

# EYE ON PRIVACY

OCTOBER 2014

## WELCOME

In this issue of *Eye on Privacy*, we discuss an FTC staff report that evaluates the consumer disclosures made by a number of popular mobile shopping applications, and we address the recent explosion of class action litigation under the Telephone Consumer Protection Act based on calls or text messages to cell phones and a perceived ambiguity in what qualifies as an automated dialing system. In addition, we examine some significant new California laws on student privacy and education data, consider recent guidance from federal regulators to businesses that are considering sharing information relating to cybersecurity risks with other companies and the government, and examine an FTC staff report on mobile cramming.

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



*Lydia Parnes*

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



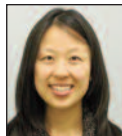
*Michael Rubin*

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

## FTC RECOMMENDS IMPROVED TRANSPARENCY AND SECURITY IN MOBILE SHOPPING APPS



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



**Sharon Lee**  
Associate, Palo Alto  
[shlee@wsgr.com](mailto:shlee@wsgr.com)



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

or find any fault with app platforms, like Google Play or Apple's App Store, with respect to the consumer disclosures of those apps. This report follows the FTC staff's March 2013 mobile payment report that recommended mobile payment providers convey clear policies regarding fraudulent and unauthorized charges, encouraged all stakeholders to raise consumer awareness about mobile payment security, and stressed the applicability of its general privacy recommendations to companies in the mobile payment marketplace.<sup>2</sup>

*Continued on page 2...*

In August 2014, the Federal Trade Commission (FTC) published a staff report that evaluates the consumer disclosures made by a number of popular mobile shopping applications and makes recommendations to the providers and users of those apps.<sup>1</sup> The FTC staff did not address

<sup>1</sup> FTC staff, "What's the Deal? An FTC staff Study on Mobile Shopping apps" (Aug. 2013), available at <http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf>.

<sup>2</sup> FTC, "Paper, Plastic...or Mobile?: An FTC Workshop on Mobile Payments" (March 2013), available at <http://www.ftc.gov/opa/2013/03/mobilepymts.shtm>. For information relating to the March 2013 report, see WSGR Alert: FTC Recommends Consumer Protections for Mobile Payment Industry, March 28, 2013, available at <http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-mobile-payment-industry.htm>.

### IN THIS ISSUE

**FTC Recommends Improved Transparency and Security in Mobile Shopping Apps**.....Pages 1-3

**Appellate Courts to Address What Constitutes an "Automatic Telephone Dialing System" Under the TCPA**.....Pages 3-4

**California Enacts Landmark Student Privacy Laws**.....Pages 5-6

**Federal Agencies Reduce Barriers to Cyber Threat Information Sharing**.....Pages 7-9

**FTC Issues Carrier Billing Recommendations to Protect Consumers Against Mobile Cramming**.....Pages 10-11

In surveying shopping apps for its most recent report, the FTC staff reviewed 121 different apps available through Google Play and Apple's App Store. The FTC staff focused specifically on apps that: (i) facilitate real-time price comparisons; (ii) facilitate consumers' efforts to find and redeem coupons or discounts; and (iii) allow consumers to make purchases in physical stores. For each app, the FTC staff reviewed the app promotion pages, developer websites, and other pre-download information.

The report contained the following recommendations for the providers of shopping apps:

- Companies should disclose consumer rights and liability limits for unauthorized, fraudulent, or erroneous transactions.
- Companies should clearly describe data collection, use, and sharing.
- Companies should provide strong data security matching their promises.

The FTC staff also issued parallel recommendations for users of shopping apps.

---

## In-store purchase apps can process transactions in ways that affect which statutory protections apply to consumers for unauthorized payments

---

### Recommendations for Businesses

*Companies should disclose consumer rights and liability limits for unauthorized,*

*fraudulent, or erroneous transactions.*

Because in-store purchase apps can process transactions in ways that affect which statutory protections, if any, apply to consumers for unauthorized purchases or payments, the FTC staff reviewed 30 in-store purchase apps for descriptions of the applicable transaction model, as well as consumer dispute resolution procedures and liability limits. The majority of these apps used a "pass-through" transaction model—a transaction in which the consumer makes a purchase through an app by placing a charge directly on a credit, debit, or prepaid card. According to the report, under this model consumers have the same statutory and contractual protections as if the consumer had used the physical payment card in a traditional transaction.<sup>3</sup> The remaining in-store purchase apps followed a "stored value" transaction model, under which consumers are required to deposit funds into an account maintained by the app provider and used to pay for purchases through the app. The report explained that under this model, consumers generally do not have the same statutory protections that apply to purchases with credit or debit cards and instead, can only rely on the protections that are voluntarily provided.

The FTC staff found that only 16 of the 30 in-store purchase apps made disclosures relating to dispute resolution procedures or liability limits and furthermore, and only nine of these 16 apps provided written protections for their users. Notably, seven of the 30 in-store purchase apps disclaimed all liability arising from transactions through the app. The FTC staff also found it generally difficult to obtain clear information about the apps' applicable transaction models.

