Testimony of

Debbie Matties

Vice President, Privacy

CTIA – The Wireless Association®

on

"Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?"

before the

House Energy & Commerce

Subcommittee on Commerce, Manufacturing, and Trade

July 18, 2013

Chairman Terry, Ranking Member Schakowsky, and other Members of the Subcommittee, thank you for the opportunity to participate in today's hearing on behalf of CTIA – The Wireless Association®. My name is Debbie Matties, and I am the Vice President for Privacy at CTIA. Before joining CTIA, I served as an Attorney Advisor for Consumer Protection to former Federal Trade Commission Chairman Jon Leibowitz.

CTIA, along with AT&T, Comcast, DIRECTV, Time Warner Cable, United States Telecom Association and Verizon, is a founding member of the 21st Century Privacy Coalition (the Coalition). The Coalition was formed to advocate for modernization of U.S. privacy and data security laws to better serve consumer expectations as well as to reflect technological and competitive changes in the communications marketplace.

CTIA commends the subcommittee for exploring whether federal data breach legislation is necessary to protect consumers. Today's patchwork of state and, in certain sectors, federal information security and data breach notification laws is often confusing to businesses and provides uneven protection for consumers. A comprehensive, streamlined federal framework enforced by a single agency would create more certainty for businesses and better protect consumers from the harms associated with data breaches.

The daily cyber-attacks on commercial networks, the increasing prevalence of malware, and ongoing criminal enterprises focused on stealing consumer financial information have resulted in high-profile security breaches that have exposed information belonging to millions of consumers.[1] When such breaches subject consumers to identity theft or other financial harm,

[1] *See* Eric Dash, *Citi Says Many More Customers Had Data Stolen by Hackers*, N.Y. TIMES (June 16, 2011), http://www.nytimes.com/2011/06/16/technology/16citi.html; Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS, Apr. 26, 2011, http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426; Laura Strickler, *Secret Service Investigates Epsilon Data Breach*, CBS NEWS (Apr. 4,

consumers need to be notified so that they can take actions to protect themselves from further harm.

Yet the patchwork of state, and even federal, information security and data breach notification requirements creates inconsistent, sometimes contradictory responses to breaches that do not benefit consumers. For example, some states require breach notifications to occur "without unreasonable delay," whereas other states require specific timeframes for notification. Some states provide an exemption from breach notification for immaterial breaches, whereas other states do not. Most states provide an exemption from breach notification if consumers' information is encrypted, but other states do not.[2]

The absence of a consistent nationwide regime creates an unnecessary distraction for companies that need to (1) stop a breach, (2) evaluate the damage caused by such a breach, (3) correct whatever vulnerability resulted in the breach, (4) work with law enforcement to apprise such officials of the breach, and (5) notify consumers to help mitigate any harm. But these time-sensitive activities are hampered when a company has to sift through 47 different state regimes to determine procedures for breach notification.

Electronic information is rarely, if ever, segmented by state, so a breach invariably impacts consumers in multiple states. Because breaches often transcend state boundaries, which state law should even apply – the state in which the consumer resides, the state in which the breach occurred, or the state in which a vulnerability existed and was exploited – is often

---

2011), http://www.cbsnews.com/8301-31727_162-20050575-10391695.html. *See generally* Stephen Grocer, *Sony, Citi, Lockheed: Big Data Breaches in History*, WALL ST. J. (June 9, 2011), http://blogs.wsj.com/deals/2011/06/09/sony-citi-lockheed-big-data-breaches-in-history.

[2] *Compare* CAL. CIV. CODE § 198.29(a) (providing exception for encrypted data), *and* ARIZ. REV. STAT. ANN. § 44-7501(a) (2007) (West) (same), *with* WYO. STAT. ANN. § 40-12-502 (West 2007) (proving no exception for encrypted data).

unclear. Given the fact that breaches transcend state boundaries, a federal approach to breach notification is appropriate so that all consumers receive the same benefit. Multiple federal regimes undermine consumer protection in the same manner as multiple state regimes. For example, wireless carriers are subject to the Federal Communications Commission's Customer Proprietary Network Information (CPNI) rules to the extent that they are providing a telecommunications service, such as voice service.[3] But wireless carriers are subject to Federal Trade Commission data security enforcement to the extent that they are providing an information service, such as Internet access.

