

# EYE ON PRIVACY

FEBRUARY 2015

## WELCOME

In this issue of *Eye on Privacy*, we provide the first in a series of articles discussing the importance of privacy and data security considerations in the transactional context, examine the latest developments in Target's holiday data breach litigation, discuss an amendment to California's data breach notification law and the State Attorney General's 2014 Data Breach Report, and consider some recent guidance on the Internet of Things and device fingerprinting from EU regulators. In addition, we discuss enforcement trends for the Better Business Bureau's Advertising Accountability Program, the effect of COPPA on mobile apps, and final rules from the Consumer Financial Protection Bureau regarding the annual consumer privacy notices required to be distributed by financial institutions. Rounding out this packed issue is an examination of the FCC's dive into privacy and data security enforcement and a discussion of President Obama's recent executive order calling for greater security in consumer financial transactions.

As always, please feel free to email us at [PrivacyAlerts@wsgr.com](mailto:PrivacyAlerts@wsgr.com) if there are any topics you would like to see us cover in future issues.



*Lydia Parnes*

**Lydia Parnes**  
Partner, Washington, D.C.  
[lparnes@wsgr.com](mailto:lparnes@wsgr.com)



*Michael Rubin*

**Michael Rubin**  
Partner, San Francisco  
[mrubin@wsgr.com](mailto:mrubin@wsgr.com)

## PRIVACY AND DATA SECURITY IN TRANSACTIONS: WHAT'S THE DEAL?



**Matthew Staples**  
Associate, Seattle  
[mstaples@wsgr.com](mailto:mstaples@wsgr.com)



**Jonathan Adams**  
Associate, San Francisco  
[jadams@wsgr.com](mailto:jadams@wsgr.com)

*This article is the first in a series of articles in Eye on Privacy that will discuss the importance of privacy and data security considerations in the transactional context.*

In 2014, data privacy and data security continued to capture headlines and boardroom attention, as the EU "right to be forgotten" ruling,<sup>1</sup> the Sony cyberattack, new laws and lawsuits, and investor pressure on executives and boards regarding cybersecurity issues<sup>2</sup> provided continued

worries for legal departments, executives, and directors.<sup>3</sup> The ongoing coverage of these incidents has caused many legal departments, executive teams, and boards of

*Continued on page 2...*

### IN THIS ISSUE

**Privacy and Data Security in Transactions: What's the Deal? ...Pages 1-3**

**Consumer and Financial Institution Class Actions Survive Motions to Dismiss in Target Data Breach Litigation .....Pages 4-7**

**California Amends Data Breach Notification Law and State Attorney General's Data Breach Report May Lead to More Changes .....Pages 7-10**

**EU Data Protection Regulators Issue Guidance on the Internet of Things and Device Fingerprinting .....Pages 10-11**

**Better Business Bureau Keeps Promise of Vigorous Enforcement of Online Interest-Based Advertising Accountability Program ..... Pages 12-13**

**COPPA Looms Large for Mobile Apps ..... Page 14**

**Consumer Financial Protection Bureau Issues Final Rule Regarding Online Annual Consumer Privacy Notices ..... Pages 15-16**

**FCC Dives into Privacy and Data Security Enforcement .....Pages 17-18**

**Recent Executive Order to Push for Security of Consumer Financial Transactions, Identity Theft Remediation .....Pages 19-20**

<sup>1</sup> Case C 131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (E.C.R. May 13, 2014), available at [http://curia.europa.eu/juris/document/document\\_print.jsf?doclang=EN&text&pageIndex=0&part=1&mode=DOC&docId=152065&occ=first&dir&cid=437838](http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&pageIndex=0&part=1&mode=DOC&docId=152065&occ=first&dir&cid=437838).

<sup>2</sup> For example, Institutional Shareholder Services, a prominent proxy advisor, suggested the removal in early 2014 of seven of Target Corporation's board members in light of the data breach suffered by the company in late 2013. See Paul Ziobro and Joann S. Lublin, "ISS's View on Target Directors is a Signal on Cybersecurity," *Wall Street Journal*, available at <http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278> (updated May 28, 2014).

<sup>3</sup> According to a Grant Thornton 2014 Corporate General Counsel Survey, nearly 60 percent of in-house counsel consider privacy risks to be one of their top three concerns.

directors to become more familiar with data privacy and security risks. Many businesses are taking steps to reduce their risk exposure by reviewing and enhancing their privacy and data security programs, ensuring that they maintain appropriate cyber insurance, and working with service providers, vendors, customers, and employees to minimize the likelihood of becoming the next target of a cyberattack or class action litigation.

A critical but sometimes overlooked component of improving a company's privacy and data security risk profile is the appropriate handling of privacy and data security in the context of corporate transactions. A failure to appropriately contemplate and address privacy and data security risks in a merger, acquisition, divestiture, investment, securities offering, joint venture, strategic alliance, or other similar transaction can dramatically increase enterprise-level risk.

In the past, parties to corporate transactions often viewed privacy or data security as of only minor importance. In today's environment, however, acquirors, investors, and underwriters must conduct due diligence and engage in risk management with regard to data privacy and security issues in corporate transactions in order to avoid significant risks, to price the transaction appropriately, and to account for key practical issues (e.g., legal compliance measures, such as obtaining the consent of consumers or business counterparties to use and exploit data, that may be difficult to achieve). When a potential joint venture partner or acquisition or investment target has failed to appropriately handle data privacy or security matters, or where an acquiror, investor, or underwriter does not invest sufficiently in

conducting due diligence or mitigating identified risks appropriately, undesirable or even disastrous results could follow.

Failure to appropriately evaluate data privacy and security issues in a merger or acquisition could, for instance, result in an acquiror: (i) obtaining data that cannot be used or exploited in anticipated manners post-acquisition; (ii) acquiring compromised electronic assets or data systems; (iii) inheriting, or creating a basis for, privacy- or data security-related class actions or regulatory investigations or fines;<sup>4</sup> (iv) experiencing significant damage to reputation or losses in enterprise value or brand

---

## **A critical component of improving a company's privacy and data security risk profile is the appropriate handling of privacy and data security in corporate transactions**

---

equity—not only with regard to the acquisition or investment target, but in many cases, also its own—following the transaction; or (v) determining not to consummate an agreed-upon transaction due to potential costs or risks, or integration difficulties, identified late in the diligence process. Investors and underwriters in financings and securities offerings, respectively, could find the company in which they are investing, or whose securities they

are underwriting, suffering many of these consequences. Indemnification or other remedies may be available for certain of these circumstances, but difficulties may arise in obtaining indemnification, and indemnification may be subject to caps or other limitations that prevent the claimant from being made whole for its losses.

Through conducting due diligence, parties may discover risks relating to inadequate data security programs and procedures, undisclosed data breaches, government investigations, non-compliance with data protection legal obligations, privacy-related litigation, or other similar matters relating to data processing or transfer. Attorneys focused on privacy and data security matters can take steps to ensure that these risks are evaluated, disclosed, remediated, and addressed appropriately, such as by: (i) reviewing the target company's or issuer's policies, practices, and obligations arising under applicable law or by contract; (ii) assessing potential liabilities that may result from deficient privacy or data security practices; (iii) drafting and negotiating appropriate representations, warranties, and covenants;<sup>5</sup> and (iv) working with business and technical subject-matter experts on integration matters.

Parties to a proposed transaction must also ensure that relevant privacy and data security representations and warranties, risk factors, and similar disclosures are drafted, structured, and negotiated to allocate risk and costs appropriately. In the mergers and acquisitions context, and in many investment scenarios, acquirors or buyers should in most instances draft strong privacy and data security representations regarding the business at issue; conversely, sellers should

---

<sup>4</sup> Regulatory authorities are monitoring merger and acquisition activity and seeking to ensure that parties to corporate transactions appropriately safeguard the privacy of consumers. For example, following the announcement of Facebook, Inc.'s acquisition of WhatsApp Inc., the Director of the Bureau of Consumer Protection at the Federal Trade Commission sent both Facebook and WhatsApp a letter reminding them of their privacy obligations to consumers. See Letter from Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc., available at [http://www.ftc.gov/system/files/documents/public\\_statements/297701/140410facebookwhatappltr.pdf](http://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf).

<sup>5</sup> The structure of a corporate transaction may affect the rights of the acquiror with regard to data, and may result in additional risks being borne by the acquiror. For instance, in mergers or stock purchases, an acquiror may be assuming the target company's past liabilities for data privacy and security compliance issues, including regulatory investigations and litigation. At the same time, certain concerns regarding whether data may be "transferred" are less relevant in reverse triangular mergers or stock purchases in which the target company continues operations than in other transaction structures such as asset purchases and forward mergers. In conducting due diligence into a target entity, acquiror's counsel should keep in mind the structure of the corporate transaction to appropriately evaluate the target company's risks and to consider restrictions upon data transfer appropriately.

*Continued on page 3...*

seek to minimize their representations and warranties regarding their data practices, and should describe any failures of those representations and warranties to be accurate

---

## **Parties to a proposed transaction must ensure that relevant privacy and data security representations and warranties, risk factors, and similar disclosures are drafted, structured, and negotiated to allocate risk and costs appropriately**

---

in the disclosure schedules to the acquisition agreement. In public securities offerings, issuers and underwriters should attempt to minimize their respective risks in the underwriting agreement but work cooperatively to cause the registration statement to convey appropriate disclosures to the public.

Data privacy- and security-related integration concerns in many corporate transactions merit specific mention. In many cases, privacy policies must be revised or harmonized, registrations (such as with the Department of Commerce regarding the EU/U.S. and Swiss/U.S. Safe Harbors, or with data protection authorities in European states) must be updated, and privacy and data security must be accounted for in transferring employee and user data. With many transactions structured with simultaneous execution and closing, and many others contemplating abbreviated pre-closing periods, companies often must not only plan

but also begin to execute post-signing, pre-closing matters (including closing conditions and other pre-closing covenants) before transaction documents are even executed. Where these covenants or closing conditions involve data privacy or security matters, they may require an acquired entity to amend certain agreements, modify privacy policies, obtain consumer or user consents to data transfers, and make other significant undertakings.

For companies that seek investment or that may be acquired or pursue a public securities offering in the future, paying attention to privacy and data security is critical, particularly when a company is involved in a regulated sector (such as health care or payments), has international operations, or engages in significant uses of consumer data. For these companies, incorporating privacy-by-design<sup>6</sup> into product development and contractual arrangements may reduce the burden on the company in a corporate transaction, result in fewer obligations and risks in connection with the transaction, and contribute to obtaining its desired consideration and other commercial terms in the transaction. If a company develops an understandable, appropriate approach to data privacy and security before entering into (or negotiating) a corporate transaction, the company can: (i) be more confident that its representations, warranties, and disclosures are accurate, thereby decreasing the likelihood of post-closing indemnification claims; (ii) avoid needing to take significant operational and technical remediation measures in the context of the transaction or during pre-transaction planning, which can place significant stress on a company's management and technical personnel; and (iii) permit a prospective acquirer or investor to have greater confidence in the company's compliance approach.

