing state Internet content restrictions has held that where a state imposes age-screening restrictions that apply to out-of-state websites and the websites must apply them to all visitors because they cannot be sure which visitors come from the regulating state, such regulations violate the Dormant Commerce Clause.[19] This line of authority is very significant in the current Internet environment because IP address-based geo-location is inaccurate in a significant number of circumstances. For example, all blackberry users have IP addresses indicating that they are from Canada and all AOL ISP subscribers have IP addresses indicating that they are from Virginia. Thus, websites that do not collect street addresses cannot be sure whether they are dealing with a resident from a state that imposes onerous regulation. Thus, state laws that apply to the Internet and impose restrictions regardless of whether the defendant is aware of the state of residence of its users have the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction.[20]

First Amendment curbs on state regulation of speech over the Internet are typically better understood. The Supreme Court has made clear that speech over the Internet medium deserves the highest level of First Amendment protection.[21] First Amendment case law also makes clear that the government may not, in advancing its compelling interest in protecting children, reduce adults to receiving only expression suitable for children if less restrictive alternatives would be at least as effective in achieving the government's legitimate purposes. *See, e.g., Communications of Cal., Inc. v. FCC,* 492 U.S. 115, 126 (1989).

---

[14] *See, e.g., American Library Ass'n v. Pataki,* 969 F. Supp. 160, 168 (S.D.N.Y. 1997).
[15] *Healy v. Beer Institute*, 491 U.S. 324, 335-40 (1989).
[16] *American Booksellers Foundation v. Dean*, 342 F.3d 96, 104 (2nd Cir. 2003).
[17] *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).
[18] *Id.*
[19] *Johnson v. ACLU,* 194 F.3d 1149, 1161-62 (10th Cir. 1999); *PSINET, Inc. v. Chapman,* 362 F.3d 227 (4th Cir. 2004); *American Booksellers Foundation v. Dean*, 342 F.3d 96, 102 (2d Cir. 2003); *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 177 (S.D.N.Y. 1997).
[20] *Healy v. Beer Institute*, 491 U.S. at 335-40.
[21] *Reno v. ACLU*, 521 U.S. 884 (1997).

The First Amendment provides strong protection for freedom of expression against state content-based or speaker-based restrictions on speech, and guarantees older minors the right to communicate and to receive information. It acts as an important counterweight against privacy laws that would prevent older teenagers from speaking on the Internet without parental consent.

The First Amendment also protects against overbroad or selective restrictions against advertising over the Internet and other communications media. *See, e.g., Greater New Orleans Broadcasting v. F.C.C.*, 527 U.S. 173 (1999); *Verizon Northwest v. Schowalter*, 282 F. Supp. 2d 1187, 1194(W.D. Wa. 2003) (invalidating state opt-in requirement for use of CPNI).

It would be particularly helpful if the Department of Commerce report explained and discussed the importance of these theories to provide guidance to states in avoiding creating barriers to innovation and freedom of expression.

II. Responses to Specific Questions in the NOI on State Privacy Laws)

Our comments now turn to supplying what we hope are helpful answers to the Department's specific questions regarding state privacy laws.

The Department's very thoughtful preamble actually understates the volume of state privacy laws. As mentioned above, almost every state has both data breach and at least several other sectoral privacy laws. California alone has more than 20 such laws[22].

"A. What, if any, hurdles do businesses face in complying with different state laws concerning privacy and data protection?

The largest hurdles typically arise with regard to four types of state laws:

(1) State laws that impose liability in class action lawsuits for statutory damages for non-intentional conduct. These create significant insurance risks and greatly complicate negotiations of arrangements between business entities that touch or secure the data at issue.

(2) State laws that impose hard or soft technology mandates – for example, to implement a specific Internet safety solution, to use encryption, and only encryption, to protect personal data, or an exception for encryption, and only encryption, from breach notification. These distort the market for technology, freeze technology developments, and force some companies to switch to different product or service offerings.

(3) State laws that require a *sui generis* state-specific notice or website configuration, or protocol for handling data.

(4) Widely divergent or incompatible state requirements regulating or imposing liability for the same activity.

[22] For a helpful overview, see the website of the California Office of Privacy Protection, http://www.privacy.ca.gov/privacy_laws.htm.