As a result of this survey, the FTC staff reiterated the recommendation made in its March 2013 mobile payment report that in-store app providers (and particularly, providers of "stored value" apps) should provide clear pre-download information to consumers

regarding consumer dispute resolution procedures and liability limits.

---

## FTC staff found that only 16 of the 30 in-store purchase apps surveyed made disclosures relating to dispute resolution procedures or liability limits

---

*Companies should clearly describe data collection, use, and sharing.* Given the capability of mobile devices and mobile apps to collect a significant amount of user data, the FTC staff surveyed the privacy policies for all shopping apps that it reviewed. Nearly all of the apps surveyed were governed by privacy policies, whether available on the app developers' websites or on the apps' promotion pages within Google Play or the Apple iTunes Store. In many cases, however, the FTC staff considered the disclosures relating to data collection and, in particular, data use and sharing, to be vague, which they believed would make it difficult for consumers to assess how the particular shopping app would actually handle their data.

Consequently, while the FTC staff was encouraged by the number of readily available privacy policies, it nonetheless found that the privacy policies "fail[ed] to achieve what should be the central purpose of any privacy policy—making clear how data is collected, used, and shared." As a corollary, the FTC staff suggested that app developer should further consider reasonable data collection and use limitations.

*Companies should provide strong data security matching their promises.* The FTC

---

<sup>3</sup>The report notes that federal law limits consumer liability for credit and debit transactions and provides dispute resolution procedures for errors. However, for prepaid card transactions, consumers must generally rely on their contracts with these card providers for these protections.

Continued on page 3...

staff reviewed the privacy policies of all surveyed shopping apps for security-related language because, according to the report, consumers often cite security concerns as hindering their adoption of mobile payment technologies. The FTC staff found that over 80 percent of the shopping apps surveyed made promises in their privacy policies relating to the apps' data security practices. Although the FTC staff did not test the apps to verify their security-related promises, it encouraged all companies offering shopping apps to secure the data they collect and honor any such promises made to consumers. To this end, the report directed app developers to look to the "reasonable and appropriate

security standards for mobile apps" promulgated by the FTC in its enforcement actions and business guidance materials.

### Recommendations for Consumers

The FTC staff also issued a number of recommendations for consumers using shopping apps, which are synchronized with its recommendations to companies. First, the FTC staff advised that consumers should review each shopping app's dispute resolution procedures and liability limits and, in the context of applicable statutory protections, consider the payment methods they will use to fund their purchases. Likewise, the FTC

staff encouraged consumers to seek information about how their data will be collected, used, and shared by shopping apps before downloading them.

### Implications

As evidenced by and stated in the report, the FTC staff has continued to make emerging mobile issues a high priority. Although the report did not call for greater federal oversight or rulemaking, shopping app providers should consider the report's recommendations and determine how to best implement these recommendations into their apps and business practices.

## APPELLATE COURTS TO ADDRESS WHAT CONSTITUTES AN "AUTOMATIC TELEPHONE DIALING SYSTEM" UNDER THE TCPA



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

During the past decade, there has been an explosion in class action litigation under the Telephone Consumer Protection Act<sup>1</sup> (TCPA), a well-intended statute meant to address abusive telemarketing practices. As of late, many of these suits are based on calls or text messages to cell phones. The TCPA prohibits non-emergency calls (interpreted by the FCC to include text messages) to a cell phone made using an "automatic telephone dialing system" without the prior express consent of the called party.<sup>2</sup> A perceived ambiguity in what type of equipment qualifies as an "automatic telephone dialing system" has fueled these litigation fires and has led to hundreds of cases being filed against companies that do not use telemarketing

equipment but communicate with their users or facilitate their users' communications via text message. An end to the litigation explosion in this area may be just around the corner as federal appellate courts consider the issue.

### The Conflicting Authority

The TCPA defines "automatic telephone dialing system" as "equipment which has the capacity—(A) to store or produce telephone numbers to be called, *using a random or sequential number generator*; and (B) to dial such numbers."<sup>3</sup> Congress purposefully included the "using a random or sequential number generator" limitation because it meant to regulate only the particular kinds of automated calling technologies that were used by telemarketers to make unsolicited phone calls to unwilling recipients—equipment that could generate and dial

A perceived ambiguity in what type of equipment qualifies as an "automatic telephone dialing system" has fueled these litigation fires

random or sequential phone numbers.<sup>4</sup> Congress was concerned that through the use of dialing systems that could generate and dial random phone numbers, or sequential phone numbers (555-1111, 555-1112, 555-1113, etc.), intrusive telemarketing calls might reach unlisted numbers, hospitals, or emergency organizations.<sup>5</sup> Likewise, Congress was concerned that telemarketers might "dial

<sup>1</sup> 47 U.S.C. § 227

<sup>2</sup> See *id.* § 227(b)(1)(A)(iii).