Public companies must evaluate the level of disclosure they provide surrounding their data privacy and security practices in various contexts, including: (i) in connection with a material acquisition, determining whether an acquired business or acquired assets will require additional disclosures in the company's securities filings; (ii) ensuring that risk factors in its annual and quarterly filings reflect the company's privacy- and data security-related risks, particularly where user or consumer data is a critical source of value to the company; and (iii) in connection with an initial public offering, considering how to disclose data privacy- and security-related risks, and related policies and procedures, in risk factors and other applicable portions of the initial registration statement. Conducting these evaluations and preparing appropriate disclosures can reduce the risk of SEC inquiry into data privacy- and security-related practices and reduce the risk of liability for misstatements and omissions in securities filings.

---

## **Conducting evaluations and preparing appropriate disclosures can reduce the risk of SEC inquiry into data privacy- and security-related practices**

---

*In future issues, Eye on Privacy will examine the ways in which privacy and data security affect corporate transactions, and how companies can protect themselves, their brand, and their users and customers as they grow.*

---

<sup>6</sup> Privacy by design means, in essence, accounting for privacy and data security considerations at every stage in the design and development of a product or service. For additional information, please see the treatment of the subject in the Federal Trade Commission's report entitled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. For additional information, see Ann Cavoukian, *Privacy by Design*, available at <https://www.ipc.on.ca/images/resources/privacybydesign.pdf>.

# CONSUMER AND FINANCIAL INSTITUTION CLASS ACTIONS SURVIVE MOTIONS TO DISMISS IN TARGET DATA BREACH LITIGATION



**Maggie Lassack**

Of Counsel, Washington, D.C.  
mlassack@wsgr.com



**Wendell Bartnick**

Associate, Austin  
wbartnick@wsgr.com



**Joseph Molosky**

Associate, Washington, D.C.  
jmolosky@wsgr.com

Cases brought by consumer plaintiffs following data breaches often have been dismissed because courts concluded that the plaintiffs failed to adequately allege sufficient harm to satisfy either Article III standing requirements or the required elements of an underlying cause of action, such as negligence or a violation of state consumer protection law. But on December 18, 2014, a federal court in Minnesota ruled that the consumer plaintiffs suing Target Corp. in the wake of its 2013 holiday-season data breach had alleged sufficient injury to satisfy both Article III standing requirements and the necessary elements of their underlying causes of action.<sup>1</sup> As a result, the court denied the majority of Target's motion to dismiss the case.

That ruling was the second blow the court issued to Target late last year: Just two weeks earlier, on December 2, 2014, the court issued an order that largely denied Target's motion to dismiss the case brought against it by the financial institutions that issued payment cards to the consumers whose information was compromised in the breach.<sup>2</sup> The court is one of the first to rule that such financial institutions adequately pleaded that a retailer owed them a duty of care to provide reasonable security for consumers' payment card information.

This article describes both rulings and discusses their potential implications not only for Target, but for any company suffering a data breach.

## Background

In December 2013, Target announced that during a period of more than three weeks during the busy holiday shopping season, hackers stole the payment card information or other personal information of more than 110 million Target customers. Numerous lawsuits followed, and all federal lawsuits were consolidated into a multidistrict litigation pending before Judge Paul A. Magnuson of the U.S. District Court for the District of Minnesota, where Target is headquartered. The Target multidistrict litigation includes class actions brought by consumers whose information was compromised during the breach and by the financial institutions who issued payment cards to those consumers. Those financial institutions allege that retailers and thousands of banks nationwide could suffer fraud-related losses in excess of \$18 billion due to the Target breach, which is one of the largest in U.S. history. Target moved to dismiss the case brought by the financial institutions on September 2, 2014, and one month later, on October 1, 2014, Target moved to dismiss the case brought by the consumers.

## Target's Motion to Dismiss Financial Institutions' Case

The financial institutions allege that Target: (1) committed negligence by failing to provide reasonable and adequate security for its customers' personal and financial information; (2) violated the Minnesota Plastic Security Card Act (MPSCA) by retaining certain payment card information from sales transactions for more than 48 hours; and (3) committed a negligent misrepresentation by representing that it had adequate data security measures and failing to inform the

financial institutions of material weaknesses in those measures.<sup>3</sup>

Target moved to dismiss the financial institutions' complaint in its entirety, arguing primarily that the financial institutions' negligence and negligent misrepresentation claims failed because Target did not owe the financial institutions a duty of care under Minnesota law. Target argued that it did not have a duty of care to protect the financial institutions from harm caused by third-party hackers unless it had a "special relationship" with the financial institutions, which Target contended it did not.

The court largely denied Target's motion, upholding the financial institutions' negligence and MPSCA claims, and dismissing their negligent misrepresentation claim without prejudice. The court ruled that the financial institutions adequately pleaded that Target had a duty of care under general negligence law because they alleged that Target's own conduct created a foreseeable risk of the harm that occurred in connection with the breach, and that the financial institutions were foreseeable victims of that harm. The court reasoned that a plaintiff is required to plead the existence of a "special relationship" only when alleging that action by someone other than the defendant created the foreseeable risk of harm to the plaintiff.

The court found that the financial institutions "undoubtedly" alleged a MPSCA violation by alleging that Target retained data in violation of the MPSCA, and that the hackers were able to access some of that data, which worsened the consequences of the breach.<sup>4</sup> The court also found that the existence of the MPSCA bolstered its ruling that the financial institutions adequately pleaded a duty of care under general negligence law because the statute reflects "Minnesota's policy of punishing companies that do not secure consumers' credit- and debit-card information."<sup>5</sup>

<sup>1</sup> *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (D. Minn. Dec. 18, 2014) (hereinafter Consumer Order).

<sup>2</sup> *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (D. Minn. Dec. 2, 2014) (hereinafter Financial Institution Order).

<sup>3</sup> The Financial Institutions allege that Target made these representations through its privacy policy, its agreement to comply with payment card operating regulations and the Payment Card Industry Data Security Standards (PCI DSS), and other unspecified actions and representations.

<sup>4</sup> Financial Institution Order at 15.

<sup>5</sup> Financial Institution Order at 7.

*Continued on page 5...*

Although the court found that the financial institutions adequately pleaded a duty of care with respect to their negligent misrepresentation claim, it nonetheless dismissed the claim without prejudice because the financial institutions failed to plead reliance on Target's alleged omissions about material weaknesses in its data security measures, and reliance is a required element of a negligent misrepresentation claim under Minnesota law.<sup>6</sup>

**Target's Motion to Dismiss Consumers' Case**

The 121-page complaint brought by more than 100 named consumer plaintiffs alleges several detailed claims, including violations of state consumer protection laws, violations of state data breach notification laws, negligence, breach of implied contract, and unjust enrichment.<sup>7</sup> Target filed a motion to dismiss, which tested the plausibility of these claims. To overcome a motion to dismiss, a complaint must contain enough facts to suggest that discovery will reveal evidence of a legally cognizable claim. Therefore, the bar to overcome a motion to dismiss is much lower than a summary judgment motion—the claims need only be plausible.

The court granted Target's motion in part and denied it in part, upholding the majority of the consumers' claims. The court permitted most of the consumer protection, data-breach notification, and negligence claims to proceed. The court also permitted the implied breach of contract and unjust enrichment claims to proceed.

*Standing.* To sue in federal court, plaintiffs must have "standing." Many plaintiffs have been unable to meet the threshold requirement of standing in data breach-related class action litigation because they have been unable to allege concrete, particularized damages fairly traceable to the breach. The Supreme Court recently explained in *Clapper v. Amnesty International USA* that "[t]o establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."<sup>8</sup> Some commentators saw this recent holding by the Supreme Court as defendant-friendly, particularly in data breach cases. Indeed, some recent cases bore that out.<sup>9</sup>

Target relied on *Clapper* when it argued that the consumers did not have standing because they did not allege that the expenses they incurred were unreimbursed or that their alleged loss of access to account funds was not due to their own decisions to close their accounts. The court disagreed with Target's arguments stating that they "gloss over" the actual allegations made and impose too high a standard for a motion to dismiss.<sup>10</sup> The court found that the consumers had "plausibly allege[d] that they suffered injuries that [we]re 'fairly traceable' to Target's conduct,"<sup>11</sup> by alleging "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."<sup>12</sup> The court held that the consumers sufficiently pleaded Article III standing and noted that Target could move for summary judgment on this issue should

discovery not support the consumers' injury allegations.<sup>13</sup> Interestingly, the court concluded without discussion that the consumers' alleged injuries were fairly traceable to the breach and seemingly postponed the analysis to the summary judgment stage.

*Claims under State Consumer Protection Laws.* Most states have consumer protection laws barring deceptive and unfair trade practices. The consumers alleged that Target violated these laws by having inadequate data security and by failing to provide notice of the data breach more quickly to the consumers. Target argued that the consumers failed to allege economic injury, as required under some state laws, but the court concluded that the Consumers adequately alleged unreimbursed late fees, new card fees, and other charges. Target also argued that some state consumer protection laws apply to omissions only when there is a duty to disclose, and that the consumers failed to adequately plead that Target had such a duty. Stating that neither party provided the court any legal precedent to help make its determination, the court concluded that the consumers' allegations that Target knew the data was sensitive and at risk from an ongoing breach was sufficiently plausible to establish that Target had a duty to disclose.<sup>14</sup> Therefore, most of the consumers' claims under state consumer protection laws remain in the case.<sup>15</sup>

*Claims under Data Breach Notice Statutes.* The consumers also alleged that Target violated state data breach notice statutes by

<sup>6</sup> The court provided the financial institutions with 30 days to amend their negligent misrepresentation claim.

<sup>7</sup> The consumers alleged seven claims in all, including claims based on contract and bailment theories that the court dismissed.

<sup>8</sup> *Clapper v. Amnesty Int'l USA*, 568 U.S. \_\_\_\_, 133 S. Ct. 1138, 1147 (2013). We discussed *Clapper* in a previous Eye on Privacy article located at <https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/May2013/index.html#4>.

<sup>9</sup> See, e.g., *Lewert, et al. v. P.F. Chang's China Bistro, Inc.*, No. 1:14-cv-4787, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014) (on appeal); *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118 (S.D. Ohio Feb. 10, 2014); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013); see also, *In re: Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 12-347-JEB-MDL 2360, 2014 WL 1858458 (D.D.C. May 9, 2014); *Strautins v. Trustwave Holdings, Inc.*, No. 12-C-09115, 2014 WL 960816 (N.D. Ill. 2014); *Polanco v. Omnicell, Inc.*, No. 13-1417-NLH-KMW, 2013 WL 6823265 (D.N.J. Dec. 26, 2013). But see, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 972 (S.D. Cal. 2014).