More generally, simply tracking the huge variety of state regulation is both expensive and burdensome, and for that reason beyond the capacities of small businesses.

"B. Is there harmonization among state laws governing data protection? Please describe any significant differences among the states"

General Data Security Laws: Specifically with regard to data security laws, until 2008, there was very positive harmonization of state laws (requiring use of "reasonable security measures").[23] This changed with the Massachusetts data security regulations and Nevada data security mandate law.[24] The Nevada law is a particularly sharp contrast. It imposes a technology mandate to use encryption, and only encryption, to protect the type of "personal information" that would trigger a breach notice obligation under Nevada law. The law requires encryption at all times that the personal information is transported or stored outside the premises of a business. It also includes a vaguely worded mandate to comply at all times with the Payment Card IndustryData Security Standard for protection of payment data.

By contrast, in Massachusetts, the legislature left room to authorize other data protection technologies beyond encryption, and eventually the regulator who issued the regulations moved to a technology neutral approach. *See* 201 C.M.R. § 17:00. That state's other requirement to have a comprehensive written information security program if companies maintain personal information about Massachusetts residents may not be understood by many state businesses, but it is well-intentioned and technology neutral.

While Massachusetts' data security statute is technology neutral, the original version of the Office of Consumer Affairs and Business Regulation's regulations to implement the law allowed only encryption as a technology protection measure. These rules were repeatedly stayed, then amended last year to allow other technology protection methods. Nonetheless, this spring, a State Representative attempted to add an amendment rider to the State budget that could have had the effect of restoring the encryption mandate.

For its part, the New Jersey Division of Consumer Affairs initially drafted very problematic, highly specific data security standards to implement the state's data security and identity theft statute, P.L. 2005, c. 226. These draft rules, first circulated in 2007, were based upon medium-sized business data security best practices, but not adapted to small or large organization approaches. Those regulations are still under consideration, but the Department of Consumer Affairs withdrew them in 2008 before they took effect, and has not reinstituted them.

Payment Card Data Security Laws: This year, Washington State enacted a much better considered, technology-neutral payment card data security law. The law provides for safe harbors from liability for a breach of payment card data, if a merchant either passed a PCI audit

[23] *See, e.g.,* ARK. CODE ANN. §§ 4-110-104(b), CAL. CIV. CODE § 1798.81.5(b), CT. GEN. STAT. § 42-471, MD. CODE, COM. LAW § 14-3503, ORE. REV. STAT. § 646A.622, R.I. GEN. LAWS § 11-49.2-2(2), TEX. Bus. & COM. CODE § 521.052, and UTAH CODE ANN. § 13-44-202.

[24] *See* MASS. GEN. LAWS CH. 93H.; NEV. REV. STAT. CH. 603A.

within a year of the breach or protects data using encryption (or another comparably effective method based on how encryption was defined in the bill). H.B. 1149, amending REV CODE WASH. CH. 19.255. By contrast, in 2007, Minnesota enacted a different requirement that all merchants delete magnetic stripe and CCV code data within 48 hours or else face strict liability for a data breach involving payment card data. REV. MINN. STAT. § 325E.64. Other proposals have been considered in many states (e.g. CA, TX, IL, WI, CT) and they remain a significant potential barrier to innovation.

Data Destruction Laws: State data destruction laws are somewhat harmonized but not totally so. Some states (at least California and Connecticut) require secure data destruction for any personally *identifiable* information, while others require secure destruction for a smaller subset of data elements that are more sensitive. Imposing a secure data destruction requirement for ordinary name and address information is burdensome and expensive.

Medical Information Laws: More dramatically, the California Medical Information Act (CMIA) at California Civil Code § 56.36, contains a provision that creates huge ($1,000 per act of release) class action liability for breaches of medical data that involve negligence. This provision creates significant liability risk for the promotion of electronic health records, which is a significant American Recovery and Reinvestment Act and Administration priority. As class action lawsuits brought under this provision proliferate, they risk raising insurance costs for electronic medical records.