<sup>3</sup> *Id.* § 227(a)(1) (emphasis added).

<sup>4</sup> See, e.g., S. Rep. 102-178, at 2 ("[h]aving an unlisted number does not prevent those telemarketers that call numbers randomly or sequentially"); *id.* ("some automatic dialers will dial numbers in sequence, thereby tying up all the lines of a business and preventing any outgoing calls").

<sup>5</sup> See, e.g., 137 Cong. Rec. 35302 (Nov. 26, 1991); H.R. Rep. No. 102-317, at 10 (1991) ("Telemarketers often program their systems to dial sequential blocks of telephone numbers, which have included those of emergency and public service organizations, as well as unlisted telephone numbers."); S. Rep. No. 102-178, at 2 (1991); H.R. Rep. No. 101-633, at 3 (1990).

Continued on page 4...

numbers in sequence, thereby tying up all the lines of a business and preventing outgoing calls.”<sup>6</sup>

Properly giving meaning to each term used by Congress in this definition, and consistent with congressional intent, numerous courts have construed the definition of “automatic telephone dialing system” as requiring that the equipment used to place the calls or send the texts have an existing capacity to generate and dial random or sequential telephone numbers.<sup>7</sup>

Other district courts, however, have concluded that the equipment at issue need not have a capacity to generate and dial random or sequential phone numbers to qualify as an “automatic telephone dialing system.” These courts reason that when deciding whether a “predictive dialer”—a specific type of telemarketing dialing equipment used to time live telemarketing calls predicting when a telemarketer will be available to be connected with the consumer who answers—falls within the definition of an ATDS, the FCC somehow expanded the statutory definition of “automatic telephone dialing system” to encompass any system capable of

placing calls or sending texts to stored lists of numbers without human intervention.<sup>8</sup>

### The Opportunity for Appellate Courts to Provide Much Needed Clarification

In *Dominguez v. Yahoo!, Inc.*,<sup>9</sup> the district court properly concluded that to qualify as an “automatic telephone dialing system,” the equipment at issue must have the present capacity to generate random or sequential telephone numbers. Because the undisputed evidence reflected that the defendant’s system lacked that capacity, the court granted summary judgment for the defendant. The plaintiff has appealed this decision to the Third Circuit.<sup>10</sup> The appeal has been fully briefed and is directed at the proper interpretation of “automatic telephone dialing system” under the TCPA.

In *Sterk v. Path, Inc.*,<sup>11</sup> the district court concluded that equipment qualifies as an “automatic telephone dialing system” if it merely can dial numbers from a stored list without human intervention. Following that decision, the case was assigned to a new judge who granted the defendant’s motion to certify the prior judge’s decision for

immediate appeal to the Seventh Circuit. In so doing, the new judge concluded that there are substantial grounds for disagreement as to whether the prior judge properly construed the term “automatic telephone dialing system” under the TCPA.<sup>12</sup> The parties are now awaiting a decision from the Seventh Circuit as to whether it will agree to take the appeal.

### Conclusion

The Third Circuit will soon decide the proper scope of an “automatic telephone dialing system” under the TCPA, and the Seventh Circuit also may do so. Hopefully, these courts will take the opportunity to give meaning to each word used by Congress and further congressional intent by limiting the scope of an “automatic telephone dialing system” to include only equipment that has the capacity to generate and dial random or sequential telephone numbers. This clarification is necessary to stem the tide of opportunistic TCPA class action litigation against innovative companies that communicate with their users via text but do not engage in telemarketing and take such companies outside the scope of the statute.

<sup>6</sup>S. Rep. No. 102-178, at 1-2.

<sup>7</sup>See, e.g., *Dominguez v. Yahoo!, Inc.*, No. 13-1887, 2014 U.S. Dist. LEXIS 36542, at \*19 (E.D. Pa. Mar. 20, 2014) (granting summary judgment to defendant because it was undisputed that its system could not generate random or sequential phone numbers); *Gragg v. Orange Cab Co.*, No. C12-0576RSL, 2014 U.S. Dist. LEXIS 16648, at \*7-10 (W.D. Wash. Feb. 7, 2014) (same); *Stockwell v. Credit Mgmt.*, No. 30-2012-00596110, slip op. at 2 (Cal. Super. Ct. Oct. 3, 2013) (granting summary judgment for defendant where plaintiff failed to rebut defendant’s evidence that it had no number generator); *Hunt v. 21st Mortg. Corp.*, No. 2:12-cv-2697, 2013 U.S. Dist. LEXIS 132574, at \*11 (N.D. Ala. Sept. 17, 2013) (“The court therefore holds that, to meet the TCPA definition of an ‘automatic telephone dialing system,’ a system must have a present capacity, at the time the calls were being made, to store or produce and call numbers from a number generator”); *Ibey v. Taco Bell Corp.*, No. 12-cv-0583-H, 2012 U.S. Dist. LEXIS 91030, at \*9 (S.D. Cal. June 18, 2012) (dismissing TCPA claim for failure to plausibly plead use of ATDS; Plaintiff’s allegation that there ‘was no human intervention’ did not satisfy statutory requirements; “[A] system need not actually store, produce, or call randomly or sequentially generated numbers, it need only have the capacity to do it”).