<sup>10</sup> Consumer Order at 4.

<sup>11</sup> Consumer Order at 4 (quoting *Allen v. Wright*, 468 U.S. 737, 753 (1984), abrogated on other grounds, *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377 (2014)).

<sup>12</sup> Consumer Order at 4.

<sup>13</sup> Consumer Order at 4.

<sup>14</sup> Consumer Order at 12.

<sup>15</sup> The court dismissed the consumers' claims under three state consumer protection laws because the laws did not confer a private right of action, and the court held that the Consumers may not maintain a class action as to their claims under the consumer protection laws in nine states. Consumer Order at 18.

Continued on page 6...

not providing breach notice quickly enough, and that they were harmed because they “would not have shopped” at Target and had their information stolen had they known about the breach. Target argued that courts have rejected the “would not have shopped” theory unless the security was an intrinsic part of the purchased product or service (e.g., data security software, password-protected subscription service, or storage of credit card information for ongoing use).<sup>16</sup> The court found that the consumers’ “would not have shopped” theory of damages could prove true through discovery, and permitted the claims to proceed.<sup>17</sup>

**Negligence Claim.** The consumers alleged that Target was negligent by providing inadequate data security and failing to disclose the breach in a timely manner. Target again argued that the negligence claim must fail because the consumers failed to allege any cognizable damages. Just as with the other arguments, while Target may successfully defend against this claim after discovery, the court determined that the consumers’ allegations were plausible.<sup>18</sup>

**Breach of Implied Contract Claim.** The consumers alleged that they formed an implied contract with Target where Target agreed to safeguard personal and financial information as part of processing credit and debit card transactions. Consumer plaintiffs in prior data breach cases have had mixed success when facing motions to dismiss claims for implied breach of contract.<sup>19</sup> The court here decided to allow the breach of implied contract claim, finding that the consumers plausibly alleged the existence of

an implied contract, as well as its terms.

**Unjust Enrichment Claim.** The consumers also alleged unjust enrichment under both an “overcharge” theory and the previously described “would not have shopped” theory. The “overcharge” theory asserts that consumers paid for data security as part of the price of the products they purchased. The court found the “overcharge theory” to be meritless because all consumers paid the same price regardless of payment method, and consumers who pay cash have no data security risk. The court accepted the unjust enrichment claim based on the “would not have shopped” theory. The court found that a reasonable jury could find that Target was unjustly enriched if the Consumers can prove that: (1) they shopped at Target after Target knew or should have known about the breach; and (2) they would not have shopped there if they had known about the breach.<sup>20</sup>

Target now faces the costly prospect of conducting discovery, challenging class status certification, and preparing to challenge the consumers’ claims in a motion for summary judgment.

## Implications

To date, issuing banks have brought relatively few cases against retailers in connection with data breaches. The Target court is one of the first to rule that issuing bank plaintiffs adequately alleged a duty of care, as required to bring a negligence claim against a retailer in connection with a data breach.<sup>21</sup> Courts in several prior cases have dismissed negligence claims brought by issuing banks, finding that the relevant state’s economic loss doctrine

prohibited the claims,<sup>22</sup> or that the issuing banks failed to adequately plead a duty of care under the relevant state law.<sup>23</sup>

The court’s denial of Target’s motion to dismiss the financial institutions’ case does not indicate that the case will ultimately be successful. But the ruling is significant because issuing bank plaintiffs can more easily establish actual economic injury in connection with a data breach than consumer

---

**The Target court is one of the first to rule that issuing bank plaintiffs adequately alleged duty of care**

---

plaintiffs. Although states apply different standards to negligence claims for purely economic injury, the court’s denial of Target’s motion to dismiss the financial institutions’ negligence claim likely will encourage issuing banks to bring similar cases following future data breaches. And in states like Minnesota, where the economic loss doctrine does not necessarily bar recovery for economic injuries alleged by issuing banks, those cases may survive motions to dismiss, increasing their value significantly.

The court’s decision in the consumers’ class action could also have far-reaching implications. The court’s decision to allow most of the consumers’ claims does not

<sup>16</sup> See *In re Adobe Systems, Inc. Privacy Litig.*, 2014 U.S. Dist. LEXIS 124126, at \*67 (N.D. Cal. Sept. 4, 2014) (software and online services that were security dependent); *In re LinkedIn User Privacy Litig.*, 2014 U.S. Dist. LEXIS 42696, at \*3-4 (N.D. Cal. Mar. 28, 2014) (password-protected subscription service); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 972 (S.D. Cal. 2014) (storing credit card number for future purchases).

<sup>17</sup> The consumers conceded or the court dismissed claims under twelve state breach notification laws because the laws did not confer a private right of action. Consumer Order at 27-28.

<sup>18</sup> The court dismissed the negligence claims in five states due to those states’ economic loss rule. Consumer Order at 39.

<sup>19</sup> See, e.g., *In re Zappos.com, Inc.*, No. 3:12cf325, 2013 WL 4830497, at \*3 (D. Nev. Sept. 9, 2013) (finding that statements about data security measures do not create an implied contract); *Krottnner v. Starbucks, Corp.*, 406 F. App’x 129 (9th Cir. 2010) (holding that no implied contract was created when plaintiffs did not allege they saw or read documents relied upon for the contract). *But see, e.g., Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (2011) (holding that a purchase made with a payment card may create an implied contract to maintain reasonable security of that data in a pre-*Clapper* case); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531-32 (N.D. Ill. 2011) (same).

<sup>20</sup> Consumer Order at 44-45.

<sup>21</sup> The court in *Sovereign Bank v. BJ’s Wholesale Club, Inc.*, 395 F. Supp. 2d 183, 193-95 (M.D. Pa. 2005) held that issuing bank plaintiffs adequately alleged the existence of a duty in connection with their negligence claim brought against BJ’s under Pennsylvania law following BJ’s 2004 data breach. The negligence claim was later dismissed under Pennsylvania’s economic loss doctrine. See *Sovereign Bank v. BJ’s Wholesale Club, Inc.*, 533 F.3d 162, 175-78 (3d Cir. 2008).

<sup>22</sup> See *Sovereign Bank*, 533 F.3d at 175-78 (applying Pennsylvania law); *Banknorth, N.A. v. BJ’s Wholesale Club, Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006) (applying Maine law at summary judgment); *Cumis Ins. Soc’y, Inc. v. BJ’s Wholesale Club, Inc.*, 918 N.E.2d 36 (Mass. 2009).

<sup>23</sup> See *BancFirst v. Dixie Rests., Inc.*, No. CIV-11-174-L, 2012 WL 12879 (W.D. Okla. Jan. 4, 2012) (dismissing negligence claim under Oklahoma law for failure to plead a “special relationship”); see also *Digital Fed. Credit Union v. Hannaford Bros. Co.*, No. BCD-CV-10-4, 2012 WL 1521479 (Me. B.C.D. Mar. 14, 2012) (declining to recognize duty of care at summary judgment stage of proceedings).

Continued on page 7...

indicate that those claims are valid. In fact, the court repeatedly stated that Target's arguments may succeed on a motion for summary judgment. However, the court's decision significantly increases the value of the consumers' case. Unless Target settles the case, it likely will incur large expenses in connection with discovery and litigating class-certification issues before it has the opportunity to reassert its arguments in a summary judgment motion.<sup>24</sup>

This outcome suggests that the Target consumers' complaint will serve as a model for future class actions brought by consumer plaintiffs following data breaches. The Target consumers successfully alleged injury, where

many other consumer data breach plaintiffs failed. Unlike in *Barnes & Noble*,<sup>25</sup> *Galaria*,<sup>26</sup> and other cases where the courts rejected claims of damages from increased risk of fraud and the expenses plaintiffs incurred to prevent it, the Target consumers alleged damages that resonated with the court in the form of restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees.

The consumer and financial institution plaintiffs' survival of Target's motions to dismiss increases the likelihood that Target, and other companies who suffer data breaches in the future, will be required to defend on their merits negligence claims

based on alleged inadequate data security. Therefore, it will be increasingly important for companies to ensure that they have reasonable and appropriate data security measures in place. The Target cases could also be the tipping point signaling that the potential costs of data breach-related lawsuits are so high that an increasing number of businesses should actively work to decrease the risk of facing these costs, such as by regularly assessing data security risks, implementing and maintaining additional safeguards, and assessing their need for cyber liability insurance and the appropriate levels of coverage.

<sup>24</sup> This could increase the amount that Target will spend in connection with the breach, which Target estimated at \$248 million in November 2014. See Press Release, Target Corp., "Target Reports Third Quarter 2014 Earnings," November 19, 2014, available at <http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1991049>.

<sup>25</sup> *In re Barnes & Noble Pin Pad Litig.*, 12-CV-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).

<sup>26</sup> *Galaria v. Nationwide Mut. Ins. Co.*, Case No. 2:13-cv-118 (S.D. Ohio Feb. 10, 2014).

## CALIFORNIA AMENDS DATA BREACH NOTIFICATION LAW AND STATE ATTORNEY GENERAL'S DATA BREACH REPORT MAY LEAD TO MORE CHANGES



**Wendell Bartnick**  
Associate, Austin  
wbartnick@wsgr.com



**Joseph Molosky**  
Associate, Washington, D.C.  
jmolosky@wsgr.com

Prompted by data breaches affecting large retailers in the United States, the California legislature recently passed Assembly Bill 1710 (A.B. 1710) to update the state's breach notification law to require breached entities to provide free credit monitoring services to

affected individuals following certain types of data breaches. This change, effective January 1, 2015, was recommended by the California Attorney General's Office in its 2013 Data Breach Report. The Attorney General's Office recently published its 2014 Data Breach Report, and its recommendations provide insight into the office's enforcement priorities. The recommendations may also find their way into California law.

### California Breach Notification Statute

California has been a leader in providing privacy-related protections to its citizens. Like most states, California enacted a breach notification statute which requires businesses

that own or license computerized data to provide notice to affected individuals in the event of a breach involving their personal information.<sup>1</sup> The statute requires that the notice to affected individuals contain certain content<sup>2</sup> and be sent "in the most expedient time possible and without unreasonable delay."<sup>3</sup> A business may also need to notify the California Attorney General if the breach affects more than 500 California residents.<sup>4</sup>

The state has regularly expanded its breach notification statute to cover additional types of information and to require notification of the Attorney General in some instances.<sup>5</sup> The latest statutory update may obligate some

<sup>1</sup> Personal information" is defined as "an individual's first name or first initial and last name" plus any of the following: social security number; driver's license number or state ID card number; "account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account"; medical information; or health insurance information. After recent amendments, personal information also includes "a user name or email address, in combination with a password or security question and answer that would permit access to an online account." Cal. Civ. Code § 1798.82(h); Eye on Privacy, "California Extends Security Breach Notification Requirements to Online Account Credentials," November 2013, available at <https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Nov2013/index.html#3>.