Security Breach Notification: State security breach notification laws are far more effective than data security mandate laws and can significantly benefit consumers by providing them with information about security breaches that pose some risk to them. Breach notice laws differ from other (more problematic) state laws in that data holders can normally identify individuals who reside in individual states and send them notifications that comport with that state's security breach notification law.

That said, the 46 state security breach notice laws (plus laws in the District of Columbia and Puerto Rico) also contain a fairly wide array of variations in factors that make a difference for compliance (e.g. the event triggering the notification requirement (acquisition, access or acquisition, or access and acquisition), timing of notification, content of notification, regulatory entities that must be notified, when regulator notices must be made, and the content and method of notifying). In particular, it is necessary to draft different notifications for Maryland and Massachusetts, which have unique content requirements for resident notifications.

These variations raise costs and delay notifications without significantly enhancing protection of state residents from identity theft and fraud. While not in themselves a reason for enacting a federal breach notice law, when and if a federal private sector breach notice law is enacted, it should preempt all state notification laws and laws imposing liability for data security breaches.

In addition, a minority of state breach notice laws also contain disincentives to innovation in data security by creating "encryption only" exceptions to breach notice.[25] These exceptions disqualify other technologies that protect personal data from an exception for notifying data subjects and thereby make those technologies less desirable to use in protecting personal information. Encryption may actually make data less safe when keys are stored with the encrypted objects and create significant network security problems because encrypted objects flowing through Internet networks are impossible to screen for viruses and other security threats. In reality, the definitions of personal information in breach notice laws, by requiring that a name be obtained "in combination with" a sensitive data element, also recognize data segregation as providing an exemption from notification. However, this is not commonly understood, and other effective methods, such as access control technologies, do not receive an exception from notification. This sort of "soft" data security regulation distorts the market for security technologies and hinders innovation.

"C. How does complying with multiple states laws affect organizations' business activities and ability to operate online?"

&

"E. What approaches do companies take to comply with privacy laws in multiple states?"

Generally, simply tracking the huge variety of state privacy and security regulation in other states is costly and burdensome, and for that reason beyond the capacities of many small businesses.

Typically, organizations that have the resources to follow the multiplicity of state regulation in this area face a choice. They can segregate and localize data collected from particular states and ask users to confirm their addresses, for example creating variations of their website based upon the response. The compliance alternative is to comply with the most restrictive combination of state standards. For efficiency purposes, organizations almost always choose to comply with the most restrictive state laws. Moreover, there is also some risk that organizations will be found to be negligent in other states if they do not live up to standards required in the more restrictive states.

However, in some cases, where state standards are incompatible in some ways, businesses are forced to expend resources to implement a state-by-state compliance approach – for example, in the breach notice context.

In other cases, businesses decide not to deploy a particular service in a difficult or high risk compliance jurisdiction – for example, a state with *sui generis* data security mandates.

[25] *Compare, e.g*, California Civil Code § 1798.82 (requiring notification of a breach that involves "unencrypted personal information; Del. Code § 12B-101(1) (defining a "breach of a security system" to include the "unauthorized acquisition of unencrypted computerized data . . . .") *with, e.g.,* IND. CODE § 24-4.9-2-5 (technology neutral safe harbor for encrypted data and for data that is "secured by another method that renders that data unreadable or unusable.")

In the case of laws, such as state recording statutes, that reach interactions with websites or consumers in a particular state, they may forego entirely deploying an innovative service that is lawful in most states because of litigation risk in a minority of outlier states that project their law outside of their states.

"D. What types of existing state laws have the greatest impact on companies business models?"

Technology mandates or technology preferences are the most problematic for innovation. These laws prevent or strongly discourage innovation to find better methods for securing and storing data. The Nevada data security encryption mandate law and the strong preferences for encryption in many breach notice laws are prime examples.

Laws that impose class action exposure for statutory damages or multipliers or criminal penalties have a particularly strong chilling effect. Even if conduct is very likely legal, legal uncertainty is usually enough to deter companies from innovating in the area.

Laws that apply outside of the states' borders also have a major impact. The Maine teenage marketing law (now repealed) placed sweeping restrictions on the collection and transfer of personal information about minors without consideration of how the law could logically be enforced just in Maine and without any consideration of its unintended consequences for free expression. The breadth and exposure of this law were so broad that they left in-state and out-of-state businesses little choice but to sue to enjoin the law.

