Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

JULY 2014

Welcome

In this issue of *Eye on Privacy*, we address some significant new data security legislation proposed in California, cover recent updates in FCRA enforcement, and take a timely look at policy recommendations regarding big data. We also examine a number of data protection opinions recently released by EU regulators, discuss new guidance from the FCC on text messaging, and consider the effect of the New Jersey district court's rulings in the FTC's case against Wyndham. In addition, we provide an overview of privacy and data security risk assessments, which have become an increasing area of interest to companies large and small.

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

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

Proposed California Law Would Impose Data Breach Liability on Retailers and Create More Stringent Data Security Requirements for Businesses

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

Jonathan Adams
Associate, Palo Alto
jadams@wsgr.com

A proposed California law, the Consumer Data Breach Protection Act (A.B. 1710),[1] has the potential to upend the calculus of determining liability after retail data breaches, create additional data security requirements for retailers and other consumer-facing businesses operating in California, and establish new standards for data breach reporting for breaches affecting California residents. The bill, introduced by California State Assemblymen Bob Wieckowski and Roger Dickinson in February 2014 and currently pending before the California Assembly Committee on the Judiciary, may in part represent an effort to respond to the recent data breaches affecting Target Corp. and Neiman Marcus Ltd., and aims to strengthen one of the most prescriptive state statutes already in existence.

The heightened concern over data privacy in recent months might enable the passage of the bill, which is a variation of past bills

Continued on page 2...

[1] "Consumer Data Breach Protection Act," California Assembly Bill 1710, 2013-2014 Cal. Leg. Session, *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710.

In This Issue

that were vetoed by former Governor Arnold Schwarzenegger.[2] If passed, A.B. 1710 would place California alongside Washington, Minnesota, and Nevada as the states mandating particular data security provisions with respect to payment card data,[3] and would increase the data breach reporting requirements and liability associated with breaches for entities doing business in California.

Data Breach Liability

In large part, A.B. 1710 has received considerable press attention because it has the potential to shift many of the costs associated with data breaches to retailers or other customer-facing businesses and away from financial institutions. A.B. 1710 would apply to any "person or business conducting business in California that owns or licenses computerized or noncomputerized data that contains personal information." Such businesses, which include large retailers, in many cases have already borne the burden of providing notice to affected consumers, but typically have not had responsibility for costs associated with issuing new credit or debit cards. Under A.B. 1710, these businesses would bear the costs for both components of a data breach response if they are the party responsible for the loss of data pertaining to California residents.

Under A.B. 1710, certain costs in data breach response would shift to customer-facing businesses, although card issuers and financial institutions would still maintain responsibility for covering certain losses arising from the use of stolen card data. First, consumer-facing businesses would carry the liability for reimbursement of "all reasonable and actual cost[s]" for providing notice following a data breach and for replacing the affected debit or credit cards. There is, however, a safe harbor that excuses this liability, in whole or in part, if the relevant business "can demonstrate compliance with specified provisions at the time of the breach." Second, consumer-facing businesses would also bear the responsibility for offering to provide "appropriate" identity theft prevention and mitigation services, such as credit monitoring, at no cost to potentially affected consumers for a period of not less than 24 months. Historically, many companies have opted to provide credit monitoring or similar services where the potential for harm to consumers existed; this approach would be mandatory, at least with respect to California residents, under A.B. 1710. It does not appear, however, that A.B. 1710 as drafted would alter the existing statutory liability scheme that allocates the cost to financial institutions for payments made on cards reportedly stolen or hacked; losses to consumers in such circumstances are capped at the federal level by the Fair Credit Billing Act (FCBA)[4] and the Electronic Funds Transfer Act (EFTA)[5] for credit cards and debit cards, respectively.

> Currently pending before the California Assembly Committee on the Judiciary, A.B. 1710 aims to strengthen one of the most prescriptive state statutes already in existence

Beyond the provisions concerning the reimbursement of costs, A.B. 1710 would authorize civil actions by affected individuals against businesses that suffer a data breach, and would permit public prosecutors to commence actions to recover a civil penalty of up to $500 per violation, or up to $3,000 per violation for willful, intentional, or reckless violations. These liability provisions apply broadly to the California data breach statute, and not simply to the provisions created under A.B. 1710. They have the potential to reinvigorate post-data breach litigation and could expose businesses to significant class action claims or prosecutions.

Enhanced Data Security Measures

A.B. 1710 also imposes more stringent requirements on retailers' data security practices. Under the bill in its current form, businesses that accept credit card, debit card, or other similar payment mechanisms would be prohibited from doing the following:

- Storing payment-related data, unless the business has in place—and follows—a data retention and disposal policy that limits the amount of data stored and the length of time for which such data is stored to the amount and time necessary for business, legal, or regulatory purposes as outlined in the policy
- Storing sensitive authentication data, even if encrypted; such data would include the full data track contents from a payment card or device, the card

---

[2] *See, e.g.,* Assemb. 779 Veto Message, 2007–2008 Leg., 2007–2008 Sess. (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_vt_20071013.html. A.B. 779 had received unanimous backing in the Assembly, but Governor Schwarzenegger cited PCI DSS standards and marketplace risk-allocation measures in vetoing the legislation. *See also* Dan Kaplan, "Schwarzenegger Shoots Down California Data-Protection Bill," *SC Magazine*, Oct. 15, 2007, http://www.scmagazine.com/schwarzenegger-shoots-down-california-data-protection-bill/article/57998/.