<sup>8</sup>See *Sterk v. Path, Inc.*, No. 13-c-2330, 2014 U.S. Dist. LEXIS 73507, \*10-19 (N.D. Ill. May 30, 2014) (citing *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991* (“2003 FCC Order”), 18 FCC Rcd. 14014, 14091-93 (July 3, 2003) and concluding that the defendant’s system was an ATDS because it could dial lists of numbers without human intervention); *Legg v. Voice Media Grp., Inc.*, No. 13-cv-62044, 2014 U.S. Dist. LEXIS 67623, at \*9-11 (S.D. Fla. May 16, 2014) (citing 2003 FCC Order at 14,091-93 and stating that in it “the FCC expanded [the ATDS] definition when it addressed the question of ‘predictive dialer’”); *Fields v. Mobile Messengers America, Inc.*, No. 12-cv-05160, 2013 U.S. Dist. LEXIS 180277, at \*10-11 (N.D. Cal. Dec. 23, 2013) (citing 2003 FCC Order and concluding that it “broadened the definition of an ATDS beyond mere equipment that uses ‘random or sequential number generators’ to cover any equipment with ‘the capacity to dial numbers without human intervention’”(emphasis in original)).

<sup>9</sup>No. 13-1887, 2014 U.S. Dist. LEXIS 36542 (E.D. Pa. Mar. 20, 2014)

<sup>10</sup>See *Dominguez v. Yahoo! Inc.* No. 14-1751 (3d Cir.)

<sup>11</sup>No. 13-c-2330, 2014 U.S. Dist. LEXIS 73507 (N.D. Ill. May 30, 2014)

<sup>12</sup>*Sterk v. Path, Inc.*, No. 13-cv-2330 (N.D. Ill.), ECF No. 143

# CALIFORNIA ENACTS LANDMARK STUDENT PRIVACY LAWS



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

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

In keeping with its position as the nation's leader on privacy issues, the state of California recently enacted significant new laws on student privacy and education data. The Student Online Personal Information Protection Act (SOPIPA) sets forth a variety of restrictions on how operators of online services offered in schools can use and disclose student information, and requires operators to implement reasonable security measures to protect student data. A separate law (A.B. 1584) sets forth privacy requirements for providers of digital storage services and educational software used in schools. A final law (A.B. 1442) establishes privacy requirements for companies that collect students' social media information on behalf of schools. The laws were signed by Governor Jerry Brown on September 29, 2014.

---

**The Student Online Personal Information Act sets forth a variety of restrictions on how operators of online services offered in schools can use and disclose student information**

---

## SOPIPA

SOPIPA applies to operators of websites, online services, and applications (services) that are designed, marketed, and primarily used for K-12 school purposes. The law prohibits operators from showing any targeted advertising on its own services, or from using any information collected through its services for targeted advertising or marketing. Operators are also prohibited from amassing profiles about students for reasons unrelated to school purposes and from selling student information.

Subject to certain exceptions, SOPIPA prohibits operators from disclosing personally identifiable information that is created or provided by a student, parent, or school employee, or that is gathered by the operator through its service (such as name, email, home address, telephone number, social security numbers, discipline records, test results, grades, medical records, food purchases, political affiliations, religious information, text messages, search activity, photos, voice recordings, or geolocation information). SOPIPA sets forth several exceptions, such as disclosures to schools for K-12 school purposes; disclosures to service providers where a contract provides privacy and security protections; and disclosures for legitimate research purposes (i.e., research required or allowed by law, and conducted by a school, district, or education department).

SOPIPA also requires operators to maintain reasonable security measures and comply with schools' requests to delete student information.

## A.B. 1584

California's Education Code generally prohibits school districts from allowing access to student records without parental consent.

---

**California's Education Code generally prohibits school districts from allowing access to student records without parental consent; one exception is for certain contractors that provide educational services or functions**

---

One exception is for certain contractors that provide educational services or functions. A.B. 1584, which will become part of California's Education Code, makes clear that school districts are permitted to enter into contracts with third parties for the purpose of providing digital storage services (including cloud-based services) for student records, and for the purpose of providing educational software that uses or accesses student records. Student records are defined broadly to include all information directly related to a student that is maintained by a school, and all information acquired from a student in the course of using educational software assigned by a teacher or school agent.<sup>1</sup>

A.B. 1584 requires that such contracts prohibit third parties from using student records for any purposes besides those permitted in the contract, and must specifically prohibit third parties from using students' personally identifiable information to engage in targeted advertising. The contracts also must include descriptions of the third party's security measures, how it will provide notification in the event of a data breach, and how a parent or student can review and correct personally identifiable

<sup>1</sup> A.B. 1584, Section 1, Section 49073.1(a)(2).