<sup>2</sup> Cal. Civ. Code § 1798.82(d).

<sup>3</sup> Cal. Civ. Code § 1798.82(a); Eye on Privacy, "Breach Notification: Timing Is Everything," November 2013, available at <https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Nov2013/index.html#4>.

<sup>4</sup> Cal. Civ. Code § 1798.82(f).

<sup>5</sup> Eye on Privacy, *supra* note 1; WSGR Alert, "New California Security Breach Notification Requirements to Take Effect January 1," September 7, 2011, available at <https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-security-breach-notification.htm>; WSGR Alert, "California Expands the Information Subject to Security Breach Notification Requirements," December 28, 2007, available at [https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/clientalert\\_securitybreach.htm](https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/clientalert_securitybreach.htm)

Continued on page 8...

# CALIFORNIA AMENDS DATA BREACH NOTIFICATION LAW . . . (continued from page 7)

businesses victimized by a data breach to provide free credit monitoring services to affected individuals for one year. The revised statute states:

If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed [social security number, driver's license number, or California identification card number].<sup>6</sup>

The practical effect of this statutory update is somewhat unclear, because most businesses affected by a breach already provide one year of free mitigation services, and the ambiguity in the statutory language may mean the requirement only applies in a very narrow set of circumstances.

*The Amendment May Require What Most Businesses Already Do.* Many businesses already voluntarily provide free identity theft prevention and mitigation services (e.g., credit monitoring) to affected individuals after a breach. According to the California Attorney General's 2014 Data Breach Report, over 70 percent of the entities that experienced a breach involving the social security numbers or the driver's license numbers of California residents voluntarily offered to provide access to a free mitigation service for at least one year.<sup>7</sup>

*The Amendment Seems to Apply to Narrow Circumstances.* The new statutory language may apply only in narrow circumstances. The new requirement seems to apply only to an entity that both: (1) is statutorily required to notify individuals of a breach; and (2) is the source of the breach. Under the California statute, only the data owner or licensor has

the obligation to notify individuals of a breach. Entities that maintain data on behalf of other entities, typically vendors and services providers, do not have the obligation to notify individuals.<sup>8</sup> Therefore, the new requirement would seem to apply only to data owners and licensors and not to vendors and service providers.

The second factor for determining whether an entity must provide free mitigation services is whether the entity was the "source of the breach." The statute does not define the term "source of the breach," but the use of this language may significantly narrow the applicability of the requirement. Commonly, businesses use vendors and service providers to maintain their data. When such data is breached at a vendor or while being transmitted by a vendor, the vendor may be the "source of the breach." In the instance of the Target breach, an HVAC vendor did not maintain or have access to any of the breached data, but malware affecting the vendor also infected Target's computer network leading to Target's data breach. In that case, the vendor may have been the "source of the breach." In both of these examples, the statute may not require the provision of free mitigation services because the vendor, possibly the source of the breach, is not the entity required to provide notice to affected individuals.

The new statutory requirement to provide a free mitigation service may apply only when the breached entity is holding the breached data, it is the owner or licensor of the data, and its vendors and service providers were not the source of the breach. Thus, the new requirement may only apply to a narrow set of circumstances.

*The Amendment is Grammatically Ambiguous as to What is Required.* There is a grammatical argument that the statute requires an entity to provide free mitigation services for one year only after the entity has already voluntarily chosen to provide such services. Under this interpretation, businesses

are not statutorily required to provide access to the mitigation services. Some commentators, however, have taken the position that the statute requires an entity to provide the free mitigation services if it is statutorily required to notify individuals of a breach and it is the source of the breach.

The statute's lack of clarity likely creates a situation where businesses that experience a data breach involving social security numbers, driver's license numbers, or state identification numbers will not know if they must provide free mitigation services. Businesses that otherwise may not provide mitigation services in the event of a breach will need to perform a risk evaluation based on the circumstances of the breach to determine whether to provide these services at no cost to affected individuals, which add time and costs to breach responses.

*Other Related Statutory Updates.* California also updated other data-related protections through A.B. 1710. California already required owners and licensors of personal information to implement and maintain reasonable security procedures and practices.<sup>9</sup> The legislation expanded this security requirement to also cover businesses that *maintain* personal information. The statute defines "maintain" to cover situations where the business does not own or license the personal information. This change could extend the data security requirement to vendors and service providers that handle personal information for their customers.

A.B. 1710 also updated the California statute applicable to a person or businesses' use of social security numbers. The original statute prohibited individuals and businesses from publicly posting or displaying social security numbers and imposed certain security requirements when requesting or sending a social security number over the Internet.<sup>10</sup> The updated statute also prohibits the sale of social security numbers, except when the release of the social security number is part of "a larger transaction and is necessary to

<sup>6</sup> California Assembly Bill No. 1710 (2014).

<sup>7</sup> California Department of Justice, California Data Breach Report 2014 14 (October 2014), available at [https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data\\_breach\\_rpt.pdf](https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf) (statistics calculated based on breaches reported to the California Attorney General during the years 2012 and 2013) (hereinafter 2014 Data Breach Report).

<sup>8</sup> Cal. Civ. Code § 1798.82(b).

<sup>9</sup> Cal. Civ. Code § 1798.81.5(b).

<sup>10</sup> Cal. Civ. Code § 1798.85.

Continued on page 9...



identify the individual in order to accomplish a legitimate business purpose.”<sup>11</sup> Under the updated statute, businesses likely may continue to sell data assets as part of a merger or other business change and process transactions that require the disclosure of social security numbers. However, the sale of social security numbers with no other purpose, such as in the instance of a hacker selling the payload of a data breach, likely would violate the statute.

The original proposed A.B. 1710 was narrowed considerably in the legislature after strong opposition from retailers and other consumer-facing businesses.<sup>12</sup> It remains to be seen whether the bulk of the original bill will be resubmitted to the legislature following reports of more breaches at large retailers.

## 2014 California Data Breach Report

The California Attorney General’s Office released its latest Data Breach Report in October 2014.<sup>13</sup> Like the previous report, the 2014 report provides analysis of data breaches reported to the Attorney General’s Office and proposes industry and legislative recommendations. The legislature codified into law two of the five recommendations proposed in the 2013 report.<sup>14</sup> Therefore, the new report could be seen as a roadmap to future statutory requirements.

The data breach report publishes findings the California Attorney General considers important, such as the common causes of breaches. The report indicates that the number of reported breaches increased from the prior year by over 25 percent and the number of records breached increased by over 35 percent (excluding the Target and Living Social breaches that were extreme outliers). Due to the large breaches victimizing Target and Living Social, the retail sector accounted

for 84 percent of the total records breached. The common causes of the data breaches reported to the California Attorney General are consistent with global data breach statistics. A slight majority of the breaches involved computer intrusions from outside criminals. The loss or theft of devices accounted for just over 25 percent of the breaches, and unintentional errors accounted for 18 percent of the breaches.

The California Attorney General made twelve recommendations in the report, which are grouped by intended audience and listed below. The recommendations likely indicate the Attorney General’s current enforcement priorities.

- Retail Sector
  - Chip-enable point-of-sale terminals. More than 80 countries use chip-enabled payment cards, which are considered more secure than the magnetic stripes used on payment cards in the United States. Empirical evidence indicates that chip-enabled cards greatly decrease fraud in face-to-face card transactions.<sup>15</sup>
  - Encrypt payment card data end-to-end during transactions.
  - Tokenize payment card data during transactions.
  - Respond and provide affected individuals with notice promptly after a data breach. The report recommends that retailers should have a tested incident response plan and a trained response team in place to improve the quality and timeliness of breach responses.
  - Improve notice following breaches of payment card data. The report

suggests that retailers providing breach notice should provide more detail about the breach, such as the time period and specific locations of the breach, tell affected individuals about ways they can protect themselves from fraudulent use of breached information, and post a link to the notice on the company’s Internet home page for at least 30 days.

- Retailers and Financial Institutions
  - Protect debit cardholders following data breaches. Currently, when data breaches affect debit card accounts, the accounts can have funds stolen and not replaced until after a bank investigation. Moreover, customers are more likely to be liable for stolen funds depending on how quickly the customer notifies the bank of the issue. The report recommends that retailers provide notice to affected individuals explaining that cancelling affected debit cards may be the best way to mitigate harm.
- Healthcare Sector
  - Encrypt medical information on portable devices. Breaches involving healthcare-related organizations are usually more harmful, because they commonly involve social security numbers and medical information. Hardware encryption could prevent or mitigate many of the breaches because most breaches involve lost or stolen devices.
- All Industries
  - Conduct annual data security risk assessments and update privacy and security practices based on findings.

<sup>11</sup> Cal. Civ. Code § 1798.85(a)(6).

<sup>12</sup> Eye on Privacy, “Proposed California Law Would Impose Data Breach Liability on Retailers and Create More Stringent Data Security Requirements for Businesses,” July 2014, *available at* <https://www.wsg.com/publications/PDFSearch/eye-on-privacy/Jul2014/index.html>.

<sup>13</sup> 2014 Data Breach Report, *supra* note 7.

<sup>14</sup> California Department of Justice, Data Breach Report 2012 (2012), *available at* [http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data\\_breach\\_rpt.pdf](http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf) (making the following recommendations: (1) encrypt personal information in transit; (2) review and update security controls; (3) improve breach notice readability; (4) offer mitigation products to victims of data breaches involving social security numbers or driver’s license numbers (codified into law); and (5) legislation to include online account credentials as personal information in breach notification statute (codified into law)).

<sup>15</sup> See Douglas King, “Chip-and-Pin: Success and Challenges in Reducing Fraud,” Retail Payments Risk Forum, January 2012, *available at* [https://www.frbatlanta.org/-/media/Documents/rprf/rprf\\_pubs/120111wp.pdf](https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/120111wp.pdf).

*Continued on page 10...*

- Encrypt portable devices and personal information during transit.
- Improve readability of any breach notices. The report suggests that breach notices are written at a college level, instead of the average adult reading level.
- California Legislature
  - Amend the breach notification statute to: (1) strengthen the substitute notice provision that commonly is used in large breaches; (2) clarify the roles and responsibilities of data owners and data maintainers in the event of a breach; and (3) require a final breach report to the California Attorney General.
  - Collect funds to help small businesses upgrade point-of-sale systems.

## Conclusion

California updated its breach notification law in a way that could require the provision of free mitigation services to data breach-affected individuals. However, the statutory language and the current business practices of organizations already providing these free services when they are involved in breaches may mean that the updated statute may not

make much practical difference to individuals affected by breaches.

The 2014 Data Breach Report demonstrates the California Attorney General's concerns related to the data breaches involving retailers and other industry sectors. These concerns are areas the Attorney General will likely continue to monitor closely for possible investigations, and the associated recommendations could ultimately be codified into law by the California legislature. Therefore, businesses may benefit by reviewing the recommendations in the report and considering how they may implement them.