[3] *See* RCW Ch. 19.255 (Washington law incorporating concepts from PCI DSS for data security standards); Minn. Stat. § 325E.64 (Minnesota Plastic Card Security Act prohibiting retention of certain card data for more than 48 hours after authorization of a transaction); Nev. Rev. Stat. Ch. 603A (incorporating PCI DSS standards by reference for compliance with state law).

[4] Fair Credit Billing Act, Pub. L. No. 93-495 (as amended), codified at 15 U.S.C. § 1601 et seq.

[5] Electronic Funds Transfer Act, Pub. L. No. 95-630 (as amended), codified in scattered sections of 12 U.S.C. ch. 3 and 15 U.S.C. ch. 41.

verification code or similar value, and the personal identification number (PIN) or encrypted PIN block for a card

- Storing any sensitive information that is not needed for business, legal, or regulatory purposes
- Storing other sensitive payment-related data, including payment verification codes or values, PIN numbers, Social Security numbers, or driver's license numbers
- Retaining the primary account number associated with a payment mechanism, unless it is retained in compliance with the law and is stored in a form that is "unreadable and unusable" to unauthorized persons
- Sending payment-related data over open, public networks unless the data is encrypted using strong cryptography and security protocols, or is otherwise rendered indecipherable
- Failing to limit access to payment-related data to those employees whose job requires such access

Compliance with all of the above provisions would serve to excuse partial or full liability from costs associated with providing notice and issuing new credit or debit cards. As currently drafted, however, the retailer would still be responsible for the costs of consumer credit monitoring. Additionally, the requirements proposed by A.B. 1710 may come into conflict with existing requirements imposed on retailers by financial institutions and card issuers, including requirements to store payment data for certain purposes and authorization data to defend against chargebacks. Reconciling these rules will likely be an important part of the legislative process in which card issuers and financial institutions provide input to synchronize the requirements placed on consumer-facing businesses.

Other Provisions of A.B. 1710

In addition to the liability-shifting and retailer requirements described above, A.B. 1710 would limit actions that persons or businesses may take with respect to individuals' Social Security numbers. Existing law currently prohibits persons or entities, with few exceptions, from publicly posting or displaying Social Security numbers, or from taking other actions that might compromise the security of Social Security numbers, unless required by federal or state law. A.B. 1710 would prohibit anyone within California from selling, advertising for sale, or offering to sell an individual's Social Security number.

A.B. 1710 would also remove the encryption safe harbor from California's data breach notification statute. In its current form, disclosures of breaches must be made where "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[6] The word "unencrypted" would be removed under A.B. 1710, which would have the likely effect of increasing the number of reportable breaches in California.

Another minor change under A.B. 1710, but one with implications for entities that maintain paper documents, is the expanded scope of California's data breach notification law to include breaches implicating non-computerized data. Entities that experience a data breach are not currently obligated to provide notice relating to data breaches involving paper files; under A.B. 1710, notice would be required. If this proposed change comes into effect, companies that maintain physical copies of documents containing personally identifiable information should ensure that robust records management and destruction policies are in place to avoid a reportable breach involving those physical documents.

> The bill would expand the manner and timing in which a business must provide notice to affected California residents following a data breach

A.B. 1710 would also expand the manner and timing in which a business must provide notice to affected California residents following a data breach. Current law requires that any entity experiencing a breach must "disclose a breach of the security of the system following discovery or notification of the breach" and that "[t]he disclosure shall be made in the most expedient time possible and without unreasonable delay . . . ." A.B. 1710 proposes that entities provide notice "within 15 days of the breach," but does not remove the existing language regarding providing notice "in the most expedient time possible and without unreasonable delay." Thus, A.B. 1710 would likely require notification as soon as reasonably possible but in no event later than 15 days after the breach. A.B. 1710 provides mechanisms by which such notification must occur: (a) email notice if the entity has an email address on record for the affected individual; (b) conspicuous posting on the entity's website for at least 30 days; and (c) notification to "major statewide media."[7] As currently drafted, A.B. 1710 would require an entity experiencing a breach to engage in all three actions, and previously accepted

[6] Cal. Civ. Code § 1798.82.
[7] The term "major statewide media" is undefined by the bill.

Continued on page 4...

means of notice, including the mailing of letters to consumers, would not be deemed sufficient notice.