*Continued on page 6...*

information. The contract must prohibit the retention of student records after completion of the contract, unless the student chooses to establish an account with the third party to keep content they create (such as research, essays, and photos). Any contract that fails to include these provisions may be rendered void.

## **A.B. 1442**

A.B. 1442, which will be incorporated into the California Education Code, applies to third parties who contract with schools to gather social media information on enrolled students. The bill requires that such contracts include provisions prohibiting the third party from using the social media information outside the scope of the contract or selling or sharing the information with anyone but the school, student, or the student's parent or legal guardian. The contract also must require the third party to destroy the information after the contract is completed, or when a student turns 18 years of age or is no longer enrolled in the school.

Under the bill, social media includes, but is not limited to, electronic "videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet website profiles or locations." It does not include "electronic service[s] or account[s] used exclusively for educational purposes or primarily to facilitate creation of school-sponsored publications, such as a yearbook or pupil newspaper, under the direction or control of a school, teacher, or yearbook adviser."<sup>2</sup>

## **Implications**

California's new student privacy laws will have a significant impact on technology companies that provide online services to California's K-12 schools. A.B. 1442 and A.B. 1584 will govern all covered contracts that come into effect on or after January 1, 2015, while SOPIPA is set to become operative on January 1, 2016. Technology companies that offer educational software, digital storage

---

**New student privacy laws will have a significant impact on companies that provide online services to California's K-12 schools**

---

services, or other services used in California schools should be cognizant of these newly enacted laws. Additionally, it is possible that other states may follow California's lead and extend the scope of their own education codes. Companies should be aware of this expansion in California's student privacy laws and ensure that their contracts and privacy practices comport with them.

---

<sup>2</sup> A.B. 1442, Section 1, Section 49073.6(a)(2).

## **Tip**

Have you checked your cookies lately? Make sure you understand how you set cookies and how you use the information you collect via cookies.

# FEDERAL AGENCIES REDUCE BARRIERS TO CYBER THREAT INFORMATION SHARING



**Jonathan Adams**  
Associate, Palo Alto  
jadams@wsgr.com

Federal regulators released guidance in the first half of 2014 that should provide comfort to businesses that are considering sharing information relating to cybersecurity risks with other companies and the government. Although these advisory opinions are nonbinding and do not carry the force of law, they provide strong indications of the priorities of the U.S. Department of Justice (DOJ) and Federal Trade Commission (FTC) with respect to facilitating the ability of businesses to engage in cybersecurity risk mitigation. Notably, under the recent guidance, the federal regulators suggest that antitrust and electronic communications privacy concerns, which may have previously made businesses hesitant to share certain information relating to cybersecurity risks, should not preclude business-to-business or business-to-government information sharing that is tailored to mitigate these risks.

## Joint Policy Statement on Antitrust Implications of Cybersecurity Risk Information Sharing

On April 10, 2014, the DOJ and FTC<sup>1</sup> issued a joint policy statement to make clear to businesses that properly designed and appropriate sharing of cybersecurity risk information is unlikely to raise antitrust concerns.<sup>2</sup> Noting that private sector entities play a “critical” role in the fight to mitigate and respond to cyber threats, Deputy Attorney General James M. Cole argued that this joint

policy statement “should encourage [businesses] to share cybersecurity information.” Until the statement, federal antitrust regulators had not weighed in on antitrust considerations relating to cybersecurity information sharing since the DOJ Antitrust Division issued specific guidance to the Electric Power Research Institute in 2000, in which the DOJ confirmed that it did not intend to take enforcement action as a result of the company’s proposal to exchange certain cybersecurity information, including exchanging actual real-time cyber threat and attack information. In the joint policy statement, the DOJ and FTC reiterated that the advice the DOJ gave to Electric Power Research Institute remains valid: in reviewing any cybersecurity risk information sharing, the antitrust regulators will examine the business purpose, nature, and likely competitive effect of information exchanges and, as set forth in the Competitor Collaboration Guidelines, will evaluate the information sharing arrangements under a rule of reason analysis to determine the overall competitive effect of the agreement in a relevant market.