More generally, in an era where for efficiency purposes data may be stored or delivered in many different states, state-specific data security laws are an impediment to innovation. It is many cases unworkable to know where personal data will be stored, and creating varying risks on a state-by-state level introduces an element of risk and legal uncertainty that is a barrier to innovation.

"G. What future directions in state law are anticipated? Does the variety of technology-specific state laws help individual Internet users exercise their rights, or does it create confusion for consumers?"

Based upon our experience following state privacy and security regulation over the past decade, we expect future developments in at least the following areas:

- Regulation of social networking sites
- Smart grid regulation (see the next paragraph)
- Online marketing to teenagers/children

- Mandates to use specific technologies or methods to protect data security (particularly for payment card data)

- Privacy regulation of IP addresses

- Requirements to retain or quickly furnish evidence to law enforcement.

Smart-grid technologies are a new technology development that is at prime risk for inconsistent regulation. Only recently, the California Public Utilities Commission released a proposed decision adopting requirements for smart grid deployment.[26] Noting that there are subtleties and complexities to privacy protections, the Commission stated that further comments and deliberation would be required, which would occur after adoption of the proposed decision. Nonetheless, in its conclusions of law, the Commission provides a preview of the extensive range of privacy protections that it is interested in, by stating that "[i]t is reasonable to determine the current state of privacy actions by asking utilities, as part of their Smart Grid deployment plan, to answer the following questions concerning the data of customers:

a. What data is the utility now collecting?
b. For what purpose is the data being collected?
c. With whom will the utility currently share the data?
d. How long will the utility currently keep the data?
e. What confidence does the utility have that the data will [be] accurate and reliable enough for the purposes for which the data will be used?
f. How does the utility protect the data against loss or misuse?
g. How do individuals have access to the data about themselves? And
h. What audit, oversight and enforcement mechanisms does the utility have in place to ensure that he utility is following their own rules?[27]"

Other than breach notification, which is self-activating, it is far from clear that state-by-state regulation in these areas will help consumers to exercise their rights, as consumers have little awareness of state privacy requirements. For example, in 2006, a new "Shine the Light Law" went into effect in California empowering Californians to obtain a full list of third party entities with whom companies had shared Californians' personal information for marketing purposes. *See* Cal. Civ. Code § 1798.83-.84. Many businesses changed their business practices to conform to this requirement, yet receive almost no requests. Uniform federal standards tend to be more broadly understood and therefore more effective for consumers.

"H. Have technology specific state privacy laws affected online innovation and business development and, if so, how?"

As discussed above in these comments, encryption mandates have affected innovation

[26] Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, Rulemaking 08-12-009, California Public Utilities Commission (May 21, 2010).
[27] *Id.* at 114-115.

and business development. Both hard mandates and soft encryption preferences – for which some encryption vendors have lobbied – have played a key role in making encryption the standard data security solution for businesses. We believe that they have discouraged investment in other solutions.

Similarly, recording statutes have slowed innovation in metrics solutions for online services and have stopped network-based behavioral advertising in its tracks. State two-party consent recording statutes are a huge barrier to innovation in wireless and wireline communications services. Two-party consent is typically impossible to obtain in the Internet context. These laws were typically drafted before the Internet was widely used as a means of communication, and carry criminal penalties and contain exposure at $1,000 per violation in class action lawsuits. However, whether they apply depends upon whether courts will interpret capturing, for example, URL destination information, as intercepting contents. The laws create legal uncertainty, for example, for services that conduct network-level metrics on Internet usage. These laws should be preempted if Congress addresses online privacy legislation.

We are also concerned that as lawsuits under California's CMIA, Civ. Code § 56.36, proliferate, they will raise the insurance costs for electronic medical records solutions.