## EU DATA PROTECTION REGULATORS ISSUE GUIDANCE ON THE INTERNET OF THINGS AND DEVICE FINGERPRINTING



**Cédric Burton**  
Of Counsel, Brussels  
cburton@wsgr.com



**Laura De Boel**  
Associate, Brussels  
ldeboel@wsgr.com

The European data protection regulators, the Article 29 Working Party (WP29), recently issued two guidance papers which clarify the data protection legal framework applicable to the Internet of Things (IoT) and to the use of device fingerprinting. Both opinions underline WP29's current focus on data-driven innovations. This article highlights the key takeaways from these two opinions.

### WP29 Opinion 8/2014 on the Internet of Things<sup>1</sup>

The WP29 opinion specifically focuses on three IoT developments: (1) wearable computing; (2) the quantified self; and (3) home automation. According to WP29, the processing of data in these contexts can trigger the application of both the Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC.

- The Data Protection Directive applies to the extent that the smart devices connected in the IoT collect, use, and disclose data about identified or identifiable individuals (i.e., "personal data"). What constitutes personal data is interpreted very broadly under EU data protection law.<sup>2</sup>

- The e-Privacy Directive and in particular the so-called EU cookies rule<sup>3</sup>, which requires prior consent for the storing of or gaining access to information in the terminal device of a user, applies when data is accessed or stored on a user's smart device.

WP29 considers that, even if the data is collected by an organization located outside the European Union, EU data protection law will apply if the connected device is located in the EU, or even if only the smartphone or tablet on which software or apps were installed to transmit the data is located in the EU.

After a detailed discussion of the risks related to the IoT, WP29 clarifies what the EU data protection requirements mean in practice for

<sup>1</sup> See the WP29's Opinion 8/2014 on the Recent Developments on the Internet of Things of September 16, 2014 (WP 223), available at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf).

<sup>2</sup> Even if anonymization techniques are applied to the data collected through smart devices, the data are likely to remain personal data. In its Opinion 5/2014 on anonymization [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf), the WP29 set a high threshold for considering data to be fully anonymized: according to the WP29, even a remote risk of re-identification is sufficient to consider data to be "personal data" under the EU Data Protection Directive. For more information, see the July 2014 issue of Eye on Privacy, available at <https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Jul2014/index.html>.

<sup>3</sup> Article 5(3) of the EU e-Privacy Directive.

*Continued on page 11...*

the IoT using various cases studies. Below are some of the main takeaways:

- The roles of the different IoT stakeholders (e.g., manufacturers of smart devices, third-party application developers, social platforms, IoT platforms) should be clearly defined and their responsibilities clearly allocated. WP29 emphasizes the need to determine which party acts as the “data controller” and which as the “data processor.” WP29 gives specific recommendations to the various stakeholders involved in the IoT ecosystem.
- WP29 emphasizes the need for users of smart devices to remain *in control*. WP29 sees a risk that users are not made aware of the data collection in the IoT or lose control over the subsequent use of their data. According to the WP29, providing user control includes:
  - Obtaining users’ freely given, specific, and informed consent to the processing of their personal data (unless another legal basis can be relied on)
  - Enabling users to switch their data to another IoT service provider if they wish to do so (i.e., “right to data portability”)
  - Allowing users to disable the “smart” feature of their device and thus to stop the collection of data while still being able to use the device as the original, unconnected version
  - Offering users granular choices about the categories of data that is collected, the time, and frequency at which data is captured, etc.

- Protecting users against data security breaches and notifying them in case of a security breach
- WP29 recommends performing a Privacy Impact Assessment before launching a new application in the IoT.
- IoT stakeholders should delete the raw data collected from the smart device after having extracted all data necessary to provide users with the smart service.
- To prevent location tracking, WP29 considers that manufacturers of smart devices should limit device fingerprinting by disabling wireless interfaces when they are not used, or by using random identifiers to prevent a persistent identifier from being used to track location.

### WP29 Opinion 9/2014 on Device Fingerprinting<sup>4</sup>

According to WP29, device fingerprinting is a technique which consists of combining various information elements to uniquely identify a device or application. This opinion uses the term in a broad sense, meaning that it comprises any set of information that can be used to single out, link, or infer a user, user agent, or device over time. This includes but is not limited to data derived from: (a) the configuration of a user agent/device; or (b) data exposed by the use of network communications protocols.<sup>5</sup>

In its opinion, WP29 confirms that device fingerprinting is subject to the consent requirement of Article 5(3) of the EU e-Privacy Directive. Although this provision is often referred to as the “cookie rule,” it generally applies to the storing of or gaining access to information in a user’s terminal device via any technique, and is not limited to cookies. Thus, if device fingerprinting relies on the storage

of or access to information stored in the user’s terminal device, it is subject to the prior consent requirements of Article 5(3).

As an example, WP29 states that device fingerprinting to enhance user authentication (i.e., to link an account to a particular device) requires the user’s prior consent. Exceptions to the prior consent requirement will only apply in limited cases where device fingerprinting is necessary for technical reasons, for instance if it is necessary for the normal functioning of a network or to optimize content layout (by accessing the screen size).

WP29 does not clarify how consent to device fingerprinting should be obtained in practice (e.g., whether implied consent is necessary or if a more affirmative action such as an explicit opt-in is required). It remains to be seen how the market will react to this opinion and whether it will implement WP29 guidance. In any event, the practical issues that were raised in the cookie consent debate will most likely apply to device fingerprinting. More information on cookie consent practices can be found at <https://www.wsgr.com/wsgr/Display.aspx?SectionName=publications/PDFSearch/wsgralert-cookie-consent.htm>.<sup>6</sup>

### Conclusion

One of the underlying messages of WP29 in both opinions summarized above is that individuals should remain *in control* over the data that is collected, processed, and disseminated about them. Although the WP29 opinions are not legally binding, they are often followed by EU privacy regulators when applying data protection law. For EU privacy regulators, the level of user control is therefore likely to be an important criterion in the evaluation of new data technologies, such as smart devices, that are launched on the EU market.

<sup>4</sup> See Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, adopted on November 25, 2014 (WP 224), available at [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf).

<sup>5</sup> According to WP29, this can include: (a) CSS information; (b) JavaScript objects (e.g., document, window, screen, navigator, date, and language); (c) HTTP header information (e.g., the number of bits of information in the User Agent string, HTTP header ordering, HTTP header variation by request type); (d) clock information (e.g., clock skew and clock error); (e) TCP stack variation; (f) installed fonts; (g) installed plugin information (e.g., configuration and version information); (h) the use of internal Application Programming Interfaces (API) exposed by the user agent/device; or (i) the use of external APIs of Web services the user agent/device is communicating with.

<sup>6</sup> WSGR Alert, “European Data Protection Regulators Issue Further Guidance on How to Obtain Cookie Consent,” October 24, 2013, available at <https://www.wsgr.com/publications/PDFSearch/wsgralert-cookie-consent.pdf>.

# BETTER BUSINESS BUREAU KEEPS PROMISE OF VIGOROUS ENFORCEMENT OF ONLINE INTEREST-BASED ADVERTISING ACCOUNTABILITY PROGRAM



**Tonia Klausner**  
Partner, New York  
tklausner@wsgr.com



**Lydia Parnes**  
Partner, Washington, D.C.  
lparnes@wsgr.com

Online interest-based advertising, sometimes called behavioral advertising, is big business. Advertisers—and the technology companies that make this business possible—use information collected from a particular computer or device, over time and across others' websites, to predict preferences and target and display advertising that is most likely to interest the user.

With encouragement from the Federal Trade Commission,<sup>1</sup> online advertising industry organizations adopted a set of "Self-Regulatory Principles for Online Behavioral Advertising<sup>2</sup> (OBA Principles)," which apply to members of those organizations: the ad networks, advertising agencies, service providers, and web publishers that engage in or facilitate the collection of online user data across websites for purposes of interest-based advertising. The Better Business Bureau (BBB) enforces the OBA Principles through its Online Interest-Based Advertising Accountability Program (Accountability Program). Recent action by the BBB reflects its commitment to vigorously enforce the OBA Principles.

The cross-industry self-regulatory program is based on seven OBA Principles developed by the Digital Advertising Alliance, the Networking Advertising Initiative, the Direct Marketing Association, the Interactive Advertising Bureau, the Better Business Bureau, the American Association of Advertising Agencies, and the Association of National Agencies, and first released in July 2009. The hallmarks of the principles are transparency and consumer choice, to provide consumers with notice about what information is being collected about them for purposes of serving interest-based ads, and to allow consumers more control over whether advertisers can collect and use this information for these same purposes.

On October 14, 2013, the Accountability Program issued its first ever compliance warning<sup>3</sup>—its first formal industry advisory on compliance with the OBA Principles. In it, the BBB made clear that a "first-party," that is a web content publisher, is responsible for providing "enhanced notice" of "third-party" data collection on their sites for OBA, through "clear, meaningful, and prominent" links (i.e., transparency) on all web pages where third parties collect user data in order to serve targeted advertising. These "enhanced notice" links provide information about the collection of consumer data by third parties, and allow consumers to opt out (i.e., consumer control). The October 14, 2013, compliance warning focused on resolving confusion among first parties (i.e., website publishers or operators) about their

responsibilities for providing "enhanced notice" when they allow third parties to collect data for interest-based advertising. The compliance warning reported that, although most web publishers complied with most of the OBA Principles, a large minority of web publishers were not providing the required "enhanced notice" links.

This compliance warning was followed in November 20, 2013, by three cases concerning websites that were not in compliance with any of the first-party transparency and control requirements.<sup>4</sup> In these three cases, the Accountability Program set out the compliance issues it had found on each website and provided compliance recommendations that each website publisher implemented to bring its website into full compliance. Taken together, the October 14, 2013, compliance warning and the three November 2013 cases provided detailed explanations of first parties' obligations under the Accountability Program's principles. In January 2014 and starting with high traffic publishers, the Accountability Program began a comprehensive review of websites to ensure first-party compliance. (A second compliance warning<sup>5</sup> was issued in August 2014 clarifying that the principles are applicable irrespective of the technology used to collect data and serve advertisements.) It was determined that while many websites were compliant with the principles, some popular sites were still not entirely compliant. True to its promise of "vigorous enforcement," the Accountability Program brought

<sup>1</sup> FTC Report, *Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.

<sup>2</sup> Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), available at <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>. See also WSGR Alert, "New Principles for the Collection of Data Online Released," November 17, 2011, available at <https://www.wsgr.com/publications/PDFSearch/wsgralert-online-advertising-data-collection.pdf>.