In the joint policy statement, the DOJ and FTC explained that the agencies recognize that the sharing of cybersecurity risk information has the potential to enhance the security, availability, integrity, and efficiency of information systems in the U.S.<sup>3</sup> The statement makes clear that “[t]he [DOJ and FTC] do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing” and suggests that firms have been overly conservative with respect to sharing data

relating to cyber threats in part because of a fear that sharing information between competitors could raise antitrust concerns. If handled appropriately, however, the DOJ and FTC view the “sharing of cyber threat information . . . [as] highly unlikely to lead to a reduction in competition” that would raise antitrust concerns. The joint policy statement cautions, however, that the legitimate sharing of cyber threat information is very different from the sharing of competitively sensitive information (e.g., pricing or output data, or business plans), which would tend to generate antitrust concerns. To the FTC and

---

**Federal regulators suggest that antitrust and privacy concerns should not preclude business information sharing that is tailored to mitigate these risks**

---

DOJ, permissible information sharing as contemplated under the joint policy statement would be limited to data that is typically technical in nature and limited in scope to cybersecurity risks. The joint policy statement, although it does not forswear enforcement action on the basis of cybersecurity information sharing, suggests that “antitrust concerns should not get in the way of sharing cybersecurity information.”<sup>4</sup>

<sup>1</sup> Michael Daniel, the White House Cybersecurity Coordinator, echoed the sentiments of the joint policy statement on the White House blog. See Michael Daniel, “Getting Serious about Information Sharing for Cybersecurity,” The White House Blog, Apr. 10, 2014, <http://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity>. Daniel noted that, in addition to executive action, the Obama administration will work with Congress and the business community to improve cybersecurity in the public and private sectors.

<sup>2</sup> DOJ & FTC, Antitrust Policy Statement on Sharing of Cybersecurity Information, Apr. 10, 2014, <http://www.justice.gov/atr/public/guidelines/305027.pdf>.

<sup>3</sup> As the joint policy statement makes clear, the DOJ and FTC would evaluate the impetus underlying information sharing, the nature of the information shared, and whether the information shared would be likely to harm competition in its rule of reason analysis to determine whether information sharing is appropriate. Although the joint policy statement notes that this is an “intensely fact-driven” inquiry, the agencies imply that the normal sharing of cybersecurity risk information—without the inclusion of additional information relating to pricing, output, business strategies, or other information that is more likely to lead to collusion—will generally be viewed as non-harmful to competition.

<sup>4</sup> James M. Cole, Dep’y Att’y Gen., Press Conference to Announce Joint Antitrust Policy Statement on Sharing of Cybersecurity Information, Apr. 10, 2014.

*Continued on page 8..*

## Department of Justice White Paper on Stored Communications Act Compliance

The Department of Justice followed the joint policy statement in May 2014 with a white paper that clarifies the DOJ's views regarding certain privacy implications of sharing cyber threat information.<sup>5</sup> The DOJ explains that companies have pressed for guidance on the permissibility of sharing communications information pertaining to cybersecurity risks with law enforcement authorities, and that the white paper should reduce the potential that "[o]verly expansive views of what information is prohibited from voluntary disclosure could unnecessarily prevent the sharing of important information that would be used to enhance cybersecurity." In this white paper, the DOJ focused on the application of the Stored Communications

Act (SCA), 18 U.S.C. § 2701 *et seq.*, in the context of voluntarily sharing aggregated data with the government to protect information systems.

Under the SCA, a provider of an "electronic communications service" (ECS)<sup>6</sup> or a "remote computing service" (RCS)<sup>7</sup> to the public is barred from knowingly divulging a record or other non-content information pertaining to one of its subscribers or customers to the government (or any other entity, in many instances) unless a statutory exception applies.<sup>8</sup> Violations of these prohibitions could result in civil liability under the SCA, 18 U.S.C. § 2707. Because of certain ambiguities in the SCA, ECS, and RCS, providers asked the DOJ whether non-content aggregate information falls within these restrictions on sharing. After evaluating the SCA's text, structure, purpose, and legislative history, as well as the scope of other federal statutes that regulate the disclosure of customer information by telecommunications companies,<sup>9</sup> the DOJ concluded in the white paper that the SCA does not prohibit such disclosures.

The DOJ further explained that it does "not believe that the SCA prohibits a provider of ECS or RCS to the public from sharing aggregated non-content data with governmental entities, as long as that aggregated data does not reveal information about a particular customer or subscriber. Reading the SCA to bar communications service providers from disclosing to the government all aggregated data related to

providing such services would effectively read out the limitation that the prohibition on disclosure does not cover all records or other information, but only those 'pertaining to a subscriber to or customer of such service.'"

Nevertheless, the DOJ qualified its opinion in the white paper to stress that, if aggregated information still contains granular details that pertain to particular subscribers or customers, the exemption described in the white paper would not apply and the SCA would prohibit such a disclosure to the government. As an example, the DOJ noted that an ECS or RCS provider could "report to a governmental entity an anomalous swell in certain types of internet traffic traversing its network or a significant drop in in Internet traffic, which could be harbingers of a serious cyber incident," but that this reporting would not be permitted if it contained "aggregated information about the total network traffic to or from a particular static IP address assigned to a customer . . . because that information would reveal facts about that particular customer."<sup>10</sup>

## Implications for Businesses

To a certain extent, the joint policy statement and white paper reflect the evolving cybersecurity risk management landscape. As the DOJ and FTC note in the statement, "some private-to-private cyber threat information sharing is taking place, both informally and through formal exchanges or agreements, such as the many sector-specific Information Sharing Analysis Centers (ISACs)

---

**Overly expansive views of what information is prohibited from voluntary disclosure could unnecessarily prevent the sharing of important information that would be used to enhance cybersecurity**

---

<sup>5</sup> DOJ, White Paper: Sharing Cyberthreat Information Under 18 USC §2702(a)(3), May 9, 2014, <http://www.justice.gov/criminal/cybercrime/docs/guidance-for-ecpa-issue-5-9-2014.pdf>.