A.B. 1710 has received considerable press attention because it has the potential to shift many costs associated with data breaches to retailers or other customer-facing businesses and away from financial institutions

The Legislative Context

A.B. 1710 has drawn strong opposition from retailers and other consumer-facing businesses. California Retailers Association president Bill Dombrowski, whose organization represents nearly three million California workers (approximately one-fifth of the California workforce), argues that the bill "arbitrarily assesses financial penalties on the retailer" rather than allowing the affected parties to resolve the incident and allocate responsibility.[8] Dombrowski has stated that "it'll be a big fight, a tough fight" for the bill to be enacted.[9] It has been suggested that the California Retailers Association's opposition, along with lobbying from the Chamber of Commerce and Bankers Association, has played a role in the failure of previous bills.[10]

It is not clear, however, that the same coalition will oppose A.B. 1710, as banks and other financial institutions are increasingly being called to cover costs relating to large data breaches. Financial institutions are now in a place where their industry has called on lawmakers to develop more stringent standards for data security. Recently, as a result of steep losses following data breaches, credit unions have begun pushing for Congress to adopt stronger cybersecurity laws to mandate federal data security standards, joining other financial institutions and major technology firms in seeking to set federal baselines for data security.[11] Although A.B. 1710 would not remove all breach remediation costs from financial institutions and card issuers, it would likely be a boon to financial institutions that have suffered losses as a result of reissuing cards where breaches exposed credit card or debit card data. This would be particularly true if other states followed California's example, as has occurred previously with data breach notification and other data-security-related laws.

The introduction of A.B. 1710 also comes at a time when California has aggressively sought to protect the privacy and data security of its residents. In February, the Office of Attorney General Kamala Harris issued a report, entitled "Cybersecurity in the Golden State,"[12] focused on improving business data security protections and enhancing responses to malware, data breaches, and other information security risks. According to the report, the Office of the Attorney General received reports of 131 data breaches affecting an aggregated 2.5 million Californians in 2012, half of which may have been preventable if companies had used stronger or stricter encryption procedures when transmitting information.[13] Attorney General Harris has also begun a stronger enforcement effort relating to data security and privacy, and the California Department of Justice now staffs a Privacy Enforcement and Protection Unit dedicated to privacy education and enforcement.

[8] *See* Kira Lerner, "Calif. Bill Would Make Retailers Liable in Data Breaches," Law360.com, Apr. 7, 2014.
[9] *See* Marc Lifsher, "Making Retailers Liable for Damages from Hacking," *Los Angeles Times*, Apr. 6, 2014.
[10] *See* Kaplan, "Schwarzenegger Shoots Down California Data-Protection Bill."
[11] *See, e.g.,* Andrew Ramonas, "Make Cybersecurity Laws a Priority, Credit Unions Plead," *Corporate Counsel*, Apr. 21, 2014.
[12] California Office of Attorney of General, Cybersecurity in the Golden State, Feb. 2014, *available at* https://oag.ca.gov/cybersecurity.
[13] *Id.*

Tip

Have you completed your U.S.-EU Safe Harbor self-certification this year? Participating companies are required to renew their certifications annually to the U.S. Department of Commerce.

FTC Continues Its Aggressive FCRA Enforcement and Ninth Circuit Lowers Standing Threshold in FCRA Cases

Wendell Bartnick
Associate, Washington, DC
wbartnick@wsgr.com

Data may well be *the* asset of the 21st century, but selling access to certain data about individuals may raise the risk of attracting unwanted attention from both regulators[1] and class action litigants. As organizations collect more types of data about consumers, they are more likely to have data that may constitute "consumer report" data under the Fair Credit Reporting Act (FCRA).[2] Organizations that try to monetize such data by selling access to consumer profiles can easily run afoul of the FCRA.

This article discusses recent Federal Trade Commission (FTC) enforcement actions against two background check companies that allegedly failed to avoid the FCRA trip wires and face a combined $1.5 million in fines.[3] The FTC aggressively enforces the FCRA and violations commonly occur due to a failure to create and implement adequate policies and procedures. This article also explains how the U.S. Supreme Court may review the Ninth Circuit's recent decision to join other federal appellate courts in making FCRA class action lawsuits easier to bring for plaintiffs. Given the appellate courts' interpretations of the FCRA, plaintiffs likely will increasingly make FCRA claims in an effort to obtain compensation for alleged general privacy violations. Any organization that sells access to data profiles about individuals is advised to determine whether it must comply with the FCRA and, if necessary, implement policies and procedures that meet the FCRA's requirements.

Fair Credit Reporting Act

Under the FCRA, a company is a "consumer reporting agency" (CRA) and has certain obligations if it assembles or evaluates information about individuals for the purpose of selling "consumer reports" to third parties.[4]

"Consumer Reports." There are two requirements that must be met before information constitutes a credit report.[5] First, the information must contain certain categories of data, i.e., data relating to credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. Second, the information must be used for the particular purpose of establishing eligibility for employment, housing, credit, or insurance, or other similar purposes. Therefore, to determine whether information constitutes a credit report, one must review the type of information and the use of the information.