<sup>3</sup> Online Interest-Based Advertising Accountability Program, Compliance Warning, "Responsibilities of First Parties for Notice of Third-Party Data Collection for Online Behavioral Advertising on Their Websites," October 14, 2013, available at <http://www.bbb.org/us/Storage/113/Documents/First-Party-Compliance-Warning-20131008.pdf>.

<sup>4</sup> See *In re* BMW of North America, LLC, No. 27-2013 (Nov. 18, 2013), available at <http://www.ascreviews.org/wp-content/uploads/2013/11/Online-Interest-Based-Advertising-Accountability-Program-Formal-Review-27.2013.pdf>; *In re* Scottrade, Inc., No. 28-2013 (November 18, 2013), available at <http://www.ascreviews.org/wp-content/uploads/2013/11/Online-Interest-Based-Advertising-Accountability-Program-Formal-Review-28.2013.pdf>; *In re* Volkswagen of America, Inc., No. 29-2103 (November 18, 2013), available at <http://www.ascreviews.org/wp-content/uploads/2013/11/Online-Interest-Based-Advertising-Accountability-Program-Formal-Review-29.2013.pdf>. Because Volkswagen had already taken steps to come into compliance before the Accountability Program's inquiry letter, the case was closed via an administrative disposition.

<sup>5</sup> Online Interest-Based Advertising Accountability Program, Compliance Warning, "The Digital Advertising Alliance's Cross-Industry Self-Regulatory Principles are Enforceable Irrespective of the Identification Technology Used," August 21, 2014, available at <http://www.ascreviews.org/wp-content/uploads/2014/08/Alternative-Identifiers-Compliance-Warning.pdf>.

*Continued on page 13...*

enforcement actions against five first-parties found to be non-compliant with the “enhanced notice” requirements: Best Buy, Answers Corp. (Answers.com), BuzzFeed, Go.com, and Yelp. Decisions in all five cases were issued October 28, 2014.<sup>6</sup> These actions were the first time the Accountability Program has moved to enforce a compliance warning.

In response to the Accountability Program’s recent actions, all five companies have agreed to revise their websites in order to comply with the “enhanced notice” transparency and consumer control requirements. In these decisions, the Accountability Program referred to “enhanced notice” as the “most innovative of the Transparency Principle’s requirements. Beyond merely alerting users that *some* third-party data collection is occurring, the enhanced notice link puts consumers one click from communication about OBA precisely when they may be curious about why they received

the ad they are looking at or what information is being collected on the web page they are visiting.” The BBB made clear that it is the

---

## The Accountability Program has vowed to continue to enforce the OBA Principles, and it clearly expects cooperation and voluntary compliance

---

obligation of first-parties to provide “enhanced notice” not just in a privacy policy, but on every page whether a third-party is collecting data for use in OBA. The BBB further clarified that this obligation is in addition to first-parties’ obligation to provide

“enhanced notice” in or around interest-based ads. The decisions state that the Accountability Program seeks to “empower...users to learn and make informed decisions about their online privacy.”


Through its recent enforcement efforts, the Accountability Program is highlighting the “enhanced notice” principle, which enables both transparency and consumer choice. According to Genie Barton, vice-president and director of the Accountability Program, some web publishers are still unaware of the “enhanced notice” links requirement, despite industry efforts to publicize them.<sup>7</sup> The Accountability Program has vowed to continue to enforce the OBA Principles, and it clearly expects the type of cooperation and voluntary compliance it received from the companies it recently challenged. In fact, the Accountability Program referred one company, Sun Trust Bank, to the U.S. Consumer Financial Protection Bureau for refusing to participate in its self-regulatory process.<sup>8</sup>

---

<sup>6</sup> Accountability Program Decisions can be found at <http://www.ascreviews.org/accountability-program-decisions/>.

<sup>7</sup> See Wendy Davis, “BBB’s Online Privacy Watchdog Faults 5 Web Publishers,” Online Media Daily, October 29, 2014, 5:08 PM, <http://www.mediapost.com/publications/article/237232/bbbs-online-privacy-watchdog-faults-5-web-publish.html>.

<sup>8</sup> See Online Interest-Based Advertising Accountability Program, Press Release, “SunTrust Bank Referred to the CFPB for Refusal to Participate in Self-Regulation,” May 8, 2014, available at <http://www.ascreviews.org/2014/05/suntrust-bank-referred-to-the-cfpb-for-refusal-to-participate-in-self-regulation/>.



Wilson Sonsini Goodrich & Rosati has a global network of experienced privacy attorneys with whom we have worked extensively. We can assist you with privacy issues in any country, interfacing with local counsel and coordinating the project on your behalf.

## Tip

Are you covered? Cyberliability insurance may help cover costs not covered by general policies when responding to data security incidents.

# COPPA LOOMS LARGE FOR MOBILE APPS



**Tracy Shapiro**  
Of Counsel, San Francisco  
tshapiro@wsgr.com



**Sonal Mittal**  
Associate, San Francisco  
smittal@wsgr.com

The Children's Online Privacy Protection Act (COPPA) prohibits companies from collecting personal information from children under the age of 13 without first providing notice to parents and obtaining their verifiable consent. The Federal Trade Commission's (FTC) recent settlements with Yelp and TinyCo serve as a reminder to mobile app developers that the failure to consider COPPA when developing and testing mobile apps can have serious consequences.

## Yelp

In 2008, Yelp launched a mobile app companion to its popular reviewing website, which requires users to register for a Yelp account in order to rate, post reviews, and "check in" at businesses. In 2009, Yelp added

---

**Settlements with Yelp and TinyCo serve as a reminder to mobile app developers that the failure to consider COPPA can have serious consequences**

---

the ability to register for a Yelp account directly to its mobile app. As part of the registration process for both the website and the mobile app, users were required to provide a date of birth. According to the FTC's complaint, while this information helped Yelp screen out children under the age of 13 on its website, the company failed to correctly implement the age screen on its mobile app. Although Yelp hired a third party to perform a

privacy review of the Yelp app a year after its launch, the third-party test results erroneously noted that the iOS application prohibited registrations from users under the age of 13. Yelp did not otherwise test the age-restriction aspect of the registration feature of the iOS version of the Yelp app, and never tested it in the Android version. Consequently, for four years, registrants of the mobile app who indicated they were under the age of 13 were nonetheless allowed to proceed and to create full Yelp accounts. Once the accounts were created, Yelp collected a multitude of personal information from users, including names, email addresses, precise geolocation data, mobile device IDs, and information about what the users posted on Yelp.

In its complaint, the FTC contended that because Yelp collected information from users who self-declared that they were under the age of 13, the company had "actual knowledge" that it was collecting information from children despite that its privacy policy clearly stated that "[Yelp] is not directed to children under 13." As such, Yelp's collection of personal information was subject to COPPA. Under the terms of settlement with the FTC, Yelp must pay \$450,000 in civil penalties and delete the information it collected from children under the age of 13.

## TinyCo

TinyCo offers free mobile apps, including "Tiny Pets," "Tiny Zoo," "Tiny Monsters," "Tiny Village," and "Mermaid Resort." The FTC alleged that the apps' features, including themes that appeal to children, brightly colored animated characters, and simple language, demonstrate that the apps were directed at children under the age of 13 and were thus subject to COPPA. According to the FTC's complaint, many of TinyCo's apps included an optional feature that collected email addresses from users, and some of the apps offered in-game currency in exchange for a user's email address. Because TinyCo collected the information from users without parental notice and consent, the FTC alleged that TinyCo's practices violated COPPA. Like Yelp, TinyCo settled with the FTC. TinyCo

must pay \$300,000 in civil penalties and delete the information it collected from children under the age of 13.

## Implications

The TinyCo case reminds developers of mobile apps for kids that there are special requirements for data collected from such apps. The Yelp case stands as a further reminder that even apps made for general audiences need to add COPPA compliance to

---

**Companies should weigh the business needs for collecting date of birth information against the risk of inadvertently collecting personal information from children in violation of COPPA**

---

their product development checklists, especially where birth dates are collected. Yelp reflects the perils of incomplete product testing as well as the general risks of collecting date of birth information from users. Companies should weigh the business needs for collecting date of birth information against the risk of inadvertently collecting personal information from children in violation of COPPA.

Beyond the hundreds of thousands of dollars in fines they will have to pay to the FTC, both companies will have to go through the onerous process of deleting all data collected in violation of COPPA as well as producing COPPA compliance reports to the FTC. Companies should keep these high costs in mind throughout the development process and ensure their products are COPPA-compliant from the outset.

# CONSUMER FINANCIAL PROTECTION BUREAU ISSUES FINAL RULE REGARDING ONLINE ANNUAL CONSUMER PRIVACY NOTICES



**Jonathan Adams**

Associate, San Francisco  
jadams@wsgr.com

The Consumer Financial Protection Bureau (CFPB) recently adopted the Privacy Notice Rule, a final rule that permits the financial institutions it regulates the option to post annual consumer privacy notices online, rather than mailing paper copies to customers, under certain conditions<sup>1</sup>.

The Privacy Notice Rule is the latest instance of regulatory relief provided to financial institutions by the CFPB. The new rule, which follows on the heels of other streamlining rulemakings by the CFPB, aims to reduce unnecessary or unduly burdensome regulatory requirements in the financial sector: the CFPB estimates that, as a result of the rule, financial institutions' compliance expenses will decrease by approximately \$17 million dollars annually.<sup>2</sup>

In addition to this significant, recurring reduction in compliance expenses for financial institutions, the CFPB anticipates that the rule will benefit consumers by providing constant online access to privacy policies presented in an understandable form. The CFPB also hopes the new rule will benefit consumers by providing incentives for financial institutions to avoid or limit the sharing of consumers' nonpublic personal information.

The Privacy Notice Rule applies only to certain depository institutions, such as commercial and savings banks, and to non-depository entities subject to the jurisdiction

of the CFPB, such as mortgage bankers, loan servicers, payday lenders, debt collectors, and remittance transfer providers. The rule does not apply to institutions that are subject to the privacy jurisdiction of the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), or the Federal Trade Commission (FTC) (save for certain motor vehicle dealers that are subject to FTC jurisdiction).