<sup>6</sup> An ECS is defined to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15); *see id.* § 2711(1).

<sup>7</sup> An RCS is defined to mean "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

<sup>8</sup> *See* 18 U.S.C. § 2702(a)(1)-(3).

<sup>9</sup> Specifically, the DOJ reviewed the Telecommunications Act of 1996 and the Cable Communications Privacy Act of 1984, which permit the disclosure of non-identifiable, aggregate information, as well as decisions by other federal regulators to exclude aggregated data from information sharing prohibitions (e.g., the decision by the FTC to exclude aggregate data from the definition of personally identifiable financial information in its rulemaking under the Gramm-Leach-Bliley Act. *See* Privacy of Consumer Financial Information, 65 Fed. Reg. 33646 (May 24, 2000) ("An example in § 313.3(o)(2)(ii)(B) clarifies that aggregate information or blind data lacking personal identifiers is not covered by the definition of 'personally identifiable financial information.' The Commission agrees with those commenters who opined that such data, by definition, do not identify any individual.")).

<sup>10</sup> The white paper notes, however, that "determining when data does not pertain to a subscriber or customer will be a highly fact-specific inquiry. A provider of ECS or RCS to the public that is making disclosures of non-content/non-customer records to the government should seek legal guidance from its own counsel for specific disclosure determinations to ensure that it is acting consistent with the SCA."

Continued on page 9...



## FEDERAL AGENCIES REDUCE BARRIERS . . . *(continued from page 8)*

that have been established to advance the physical and cybersecurity of critical infrastructures.”<sup>11</sup> Likewise, the retail industry recently announced the development of a cybersecurity information sharing platform, developed in consultation with the Financial Services ISAC.<sup>12</sup> Further, the federal government, through efforts spearheaded by the White House, has pushed businesses in recent years to improve their defenses against cybersecurity threats, although administration and congressional efforts have generated concern in the businesses community about potential exposure to liability as a result of information sharing. The joint policy statement and white paper may alleviate some of these concerns, and hasten a more widespread adoption of the National Institute of Standards and Technology’s February 2014 cybersecurity framework by relevant industry stakeholders.<sup>13</sup>

Businesses that are contemplating how they may share information relating to cybersecurity risks should also be mindful of the potential that Congress may soon enact federal cybersecurity legislation. In late July,

---

**The federal government has pushed businesses to improve their defenses against cybersecurity threats, although efforts have generated concern in the business community about potential exposure to liability**

---

the Senate Intelligence Committee approved a draft bill, the Cybersecurity Information Sharing Act of 2014 (CISA) (S. 2588), that has significant bipartisan support.<sup>14</sup> Among other things, CISA would authorize companies to monitor their own computer networks and those of their consenting customers for cyber threats and to implement countermeasures to block those threats. CISA also would authorize businesses to engage in voluntary sharing of cyber threat information with each other and with the government. Under the current draft form of CISA, business would have a defense against liability for cybersecurity information sharing, provided that the information sharing: (i) follows procedures outlined in CISA; and (ii) is not grossly negligent or an act of willful misconduct. It remains to be seen whether CISA will become law, but it has the potential to further expand the ability of businesses to share risk intelligence with one another.


---

<sup>11</sup> See DOJ & FTC, Antitrust Policy Statement on Sharing of Cybersecurity Information 3.

<sup>12</sup> See National Retail Federation, National Retail Federation Announces Information-Sharing Platform, Apr. 14, 2014, <https://nrf.com/media/press-releases/national-retail-federation-announces-information-sharing-platform>.

<sup>13</sup> See National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0), Feb. 12, 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

<sup>14</sup> Similar legislation has been proposed in previous years, but failed to pass.



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.

# FTC ISSUES CARRIER BILLING RECOMMENDATIONS TO PROTECT CONSUMERS AGAINST MOBILE CRAMMING



**Sharon Lee**  
Associate, Palo Alto  
shlee@wsgr.com



**Lixian Hantover**  
Associate, Palo Alto  
lhantover@wsgr.com

On July 28, 2014, the Federal Trade Commission (FTC) issued a staff report on “mobile cramming”—the unlawful practice of placing unauthorized third-party charges on mobile phone accounts. The report recommended five best practices primarily directed to mobile carriers but at times also directed to merchants and billing intermediaries. This report follows a number of FTC enforcement actions to combat mobile cramming, as well as a May 2013 mobile cramming roundtable convened by the FTC and attended by industry participants, consumer advocates, and regulators. Following the roundtable, the four largest mobile carriers said that they would discontinue most “Premium SMS” billing, in which a consumer purportedly authorizes a third-party charge by texting a five or six-digit number. Nonetheless, the report emphasized that the consumer protection principles embodied in its recommendations apply to any form of carrier billing (i.e., charging a good or service directly to a mobile phone account), including direct carrier billing.