Even more confusingly, location information that can be collected from a consumer's mobile device is subject to the Federal Communications Commission's CPNI rules if "the collection is undertaken at the carrier's direction and that the carrier or its designee has access to or control over that information."[4] But this requirement does not apply if the location information is simply collected by an application not at a carrier's direction or under a carrier's control.[5]

Consumers do not expect the data security rules that apply to location information to differ based upon the entity collecting such information; consumers expect the same rules to apply to the same information. Consumers use a range of functionally equivalent services and applications, often on the same communications platform. These services and applications

[3] *See* 47 U.S.C. § 222 (2008).

[4] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, CC Docket No. 96-115, at ¶ 16 (rel. June 27, 2013).

[5] In addition to uneven federal protection for consumers, federal data security and date breach notification rules to which telecommunication providers are subject do little to protect consumers from identity theft. The CPNI definition leaves out personal information like credit card numbers, but protects non-sensitive information, such as services a subscriber has ordered.

collect the same type of information, and consumers expect that the same information security standards will apply.

Consumers would greatly benefit from a unified, streamlined federal data security and breach notification regime that applies equally to all entities. Such a regime would make consumers more confident in the security of their online information, which would give them greater trust in their use of the Internet.

CTIA agrees with the Obama Administration's recommendation that "because existing Federal laws treat similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers."[6] CTIA also supports the Administration's recommendation that a federal framework "provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions."[7] That should apply not only to telecommunications carriers currently subject to the CPNI requirements, but also to cable and satellite operators subject to data breach requirements in Sections 631 and 338 of the Communications Act of 1934, respectively.[8] Under such a framework, CTIA supports a narrowing of the common carrier exemption to enable the Federal Trade Commission (FTC) to enforce information security and data breach notification requirements.

---

[6] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 39 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[7] *Id*. at 36.

[8] *See* 47 U.S.C. § 551, § 338(i).

In addition, a unified, streamlined federal data security and breach notification regime should only be enforced by the Federal Trade Commission; it should not include a private right of action. The data security and breach notification regimes of at least 15 states include a private right of action. Some trial lawyers have sought to leverage these requirements against companies that are the subject of a data breach to obtain monetary awards that are not tied to consumer injury and that often do not benefit consumers.[9] Even when no wrongdoing has occurred, companies often bear great expense going to trial under these laws.[10] A law enforcement regime will result in better compensation for consumers who have been injured.

Thank you again for the opportunity to present CTIA's views at today's hearing. CTIA fully supports a unified, streamlined federal data security and breach notification regime that is enforced by the FTC and applies to all entities. Consumers expect that their information will be afforded the same degree of protection, regardless of the entity collecting the information and of the State in which the consumer resides. A federal framework would give consumers greater confidence that the safety of their online information will be afforded the same degree of care regardless of where they live, where a breach occurs, or where hackers may be trying to access their information. Congress should enact a new law to better reflect consumer expectations.

---

[9] *See, e.g., Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *1-2 (S.D.N.Y. June 25, 2010) (collecting dozens of class actions where plaintiffs "claim to have suffered little more than an increased risk of future harm from the loss (whether by accident or theft) of their personal information"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) ("Here, no evidence suggests that the data has been—or will ever be—misused.").

[10] *See* Sasha Romanosky *et al., Empirical Analysis of Data Breach Litigation, Research Paper No. 2012-29, in* Temple Univ. Beasley Sch. of Law Legal Studies Research Paper Series (Gregory Mandel & Shyam Nair, eds., 2012), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461 (finding that defendants settle 49% of data breach lawsuits without allegations of actual harm and theorizing that defendants "may be rationally choosing to settle to avoid further litigation costs, publicity, or business distraction").