The CFPB consulted and coordinated with these other federal regulators and with state insurance authorities in developing the alternative method of delivering the annual privacy notices, as required by the Gramm-Leach-Bliley Act (GLBA),<sup>3</sup> to ensure harmonization among the agencies' rules, to the extent possible.<sup>4</sup>

## Overview of the Privacy Notice Rule

As of October 28, 2014, a financial institution that is regulated by the CFPB is permitted to post annual privacy notices online, rather than by mailing paper copies to customers, if the institution satisfies the following conditions:

- The financial institution does not share its customers' nonpublic personal information with nonaffiliated third parties in a manner that triggers opt-out rights under GLBA
- The financial institution does not include in its annual privacy notice information about certain consumer opt-out rights under Section 603 of the Fair Credit Reporting Act (FCRA)

- The financial institution's annual privacy notice is not the only notice provided to satisfy the requirements of the affiliate marketing provisions of the FCRA<sup>5</sup>
- The information the financial institution includes in the privacy notice has not changed since the customer received the previous notice
- The financial institution uses the model form provided in GLBA's implementing Regulation P<sup>6</sup>

A financial institution that avails itself of this alternative method of delivering annual privacy notices must also comply with several other provisions aimed at ensuring that customers are aware of the online annual privacy notice. Financial institutions providing online privacy notices online must:

- Continuously post the annual privacy notice in a clear and conspicuous manner on a page of its website, without requiring a login or similar steps or agreement to any conditions to access the notice<sup>7</sup>
- Mail a printed copy of its annual notice to any customer who requests such a notice by telephone, within ten days of the request
- Insert a clear and conspicuous statement at least once per year on an account statement, coupon book, or a notice or disclosure the institution issues under any provision of law. The statement must inform customers that the annual privacy notice is available on the

<sup>1</sup> Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P), 79 Fed. Reg. 64057 (October 28, 2014).

<sup>2</sup> 79 Fed. Reg. 64057, 64077.

<sup>3</sup> 15 U.S.C. § 6801 et seq.

<sup>4</sup> 15 U.S.C. § 6804(a)(2).

<sup>5</sup> 15 U.S.C. § 1681s-3 and 12 C.F.R. part 1022, subpart C.

<sup>6</sup> See 12 C.F.R. 1016.

<sup>7</sup> The Privacy Notice Rule preamble explains that the CFPB will not consider occasional or unavoidable website interruptions to violate the requirement for continuous posting. 79 Fed. Reg. 64072.

*Continued on page 16...*

financial institution's website, the institution will mail the notice to customers who request it by calling a specific telephone number and the notice has not changed

A financial institution that has changed its privacy practices or that engages in information-sharing activities for which consumers have a right to opt out must continue to deliver annual privacy notices using the permissible delivery methods predating the Privacy Notice Rule.

### **The Final Privacy Notice Rule, or More to Come from Congress?**

The CFPB characterized the final rule as a win-win for consumers and financial institutions, with consumers receiving 24/7-access to privacy policies, educating them about the various types of privacy policies, and potentially limiting the amount of an institution's data sharing with third parties to avoid having to send additional notices, while institutions benefit from reduced costs.

"Consumers need clear and accessible information about how their personal information is being used in the marketplace, but some of these requirements were redundant," CFPB Director Richard Cordray said in a statement. "Posting privacy notices online will make it easier for consumers to access these important policies, while also making it cheaper for financial institutions to provide disclosures."

Despite protestations from the financial industry that the Privacy Notice Rule, as proposed, would do little or nothing to ease the burden of annual privacy notices on most financial institutions, the CFPB issued the final rule with little or no substantive modification. Legislation currently pending in Congress could prove to be more effective than the CFPB's rule, and it is possible that those legislative proposals will not be derailed by the CFPB's effort here. These legislative proposals would, for instance, provide an exception to the annual written

---

### **The Privacy Notice Rule is the latest instance of regulatory relief provided to financial institutions by the CFPB**

---

notice requirement for any financial institution that provides nonpublic personal information in accordance with the GLBA and Regulation P, has not updated its privacy policy since its last written disclosure, and provides online access to its most recent disclosure to all customers.<sup>8</sup> Unlike the Privacy Notice Rule, which requires financial institutions to use the GLBA model form and prohibits sharing FCRA information with affiliates, effectively denying relief to all but the smallest financial institutions, the

pending legislative proposals in Congress would provide regulatory relief regardless of whether a financial institution provides an FCRA affiliate sharing opt-out or uses the CFPB model privacy notice.

### **Compliance with the Privacy Notice Rule**

Even though financial institutions seeking to use the alternative delivery method must use the CFPB's model privacy notice, the Privacy Notice Rule does not provide clear guidance as to how covered institutions may modify the model notice while still taking advantage of the alternative delivery method. Many financial institutions use the model privacy notice, and many of these institutions have slightly modified it to tailor it to their specific circumstances. The CFPB has made clear that such modifications, however minor, may mean that the financial institution will not be entitled to the safe harbor afforded by the model privacy notice.<sup>9</sup> The CFPB failed to provide helpful guidance on this issue, noting that "financial institutions may consult counsel on how to comply so as to limit the risk of government enforcement" as a result of departures from the model privacy notice. This does not serve as much encouragement for financial institutions seeking to post annual notices online, and may ultimately limit the degree to which financial institutions adopt what could be, if properly structured, a sensible and consumer-friendly alternative means of notice.

---

<sup>8</sup> See, e.g., Eliminate Privacy Notice Confusion Act, H.R. 749, 113th Cong. (passed Mar. 12, 2013); Privacy Notice Modernization Act of 2013, S. 635, 113th Cong. (introduced Mar. 21, 2013).

<sup>9</sup> See 12 CFR part 1016, App. B(1)(b). Regulators should not take issue with the notice, however, if the notice is consistent with the requirements of the GLBA Privacy Rule. See, e.g., 74 Fed. Reg. 62890, 62890 (Dec. 1, 2009) (final rulemaking notice) ("While the model form provides a legal safe harbor, institutions may continue to use other types of notices that vary from the model form so long as these notices comply with the privacy rule.")



# FCC DIVES INTO PRIVACY AND DATA SECURITY ENFORCEMENT



**Ted Serra**  
Associate, Washington, D.C.  
tserra@wsgr.com



**Victoria Jeffries**  
Associate, Washington, D.C.  
vjeffries@wsgr.com

Making a splash with its first-ever data security enforcement actions, the Federal Communications Commission (FCC) entered uncharted waters late last year by aggressively asserting its role in safeguarding consumer information. In the fall of 2014, for the first time, the FCC took administrative enforcement action in two instances against telecommunications carriers that misused data, misrepresented their data security efforts, and failed to appropriately secure customer data. The FCC's efforts demonstrate that it believes it has a role to play in the wider privacy landscape, even as the Federal Trade Commission (FTC) has thus far taken the lead on privacy and data security enforcement.<sup>1</sup>

Notably, the FCC's enforcement actions occurred in the absence of the commission having issued any guidelines, promulgated any rules under notice and comment procedures, or announced any policy objectives. Regardless, the FCC has indicated that it believes that it has jurisdiction over telecommunications carriers to scrutinize their data security and customer information use practices. The sudden arrival of a second data

security regulator creates uncertainty for businesses in the communications and technology space.

## Consent Decree with Verizon

The FCC first announced, in September 2014, that its enforcement bureau reached a settlement agreement with Verizon based on allegations of misuse of customer information.<sup>2</sup> The FCC alleged that Verizon unlawfully used the customer proprietary network information (CPNI) of two million subscribers for marketing purposes, and failed to notify subscribers of their privacy rights under FCC rules or their ability to opt out of marketing programs. The commission further alleged that Verizon failed to notify the FCC of its noncompliance within the five-day timeframe required under FCC rules. The consent decree imposed a \$7.4 million fine on Verizon as well as a three-year compliance program requiring opt-out notifications on customer bills, and billing system testing, monitoring, and reporting requirements.

## Civil Liability Notice for TerraCom and YourTel America

One month later, the FCC issued a Notice of Apparent Liability (NAL) to two carriers, TerraCom and YourTel, alleging their failure to secure sensitive customer information.<sup>3</sup> Both companies are landline and wireless phone service carriers that collect customer information from low-income applicants seeking to qualify for Lifeline/Universal Service Fund reduced rate phone service. The

parties collected applicants' Social Security numbers, names, addresses, and driver's license data. The FCC alleged that TerraCom and YourTel: stored applicants' data on unprotected servers accessible from anywhere on the Internet, thereby compromising the data of over 300,000 consumers; failed to notify customers that their information was or could be breached; and put forth privacy policies assuring applicants that information collected was appropriately secured when in fact it was not. The FCC concluded that the "carriers' failure to reasonably secure their customers' personal information violate[d] the companies' statutory duty under the Communications Act to protect that information, and also constitute[d] an unjust and unreasonable practice in violation of the Act . . ."<sup>4</sup> Consequently, and by a sharply divided vote of 3-2, the FCC issued a NAL proposing a \$10 million forfeiture penalty on the companies.<sup>5</sup>

## Legal Basis for FCC's Actions Remains Uncertain

The FCC has cast its data security efforts as a natural outgrowth of its longstanding mission to safeguard privacy in the telecommunications industry, pointing to preexisting rules governing CPNI, such as billing, call duration and location data, and customer consent requirements, along with "Do-Not-Call" efforts. Nevertheless, the statutory basis of the commission's actions is disputed, including by some of the commissioners themselves. In *TerraCom*, the

<sup>1</sup> In addition to its enforcement actions, in October 2014, the FCC joined the Global Privacy Enforcement Network (GPEN), a group of around fifty international data protection authorities that collaborates on cross-border privacy enforcement actions, develops best practices and other policies, and supports law enforcement cooperation. Together with the FTC, also a member, the FCC will now represent the U.S. in GPEN proceedings. Press Release, "FTC Joins Global Privacy Enforcement Network," October 28, 2014, available at <http://www.fcc.gov/document/fcc-joins-global-privacy-enforcement-network>.

<sup>2</sup> Press Release, "Verizon to Pay \$7.4 Million to Settle Consumer Privacy Investigation," September 3, 2014, available at [http://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0; Consent Decree & Adopting Order, Verizon, File No. EB-TCD-13-00007027 \(FCC Sept. 3, 2014\), http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2014/db0903/DA-14-1251A1.pdf](http://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation-0; Consent Decree & Adopting Order, Verizon, File No. EB-TCD-13-00007027 (FCC Sept. 3, 2014), http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0903/DA-14-1251A1.pdf).

<sup>3</sup> Press Release, "FCC Plans \$10 Million Fine for Carriers that Breached Consumer Privacy," October 24, 2014, available at <http://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy>.

<sup>4</sup> *Id.*

<sup>5</sup> Notice of Apparent Liability for Forfeiture, TerraCom, Inc. and YourTel America, Inc., File No. EB-TCD-13-00009175 (FCC Oct. 24, 2014), available at <http://www.fcc.gov/document/10m-fine-proposed-against-terra-com-and-your-tel-privacy-breaches>. Although a party issued a NAL by the FCC may pay the proposed forfeiture amount, it has a number of additional options, including appealing or seeking a reduction of the penalty from the FCC directly or forcing the FCC, in conjunction with the Department of Justice, to bring suit in federal district court to enforce its proposed judgment. 47 C.F.R. § 1.80(f) (2013).

<sup>6</sup> 47 U.S.C. § 222(a) (2012).

Continued on page 18...