Possible Consumer Reports in the Employment Context. The FCRA defines a consumer report used for "employment purposes" as "a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee."[6] Regulators and courts may conclude that consumer reports include employment screening reports about the prior work experience of job applicants, information in employment records, and information about education and licenses.[7]

CRAs' Obligations Under the FCRA. The FCRA imposes several obligations on CRAs. Generally, a CRA must have procedures in place to ensure that it provides the information in a consumer report only to permitted third parties.[8] For example, a CRA may provide a consumer report pursuant to a valid legal request, with a consumer's consent, or to a third party that intends to use the information in connection with a credit transaction, employment, insurance underwriting, license eligibility, or other legitimate business related to a transaction initiated by the consumer.[9] The FCRA requires a CRA to follow reasonable procedures to ensure the maximum possible accuracy of the information it provides in a consumer report and follow certain procedures for responding to a consumer's dispute over the accuracy of such information.[10] A CRA must also ensure that certain information is not included in a consumer report, e.g., old civil and criminal court records and other adverse items.[11] Finally, a CRA must provide notice to any furnishers of information contained in the consumer report and any recipient of the report about their responsibilities under the FCRA.[12]

---

[1] *Eye on Privacy*, "Policing Privacy: Undercover FTC Staff 'Test-Shop' Data Brokers to Identify FCRA Violators" (Sept. 2013), *available at* http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Sep2013/index.html#5.
[2] 15 U.S.C. § 1681 *et seq.*
[3] *United States v. Instant Checkmate, Inc.*, No. 14CV0675H (S.D.Cal. March 28, 2014); *United States v. InfoTrack Information Services, Inc.*, No. 14-cv-2054 (N.D.Ill. March 25, 2014). This follows a January 2014 enforcement action against TeleCheck Services, Inc. that carried a $3.5 million fine.
[4] 15 U.S.C. § 1681a (f).
[5] 15 U.S.C. § 1681a (d).
[6] 15 U.S.C. § 1681a (h).
[7] Federal Trade Commission, "40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations," *available at* http://www.ftc.gov/os/2011/07/110720fcrareport.pdf.
[8] 15 U.S.C. § 1681e.
[9] 15 U.S.C. § 1681b.
[10] 15 U.S.C. § 1681b, i.
[11] 15 U.S.C. § 1681c.
[12] 15 U.S.C. § 1681e (d).

Continued on page 6...

FTC Continues Its Aggressive FCRA Enforcement . . . *(continued from page 5)*

FCRA Obligations when CRAs Provide Consumer Reports for Employment Purposes. A CRA may provide consumer reports for employment purposes only to a third party that provides proper disclosures and obtains consent from the consumer about whom the information pertains. The third party must also certify that it will not use the information in violation of equal employment opportunity laws.[13] The FCRA requires that when a consumer report contains negative public-record information, the CRA must provide notice to the consumer at the time of providing notice to a third party and maintain procedures to keep such public-record information up to date.[14]

Potential Consequences of Noncompliance. Federal and state regulators may bring actions against alleged FCRA violators.[15] A consumer may also sue a CRA for willful or negligent noncompliance with the FCRA.[16] For willful noncompliance, the FCRA states:

> Any person who willfully fails to comply with any requirement imposed under [the FCRA] with respect to any consumer is liable to that consumer in an amount equal to the sum of—
>
> (1)(A) any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000; . . .[17]

Recent Federal Trade Commission Enforcement Actions

The FTC regularly investigates organizations that it considers to be CRAs when they do not seem to follow procedures to provide the proper notices, perform necessary diligence on data recipients, or perform required diligence to ensure the consumer report data is accurate.

Two Alleged CRAs. According to the FTC's complaint, InfoTrack sold background screening reports containing public information to employers so they could make decisions about hiring and other employment-related issues. Similarly, the FTC alleged that Instant Checkmate sold background reports pulled from public records and advertised them for use to establish a person's eligibility for employment or housing. As such, the FTC concluded that InfoTrack and Instant Checkmate were CRAs that provided consumer reports to their customers and had FCRA obligations.

> Organizations that try to monetize data by selling access to consumer profiles can easily run afoul of the FCRA

Alleged Noncompliant Practices. Both InfoTrack and Instant Checkmate allegedly knowingly failed to follow FCRA-compliant procedures in a way that constituted a pattern or practice. The complaint stated that Instant Checkmate failed to perform diligence on the recipients of the reports to ensure the recipients took reasonable steps to identify themselves to Instant Checkmate, certified the purpose for which the information was sought, and certified that the information would be used for no other purpose. Instant Checkmate allegedly furnished the reports to recipients who did not have a proper purpose. The FTC alleged that InfoTrack and Instant Checkmate failed to follow reasonable procedures to ensure the maximum possible accuracy of consumer report information. Both InfoTrack and Instant Checkmate also allegedly failed to provide notice to the recipients of the reports that stated their responsibilities under the FCRA. Moreover, InfoTrack did not provide required data furnisher notices to the third parties from whom it received information, and it did not notify consumers that public-record information about them was provided to employers, according to the complaint.

Given the knowing FCRA violations, the financial penalties are potentially higher. Both defendants agreed to significant financial judgments: $1 million for InfoTrack and $525,000 for Instant Checkmate. The defendants also agreed not to violate certain FCRA requirements or they risk additional penalties under the order.

These enforcement actions highlight the many ways an unwary seller of data can violate the FCRA if it is selling data that could be deemed a consumer report. They also demonstrate the severity of the penalties.