## Background

The FTC staff report explained that mobile cramming can occur when consumers are signed up and billed for a third-party service, such as a ringtone or recurring horoscope text messages, either without any affirmative action by the consumer or after the consumer takes an affirmative act without understanding that it will result in a charge to

the consumer’s mobile phone account. The report highlighted that many consumers do not notice third-party charges on their mobile phone bills for a number of reasons: the charges are often buried in their bill under vague terms such as “usage charges” or other terms that suggest a connection to the carrier; consumers may use automatic bill payment or have large amounts due on their bills; and in the case of pre-paid mobile phones, the consumers do not receive bills. As part of the report, the FTC staff surveyed not only its own actions addressing mobile cramming, but also federal and state initiatives addressing mobile cramming, carrier refund rates, complaint information, other efforts to estimate the extent of cramming, and international views.

## FTC Recommendations

To help protect consumers from mobile cramming, the FTC staff issued the following five recommendations:

1. *Consumers should have the right to block third-party charges.* The FTC staff recommends that upon activation of mobile phone accounts, consumers should be informed that third-party charges may be placed on their accounts and then be given the option to block all third-party charges. The FTC staff further recommends that while mobile phone accounts are active, consumers be given clear and prominent disclosures of this option. In addition, the report suggests that mobile carriers consider offering consumers the ability to block only specific providers or commercial providers.
2. *Advertisements for products or services charged to a consumer’s mobile account should not be*

---

**Mobile cramming can occur when consumers are signed up and billed for third-party service, either without any affirmative action or after the consumer takes an affirmative act without understanding that it will result in a charge to their account**

---

*deceptive.* The FTC staff recommends that before charging a consumer’s mobile phone account, merchants should clearly and conspicuously disclose information about price. Specifically, the report states that at a minimum, pricing information should be prominent, in a legible font and size and on the same page, and immediately next to a purchase button or other invitation for a consumer to agree to a charge for a product or service. Furthermore, the FTC staff recommends that carriers and billing intermediaries should implement reasonable procedures to scrutinize merchants that are risky or suspicious or that previously have run a campaign containing deceptive advertising or engaged in landline cramming. The FTC staff also recommends carriers and billing intermediaries to terminate or take appropriate action against companies engaging in unlawful practices.

*Continued on page 11...*

3. *Consumers must provide their express informed consent to charges before they are billed to their mobile accounts.* The report recommends that given the unreliability of merchants' claims that they have obtained consumer consent, carriers and intermediaries should maintain sufficient control over the consent process to address unauthorized charges. The report also suggests that carriers implement policies to investigate and take appropriate action when merchants may be cramming charges without consumers' consent, as indicated by consumer refund requests and complaints.

4. *All charges for third-party services should be clearly and conspicuously disclosed to consumers in a non-deceptive manner.* In order to help consumers understand what third-party service they are paying for, the report recommends that mobile phone bills should clearly and conspicuously disclose all charges for third-party services in a non-deceptive manner. According to the report, the mobile phone bill consequently should identify the third-party charges in relation to the third-party product or service offered and not suggest a carrier affiliation. Furthermore,

---

**Carriers should implement policies to investigate and take action when merchants may be cramming charges without consumers' consent, as indicated by consumer refund requests and complaints**

---

the report provides that billing intermediaries and merchants must provide accurate information to carriers for the purposes of these disclosures. Finally, the report recommends that third-party charges be made more conspicuous on mobile phone bills and that consumers who automatically pay their bills or use prepaid phone plans receive a notification from the carrier regarding these charges.

5. *Carriers should implement an effective dispute resolution process.* Carriers should implement a clear and

consistent process for consumers to dispute suspicious charges on their mobile phone bills and obtain refunds for unauthorized charges. The FTC staff recommends that like landline carriers, mobile carriers should allow consumers to withhold payment for disputed third-party charges during the dispute without a cut-off in phone service or an accrual of interest. When consumers do seek refunds, the report recommends that if a carrier concludes those charges were crammed, consumers could be granted refunds for the same charges in previous months. When a third party's billing activities are terminated for unauthorized charges, the report suggests that the carrier should notify consumers who incurred charges from that third party to allow them to request a refund.

**Conclusion**

The FTC will continue to monitor, investigate, and bring enforcement actions against industry participants involved in third-party mobile billing. Consequently, mobile carriers, merchants, and intermediaries who utilize carrier billing should consider how best to incorporate the five FTC staff recommendations into their policies and practices.



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.

© 2014 Wilson Sonsini Goodrich & Rosati, Professional Corporation. All rights reserved.