FCC relied on § 222(a) of the Communications Act,<sup>7</sup> interpreting the term “proprietary information” to encompass “private information that customers have an interest in protecting from public exposure”<sup>7</sup>—a breathtakingly broad standard. Indeed, the three-commissioner majority indicated that “proprietary information” is broader than CPNI and “broadly encompasses such confidential information as privileged information, trade secrets, and personally identifiable information (PII).” The FCC also relied on § 201(b) to conclude that the companies’ lack of basic security measures was an “unjust and unreasonable” practice counter to that provision.<sup>8</sup> The commission further stated that it was unjust and unreasonable to misrepresent to customers in privacy policies that information would in fact be protected, and to fail to notify customers that their data may have been compromised.

Two commissioners strongly dissented from the FCC’s decision in *TerraCom*.<sup>9</sup> They criticized their colleagues’ interpretation of the act as imposing a duty to protect PII, and disputed the notion that § 222 extends to anything beyond CPNI as defined in the statute. They also stated that the FCC’s actions ran afoul of due process by not providing advance, fair warning of carrier obligations, particularly as regards the notification obligation that the majority found implicit in the statute. Even if the act provided a sufficient legal basis for FCC data protection enforcement, the dissenters admonished that the FCC should first conduct a rulemaking to establish and provide proper

notice of the duties to be imposed on carriers. The dissenters’ statements reveal that, despite the FCC’s bold enforcement actions, the commission is deeply divided as to what, if any, is the agency’s appropriate role as a watchdog in the data security space.

## **Overlapping Enforcement or Under-Enforcement?**

Even if its statutory authority is murky, the FCC appears to have set a course to continue its efforts in the data security space alongside the FTC. While the FTC’s reach extends to a broad swath of industries, the FTC Act specifically excludes common carriers, as defined by the Communications Act, from the FTC’s jurisdiction.<sup>10</sup> It is perhaps for this reason that the FCC has waded into data protection enforcement as it relates to such carriers; otherwise, their privacy and data security practices might go unchecked. Indeed, in an ongoing dispute with the FTC over data throttling, AT&T, a common carrier, has argued that it is wholly exempt from FTC regulation, including where it offers services, like mobile data, that are not common carrier services.<sup>11</sup> Should AT&T prevail, and should courts find that the FCC exceeded its statutory authority if that agency’s jurisdiction is challenged, then the data security and privacy practices of common carriers would fall outside the jurisdiction of both agencies. And it is not just the FCC’s statutory authority that has been questioned; the FTC continues to fend off challenges to its own statutory authority to regulate privacy and data protection matters at all.<sup>12</sup>

Publicly, the FTC has pledged to cooperate with the FCC and dismissed speculation that there is a growing turf war between the agencies.<sup>13</sup> Nevertheless, the precise bounds of the FCC’s privacy and data security jurisdiction, and whether it can reach beyond common carriers, are unclear, setting the stage for conflict between the two agencies. Could the FCC extend jurisdiction over mobile application developers, telecommunications equipment manufacturers (ranging from mobile handsets and set top boxes to Internet-connected light bulbs and personal fitness trackers), cloud storage services, or other businesses whose products or services are telecom- or Internet-related? And if so, would these entities, none of which are common carriers, also be subject to FTC jurisdiction? Businesses run the risk of getting stuck in the cross-fire.

Jurisdictional issues aside, Commissioner Ajit Pai, who dissented in *TerraCom*, has called for the FCC, at the very least, to engage in rulemaking before enforcing standards of which industry was not previously apprised. A rulemaking would give businesses the opportunity to voice their concerns and share their perspective on potential rules during the notice and comment process. Regardless, the FCC will almost certainly face future challenges to its own statutory authority to bring enforcement actions in the absence of promulgated rules. As the other dissenter in *TerraCom*, Commissioner Michael O’Rielly, pointedly noted, “I would not be surprised to see this issue litigated at some point.”<sup>14</sup>

<sup>7</sup> See *TerraCom*, *supra* note 5.

<sup>8</sup> 47 U.S.C. § 201(b) (2012).

<sup>9</sup> See *TerraCom*, *supra* note 5 (Pai, O’Rielly, dissenting).

<sup>10</sup> 15 U.S.C. § 45(a)(2) (2012).

<sup>11</sup> See Emily Field, “AT&T Says it’s Out of FTC’s Jurisdiction in ‘Throttling’ Suit,” *Law360*, January 5, 2015, available at <http://www.law360.com/articles/608363/at-t-says-it-s-out-of-ftc-s-jurisdiction-in-throttling-suit>.

<sup>12</sup> Allison Grande, “Privacy Cases to Watch in 2015,” *Law360*, January 2, 2015, available at <http://www.law360.com/articles/605174/privacy-cases-to-watch-in-2015> (discussing challenges to FTC’s data protection authority brought by Wyndham Worldwide Corp. and LabMD Inc.).

<sup>13</sup> Allison Grande, “FTC Official Sees No Turf War With FCC On Data Security,” *Law360*, November 5, 2014, available at <http://www.law360.com/privacy/articles/593798/ftc-official-sees-no-turf-war-with-fcc-on-data-security>.

<sup>14</sup> See *TerraCom*, *supra* note 5 (O’Rielly, dissenting).

# RECENT EXECUTIVE ORDER TO PUSH FOR SECURITY OF CONSUMER FINANCIAL TRANSACTIONS, IDENTITY THEFT REMEDIATION



**Jonathan Adams**  
Associate, San Francisco  
jadams@wsgr.com

On October 17, 2014, the White House released its plans for a “BuySecure Initiative” in an executive order entitled “Improving the Security of Consumer Financial Transactions.” The initiative aims to push the market toward adopting more secure payment methods and to reduce the burden on consumers seeking to remediate identity theft incidents. The White House simultaneously published a fact sheet explaining the impetus for the action, the changes proposed in the order, and the potential downstream effects from the steps outlined.

The White House explained that the initiative is intended to “move [the U.S.] economy toward stronger, more secure technologies that better secure transactions and safeguard sensitive data” by having federal agencies “lead by example.” Although the president’s executive order is limited in its application to agencies within the executive branch, the White House stated that it will work with “a number of major corporations” to advance these goals and, in a speech announcing the order, President Obama announced plans for a White House summit on cybersecurity and consumer protection. Although the initiative is intended to encourage further implementation of secure payment systems and to identity theft remediation practices, the White House used the announcement to reiterate its calls for Congress to pass data breach and cybersecurity legislation.

## Securing Government Payments

The president’s order mandates that executive departments and agencies begin transitioning

payment processing terminals and agency credit, debit, and other payment cards to more secure systems, specifically systems incorporating chip-and-PIN technology.<sup>1</sup> Under the order, the Department of the Treasury will, no later than January 1, 2015, take “all necessary steps” to ensure that payment processing terminals acquired by the federal government incorporate chip-and-PIN technology. Further, the order mandates that the Department of the Treasury and General Services Administration (GSA) only issue payment cards with similar security features by that date; the order also calls for the GSA to begin replacing less secure payment cards no later than January 1, 2015. All other agencies are required to provide to the Office of Management and Budget (OMB), no later than January 1, 2015, their plans for ensuring that their payment cards have enhanced security features.

Although the order’s mandates directly affect only the executive branch agencies, the White House has indicated that these measures are intended to nudge the U.S. marketplace towards a quicker adoption of chip-and-PIN and other enhanced security measures for payment mechanisms. Already, the market has demonstrated that retailers’ prior hesitation to invest in the infrastructure needed for acceptance of chip-and-PIN payment cards is evaporating. As the fact sheet explains, a number of large companies—including American Express, Home Depot, Target, Visa, Walgreens, and Walmart—are in the process of establishing a wide framework for acceptance of chip-and-PIN cards in the private sector. Many of these private sector efforts were well under way before the order; given recent data breaches triggered by inadequate point-of-sale card security, efforts by card issuers and credit unions to shift greater risk for unauthorized

charges to retailers, and the reliance of many foreign markets on chip-and-PIN payment cards, the “BuySecure Initiative” is not groundbreaking in its push for widespread adoption of more secure payment mechanisms. By involving the federal government in this push, however, the initiative commits the government to these efforts to transition payment mechanisms and cards to use enhanced security features and may expedite adoption throughout the private sector by virtue of the White House endorsement.

## Identity Theft Remediation

The executive order included measures aimed at reducing the burden on consumers who have been victimized by identity theft, including steps to reduce the amount of time an individual consumer would need to remediate a typical identity-theft incident. The order mandates that by February 15, 2015, the Department of Justice (DOJ) and Department of Homeland Security (DHS) issue guidance to promote regular submissions by federal law enforcement agencies of identified, compromised credentials to the National Cyber-Forensics and Training Alliance’s Internet Fraud Alert System. This will be followed by the DOJ, the Department of Commerce, and the Social Security Administration which will identify, and provide information relating to all publicly available resources for identity theft victims to the Federal Trade Commission (FTC), with the expectation that these agencies will work together to streamline these resources and consolidate them (where possible) on the FTC’s website, IdentityTheft.gov. The White House expects that the consolidation of these resources will occur no later than March 15, 2015. Under the order, the OMB and GSA are required to assist the FTC in enhancing the

<sup>1</sup> “Chip-and-PIN” technology generally refers to any payment card containing EMV smart card technology that relies upon an embedded chip and a user-supplied PIN.

*Continued on page 20...*

## RECENT EXECUTIVE ORDER TO PUSH FOR SECURITY . . .

website, including coordinating with the national credit bureaus to ensure improved reporting and remediation processes in connection with the credit bureaus' systems, with the goal of launching an improved IdentityTheft.gov no later than May 15, 2015.

The White House's fact sheet explains that the "BuySecure Initiative" also includes a number of public-private partnerships and measures aimed at improving identity theft remediation. In both the fact sheet and in President Obama's announcement of the initiative, the White House lauded a number of leaders in the financial services industry, under the leadership of the Consumer

Financial Protection Bureau (CFPB), that have or will be providing their individual customers with free access to FICO scores, and that certain card issuers, including MasterCard, will provide customers with additional support in resolving identity theft and fraud claims.

### **Securing Federal Data Disclosures**

The White House also mandated that federal agencies take measures to ensure that sensitive data is shared by the government only with the appropriate recipients. Specifically, the order directed the National Security Council staff, the Office of Science

and Technology Policy, and OMB to present to the White House a plan no later than January 15, 2015, that would ensure that all federal agencies making data accessible to citizens through digital applications require the use of multi-factor authentication and a process that is effective at proving individual identity. Any such plan would need to be consistent with the 2011 National Strategy for Trusted Identities in Cyberspace. Relevant federal agencies are expected to have eighteen months following the presentation of the joint plan to implement any necessary steps for ensuring such identity verification.



650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | [www.wsgr.com](http://www.wsgr.com)

Austin Beijing Brussels Hong Kong Los Angeles New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC Wilmington, DE

This communication is provided for your information only and is not intended to constitute professional advice as to any particular situation.  
© 2015 Wilson Sonsini Goodrich & Rosati, Professional Corporation. All rights reserved.