Class Action Against Spokeo

Online data aggregator Spokeo similarly agreed to an FTC consent order for its alleged failure to comply with the FCRA.[18] The company also has been involved in a class action lawsuit that may make its way to the U.S. Supreme Court. On May 1, 2014, the company filed a petition for a writ of certiorari in the Supreme Court[19] to review the Ninth Circuit's decision to join other federal

[13] 15 U.S.C. § 1681b.
[14] 15 U.S.C. § 1681k.
[15] 15 U.S.C. § 1681s.
[16] 15 U.S.C. § 1681n, o.
[17] 15 U.S.C. § 1681n (a)(1)(A).
[18] Press Release, Federal Trade Commission, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA" (June 12, 2012), *available at* http://www.ftc.gov/opa/2012/06/spokeo.shtm.
[19] Petition for Writ of Certiorari, *Spokeo, Inc. v. Robins*, No. 13-1339 (May 1, 2014).

The FTC regularly investigates organizations that it considers to be CRAs when they do not seem to follow procedures to provide the proper notices or perform necessary diligence

appellate courts to hold that class action claims may be viable under the FCRA without proof of actual damages to the plaintiffs.[20] Thus, the FCRA may prove to be attractive for a plaintiffs' bar looking for ways around the obstacle of difficult-to-prove damages in privacy cases.

Spokeo provides a search engine that finds information about people. It collects and displays publicly available information about individuals from sources like telephone books, real estate listings, government records, and social networking websites. Spokeo provides notice on its web pages, pop-up windows, and within its terms of use stating that it does not verify the information it collects and displays, that it is not a CRA, and that it is not providing the information for FCRA-related purposes. However, these actions did not prevent a class action lawsuit from being filed.

Class Action Complaint. The plaintiff filed a class action lawsuit alleging that Spokeo is a CRA that willfully failed to comply with the FCRA. He claimed that despite the notices on its website, Spokeo marketed its services to human resource professionals and persons and entities performing background checks. In particular, he alleged that Spokeo failed to provide required notices to furnishers and recipients about their FCRA obligations. Further, the plaintiff alleged that Spokeo failed to ensure that the information provided to recipients was accurate and that the recipients complied with their FCRA disclosure obligations. He alleged that the inaccurate information provided on Spokeo's website "will affect his ability to obtain credit, employment, insurance, and the like," particularly because "he is currently out of work and seeking employment."

Trial Court Dismisses the Case. As in many other privacy cases, the trial court dismissed both the complaint and the amended complaint on the grounds that the plaintiff failed to meet Article III standing requirements when he did not adequately allege an injury-in-fact. The trial court concluded that the plaintiff's concern that the information on the Spokeo website could affect his employment prospects was not an actual or imminent harm adequate to constitute an injury-in-fact. In a rare occurrence, the trial court first concluded that the plaintiff had adequately met the standing requirements in the amended complaint, but subsequently reversed itself and dismissed the case. The indecision of the trial court exemplifies courts' challenges with standing in privacy cases. Courts have been struggling with and inconsistently analyzing the standing issue in privacy cases where the harm to the plaintiff is unclear.

Ninth Circuit Reverses Trial Court and Rules the Lawsuit May Continue. The Ninth Circuit reversed the trial court and concluded that the plaintiff has standing under the FCRA due to the act's peculiar wording.[21] Normally, for plaintiffs to meet standing requirements, they must adequately allege an injury-in-fact that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[22] As discussed in a prior article, the United States Supreme Court recently seemed to make meeting the injury-in-fact threshold more difficult.[23] Under the Ninth Circuit's holding in this case, however, standing has become a much easier threshold to cross in FCRA cases.

Ninth Circuit Holds That No Actual Damages Are Necessary to Sue Under the FCRA in Certain Circumstances. According to the Ninth Circuit, the FCRA does not require a showing of actual harm when a plaintiff sues for willful violations. The Ninth Circuit interpreted the damages portion of the statute such that a consumer can sue for (1) actual damages or (2) damages between $100 and $1,000 when a defendant willfully violates the FCRA. The Ninth Circuit concluded that the FCRA created a private cause of action for consumers to enforce their statutory rights, and a willful violation of

The FCRA may prove to be attractive for a plaintiffs' bar looking for ways around the obstacle of difficult-to-prove damages in privacy cases

[20] *Robins v. Spokeo, Inc.*, No. 11-56843 (9th Cir. Feb. 4, 2014). *See also Beaudry v. TeleCheck Servs., Inc.*, 579 F.3d 702, 705-07 (6th Cir. 2009); *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 952-43 (7th Cir. 2006).

[21] *Robins v. Spokeo, Inc.*, No. 11-56843 (9th Cir. Feb. 4, 2014).

[22] *Clapper v. Amnesty Int'l USA*, 568 U.S. _____, 133 S. Ct. 1138 (2013).; *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. ___, 130 S.Ct. 2743, 2752 (2010).

[23] See our *Eye on Privacy* article discussing the case, titled "*Clapper v. Amnesty International USA*: The U.S. Supreme Court Strengthens Defendants' Shield Against Privacy Class Actions" (May 2013), at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/May2013/index.html#4.

Continued on page 8...

FTC Continues Its Aggressive FCRA Enforcement . . . *(continued from page 7)*

those rights is a sufficient injury-in-fact to confer standing. Thus, plaintiffs have standing even without suffering actual damages as long as they claim that the defendant willfully violated the FCRA.