III. International

Barriers to innovation flowing from non-U.S. privacy and data protection laws are significant. Three technology-related examples are as follows:

Data Transfers: Even using model clauses approved by the European Union, it is both expensive and slow to effectuate compliant data transfers from all the E.U. member states to other parts of the world other than the handful of jurisdictions deemed to provide "adequate protection" or to the U.S. under the U.S.-E.U. Safe Harbor Agreement. Half of E.U. jurisdictions require prior approval of the clauses and some take as long as four months to finish their reviews. Israel, Hong Kong and Mexico will all likely require different contractual provisions to comply with their laws. Even in Europe, there is no one-stop-shop filing option for these agreements, and filing and translation requirements vary widely among E.U. member state jurisdictions. This adds significant cost and delay to cloud computing, global IT help desk support and a wide range of other services that require trans-border data transfers.

Social Networking: The laws of many E.U. jurisdictions require the consent of all individuals in a photograph before a photograph may be posted on a social networking site or photo-sharing site. This has the effect of mandating take down obligations for all such photos posted on public sites. It also complicates employer use of collaborative work social networking applications that permit posting of photographs, since employers must require employees to obtain the prior consent of all individuals in the photo before posting.

Online Advertising Analytics: On their face, European opt-in consent requirements require not only notice, but also the affirmative consent of Internet users. However, entities in the Internet advertising eco-system that do not have a direct relationship with consumers are

unable to obtain consent. They depend upon the website owner, advertiser, or network advertiser to obtain consent. While Data Protection Authorities in E.U. member states have not enforced the opt-in requirement aggressively in this context, this relationship creates significant uncertainty for advertising companies that locate with in the E.U.

Concern About U.S. Government Access to Data Stored in the U.S.: There is also significant concern, particularly among foreign governments and data protection authorities, about allowing their data to be stored in the U.S. because of (unjustified) concerns that the U.S. government will secretly obtain access to that information. This impedes sales of some U.S. technology solutions, including hosting and data center solutions, abroad.

What Models for Protection of Privacy Rights Across Borders Have Proven Effective? The International privacy barriers to innovation are an area where the Department can play a critical role. The Department already has a strong track record of success in this area through its work on the U.S.-E.U. Safe Harbor Agreement, which is the single most helpful international privacy harmonization agreement for businesses achieved to date. Every year, the Safe Harbor saves U.S. and European companies hundreds of millions of dollars in compliance costs. It drives U.S. companies to implement a larger range of fair information practices and is fully enforceable by the Federal Trade Commission.

The Department is a critical representative of business and economic considerations in international data protection *fora*. The U.S. private sector does not have standing to participate effectively in these discussions and while it appreciates the FTC's work in these *fora*, the Commerce Department's presence has been missed.

How might privacy regimes in the U.S. and other jurisdictions across the globe be harmonized? The Department's tireless efforts to nurture the APEC privacy framework are very valuable both to demonstrate the diversity of privacy solutions in the world and to show the effectiveness of a multi-national system where data receiving organizations commit to follow an accountability framework. They show a diversity of solutions for data protection and avoid isolation of the U.S. approach to privacy.

Harmonization of substantive laws appears very unlikely and impractical, although a globally harmonized approach should be the ideal way forward.. It is important to recognize that full harmonization has not occurred even within the E.U. data protection regime. Requirements vary among member states. While the mutual recognition procedure for Binding Corporate Rules applications is a welcome step forward for companies that can afford to undertake that process, only 19 E.U. member states currently work jointly on BCR applications[28], and several EU member state DPAs refuse categorically to recognize them.

Because nations will not jettison their national legal regimes, a gradually expanding mutual recognition model may hold promise in extending the safe harbor approach to other jurisdictions. The best hope for reducing the significant barriers to innovation caused by

[28] These are Austria, Belgium, Bulgaria, the Czech Republic, Cyprus, France, Germany, Ireland, Iceland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovenia, Spain, and the UK.

conflicting international privacy regimes is to work toward cross-border recognition of compliance initiatives, along the lines of the ground-breaking U.S.-E.U. Safe Harbor Agreement.

Like the Safe Harbor Agreement, receiving entities would make enforceable commitments to follow the framework, subject to enforcement if those representations were false. This way, data protection commitments could follow personal data wherever it travelled, preserving the privacy guarantees that data subjects reasonably expect. At the same time, the costs and inefficiencies of the current data transfer model would be avoided and national boundary barriers to cross-border innovation would be reduced significantly.

Respectfully submitted,

_____
Jim Halpert
General Counsel

Adrian Copiz
Counsel
(202) 799-4000