The Ninth Circuit's conclusion seems to be consistent with holdings in the Sixth and Seventh Circuits where those courts also allowed class action lawsuits to continue without sufficient allegations of actual damages when the plaintiffs alleged that the defendants willfully violated the FCRA.[24] Now, the U.S. Supreme Court will have an opportunity to weigh in.[25]

> Defending cases on the merits is expensive, and many class actions settle after a defendant loses on the motion to dismiss

Implications

Is Your Organization a CRA and Does It Provide Consumer Reports? The FCRA risk has increased for organizations that gather and sell access to data about individuals. If your organization sells consumer data, now is a good time to assess whether it may be a consumer reporting agency under the FCRA. To comply with the FCRA, your organization will need to implement policies and procedures that govern how it collects consumer data, provides consumer report data, and provides notice to the data subjects, data furnishers, and data recipients. Failure to correctly determine whether FCRA compliance is necessary and to implement required policies and procedures may be costly, as the FTC's actions show.

Has the Standing Requirement Been Eviscerated in FCRA Class Action Cases? FCRA class action litigation likely will be on the rise. In three circuits, plaintiffs in FCRA cases seem to be able to bypass most of the difficult-to-achieve standing requirements at issue in many privacy cases. Plaintiffs must still allege that their individual statutory rights under the FCRA have been violated and that the claims meet the standards of causation and redressability. However, in the Ninth Circuit, at least, these prongs are usually met by plaintiffs alleging willful violations of the FCRA that directly affect them.

Class Suitability and Merits Arguments Remain. After passing the standing threshold, plaintiffs still must meet class certification requirements. Moreover, meeting standing requirements does not factor into the assessment of whether a defendant actually violated the FCRA. Therefore, defendants may have valid legal arguments to make on the merits. Defendants can argue that they are not CRAs and that they do not provide consumer reports. They can also argue that they did not "willfully" violate the FCRA. However, defending cases on the merits is expensive, and many class action cases settle after a defendant loses on the motion to dismiss. Therefore, the number of class action litigants alleging FCRA violations likely will increase.

Does the Same Legal Conclusion Apply to Violations of Other Privacy Laws? The FCRA language granting individuals damages even without allegations of actual harm is uncommon. Normally, tort claims and alleged statutory violations require allegations of actual harm to meet standing requirements. Therefore, courts likely will continue to dismiss most privacy cases where plaintiffs do not adequately allege actual harm. However, enterprising plaintiffs will undoubtedly allege FCRA violations when possible to take advantage of the diminished standing threshold.

To alleviate FCRA-related risk, organizations that sell consumer data are advised to assess whether they may be considered consumer reporting agencies under the FCRA. If the organization believes it may be a CRA, it can implement the policies and procedures necessary to ensure compliance with the FCRA.

---

[24] *Beaudry v. TeleCheck Servs., Inc.*, 579 F.3d 702, 705-07 (6th Cir. 2009) (holding that the FCRA "permits a recovery when there are no identifiable or measurable actual damages" when the information in the defendant's systems contained allegedly false and negative information about the plaintiff); *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 952-43 (7th Cir. 2006) (holding that the FCRA "provide[s] for modest damages without proof of injury").

[25] The U.S. Supreme Court previously declined to hear the similar FCRA case coming out of the Sixth Circuit. The Supreme Court was not asked to hear the FCRA case in the Seventh Circuit.

President's Counselor Makes Recommendations on Privacy and Other Values in Big Data Age

Lydia Parnes
Partner, Washington, DC
lparnes@wsgr.com

Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

In January 2014, President Barack Obama charged his counselor John Podesta with looking at: (a) how the challenges inherent in big data are being confronted in the public and private sectors; (b) whether the United States can forge international norms on how to manage big data; and (c) how the United States can continue to promote the free flow of information in ways that are consistent with both privacy and security. Two reports were published on May 1, 2014, in response to this charge, one focusing on policy and big data (the "Policy Report")[1] and the other complementing and informing the Policy Report with a focus on technology and big data (the "Technology Report").[2]

Both reports acknowledge that there is no one definition of "big data." However, big data is differentiated from data historically collected about individuals ("small data"[3]) in two ways: big data's quantity and variety, as well as the scale of analysis that can be applied to big data. And, while both reports view big data as potentially providing great benefits to the economy, society, and individuals, they also identified its potential to cause significant harm.

Based on the premise of embracing big data while protecting fundamental values such as privacy, fairness, and self-determination, the Policy Report makes recommendations in the following five areas: (1) preserving privacy values; (2) robust and responsible education; (3) anti-discrimination; (4) law enforcement and security; and (5) data as a public resource. The Policy Report elevates six of its recommendations, which are described in more detail below, as deserving prompt White House attention and development.

Preserving Privacy Values

Advancing the Consumer Privacy Bill of Rights. The Policy Report urges the prompt re-examination of the Consumer Privacy Bill of Rights in light of the novel privacy implications presented by big data. Specifically, the Policy Report recommends considering whether the notice and consent framework (which focuses on obtaining user permission prior to collecting data) has found its practical limit in big data and should be supplemented or replaced by a responsible-use framework. A responsible-use framework focuses on how data is used and consequently, according to the Policy Report, "holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection." The Policy Report also asserts that a responsible-use framework "shifts the responsibility [for privacy] from the individual, who is not well equipped to understand or challenge consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data."

Passing National Data Breach Legislation. Rather than using a patchwork of 47 state laws that govern when and how the loss of personally identifiable information must be reported, the Policy Report urges passing one national data breach standard that imposes reasonable time periods for notification, minimizes interference with law enforcement investigations, and potentially prioritizes notification about large, damaging incidents over less significant incidents. To support this recommendation, the Policy Report highlights individuals' right to know if the increasing amount of information collected about them has been stolen or improperly exposed.

Extending Privacy Protections to Non-U.S. Persons. The Policy Report asserts that because privacy is a worldwide value, privacy policies should be applied to non-U.S. persons where practicable or alternative privacy policies should be established that apply appropriate and meaningful protections to personal information regardless of a person's nationality.

Additional Privacy Recommendations. To protect privacy values, the Privacy Report makes four additional recommendations on a less urgent basis:

> While the reports view big data as potentially providing great benefits to the economy, society, and individuals, they also identified its potential to cause significant harm

[1] The Policy Report, *Big Data: Seizing Opportunities, Preserving Values*, available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[2] The Technology Report, *Big Data and Privacy: A Technological Perspective*, available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.
[3] The Technology Report defines small data as "the collection and use of data sets by private and public sector organizations where the data are disseminated in their original form or analyzed by conventional statistical methods." The Technology Report, page ix.

Continued on page 10...

President's Counselor Makes Recommendations . . . *(continued from page 9)*

- Data brokers and the data services industry generally should be more transparent to consumers about how their data is collected, shared, and reused. Specifically, they should "follow the lead of the online advertising and credit industries and build a common website or online portal that lists companies, describes their data practices, and provides methods for consumers to better control how their information is collected and used or to opt-out of certain marketing uses."

- Consumers should have stronger "Do Not Track" tools that help them control when and how their data is collected, given the growing array of technologies available for data collection.

> How personal data is collected, shared, and used should be considered an essential skill in K-12 education and integrated into the curriculum

- The government should lead a consultative process to assess how the Health Insurance Portability and Accountability Act[4] and other laws can best accommodate medical advances and healthcare cost reductions that big data can enable, including whether and how to regulate personal health information held by entities that are not currently regulated under such laws.

- The United States should lead international conversations on big data that reaffirm its commitment to interoperable global privacy frameworks, including to promote collaboration on data flows between the United States, Europe, and Asia.

Robust and Responsible Education

Ensuring Data Collected on Students in School Is Used for Educational Purposes. The Policy Report urges the federal government to not hamper innovation in educational technology, while simultaneously ensuring that data collected in schools or another educational context is used for educational purposes and not for inappropriate purposes. The Policy Report describes such an inappropriate purpose as building "extensive profiles about students' strengths and weaknesses that could be used to their disadvantage in later years." Specifically, the Policy Report calls for the privacy regulatory framework under the Family Educational Rights and Privacy Act[5] and Children's Online Privacy Protection Act[6] to be modernized with these considerations in mind.

Additional Education Recommendation. In furtherance of robust and responsible education, the Privacy Report less urgently recommends teaching how personal data is collected, shared, and used as an essential skill in K-12 education, and for such teaching to be integrated into the standard curriculum.

> To ensure the responsible use of big data in law enforcement, the protection for digital content should be consistent with that in the physical world

Anti-discrimination

Expanding Technical Expertise to Stop Discrimination. To help prevent discrimination that big data may enable, the Policy Report urges the federal government to expand its technical expertise to include the ability to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and to develop a plan for investigating and resolving violations of law.

Additional Anti-discrimination Recommendations. The Policy Report also makes two less urgent recommendations to help prevent discrimination enabled by big data:

- New practices may be needed to ensure fairness for consumers, who should know whether prices they are offered are systematically different from prices offered to others, particularly in unexpected situations.

---

[4] The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, was implemented through the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), 45 CFR Part 160 and Part 164, Subparts A and E. The Privacy Rule covers the use and disclosure of health information by organizations subject to the Privacy Rule and sets standards for individuals to understand and control how such health information is used. For more information, see the WSGR Alert, *HIPAA Omnibus Rule Compliance Deadline*, available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-HIPAA-omnibus-rule.htm.

[5] The purpose of the Family Educational Rights and Privacy Act it to protect the privacy of student "education records." See 20 U.S.C. § 1232g; 34 CFR Part 99.

[6] The Children's Online Privacy Protection Act of 1998 and the Federal Trade Commission's implementing regulations require online services that collect information from children under the age of 13 to provide detailed notice to parents about the information being collected and its uses, and to obtain parents' verifiable consent prior to collecting, using, or disclosing personal information from such children. For more information, see the WSGR Alert, *FTC Releases Final Amendments to Children's Online Privacy Protection Rule*, available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-COPPA-final-amendments.htm.

- Government and private civil rights defenders should apply big data technologies to their advantage by using them to identify and empirically confirm instances of discrimination and characterize the harms they caused.

The reports demonstrate the White House's continuing attention to privacy issues, but shift attention—although not yet the compliance burden—from collection to responsible use

Law Enforcement and Security

Amending the Electronic Communications Privacy Act (ECPA). To ensure the responsible use of big data in law enforcement and security, the Privacy Report urges Congress to amend the ECPA[7] to make protection for digital content consistent with that in the physical world, "including by removing archaic distinctions between email left unread or over a certain age."

Additional Recommendations. The Privacy Report makes five less urgent recommendations for ensuring big data's responsible use in law enforcement, public safety, and national security:

- The use of predictive analytics by law enforcement should continue to be subject to careful policy review, as well as protections for individual privacy and civil liberties.
- Federal agencies with expertise in privacy and data practices should provide technical assistance to other agencies seeking to deploy big data techniques.
- Government use of lawfully acquired commercial data should be evaluated to ensure consistency with values. Particularly, services that employ big data techniques should incorporate appropriate oversight and protections for privacy and civil liberties.
- Federal agencies should implement best practices for institutional protocols and mechanisms that can help ensure the controlled use and secure storage of data. Particularly, data tagging to enforce usage limitations, controlled access policies, and immutable auditing should be evaluated for integration into databases and data practices to provide built-in protections for privacy, civil rights, and civil liberties.
- Big data analysis and information sharing should be used to strengthen cybersecurity.

Data as a Public Resource

The Privacy Report has three less urgent recommendations for harnessing data as a public resource:

- Government data should be accurate and securely stored, and to the maximum extent possible, open and accessible.
- All departments and agencies should, in close coordination with their senior privacy and civil liberties officials, examine how they might best harness big data to help carry out their missions.
- The country should dramatically increase investment for research and development in privacy-enhancing technologies, encouraging cross-cutting research that involves not only computer science and mathematics, but also social science, communications, and legal disciplines.

Conclusion

These reports demonstrate the White House's continuing attention to privacy issues, but shift attention—although not yet the compliance burden—from collection (including notice and consent for collection and focused collection) to responsible use.

Companies should prepare to participate in processes proposed by the Policy Report or adapt to the greater focus on responsible usage that may be necessary if new standards emerge, including the possibility of new federal legislation.

[7] The ECPA was enacted in 1986 to protect wire, oral, and electronic communications in transit from interception, as well as communications in electronic storage from unauthorized access. See 18 U.S.C. §§ 2510-2522.

EU Data Protection Regulators Issue Several Opinions on Key EU Data Protection Issues

Christopher Kuner
Senior Of Counsel, Brussels
ckuner@wsgr.com

Cédric Burton
Of Counsel, Brussels
cburton@wsgr.com

The body of European data protection regulators known as the Article 29 Working Party (WP29) has been exceptionally prolific lately. In April 2014, WP29 adopted no less than five opinions and issued a number of other statements and letters on various topics. While not directly binding, WP29's publications offer insight into the regulators' views, which are generally a good indication of how the regulators will seek to apply the law.

In this article, we provide an overview of the most important documents issued. We discuss Opinion 5/2014 on anonymization,[1] Opinion 6/2014 on legitimate interests as a basis for processing,[2] the letter to Commissioner Viviane Reding on data transfers from the EU to the U.S.,[3] and the letter to the Council of the EU on the one-stop-shop mechanism.[4]

Opinion on Anonymization Techniques

The opinion[5] stresses the difficulty of creating truly anonymous datasets under EU data protection law and provides recommendations on good anonymization practices. It is quite technical and goes into the details of selected anonymization techniques such as randomization and generalization (including certain forms of those techniques). The main takeaways from the opinion are as follows:

1. The threshold for effective anonymization in the EU is high, as it requires that re-identification of an individual by the data controller *or any third party* (e.g., recipient or attacker) is excluded.

2. Whether the data is actually anonymized requires a case-by-case analysis taking into account the available technology, the risks for individuals, and contextual elements.

3. All anonymization techniques have advantages and disadvantages (such that the best solution is a combination of multiple techniques) and should be assessed in light of the following three criteria:

   i. When is it possible to identify an individual?

   ii. When is it possible to link records that relate to an identified individual?

   iii. When can information be inferred concerning an identified individual?

4. Pseudonymization (i.e., replacing a unique attribute in a record with another) is not a method of anonymization; rather, it is a security measure that makes it harder to link back to an individual. Therefore, EU data protection law continues to apply to pseudonymized data. WP29 lists some commonly used pseudonymization techniques such as encryption, hash function, and tokenization.

5. The use of anonymized datasets can still present residual risks to individuals (e.g., use anonymized statistics to enrich existing profiles) and requires regular risk evaluations, controls, and monitoring.

> WP29's publications are generally a good indication of how the regulators will seek to apply the law

Opinion on Legitimate Interest as a Legal Basis

The opinion[6] aims to clarify one of the key provisions of EU data protection law: Article 7(f) of the Data Protection Directive, which is often called the "legitimate interest" legal basis. This opinion is actually one of the most awaited and longest opinions from WP29. Under EU data protection law, a data controller must rely on a legal basis to legitimize the processing of personal data. Several grounds exist and are restrictively listed in Article 7 of the Data Protection Directive. Article 7(f) is one of them and legitimizes the processing of personal data when the "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject […]."

As an introduction, WP29 clarifies that reliance on legitimate interest legal basis requires a case-by-case analysis and should

[1] Article 29 Working Party, Opinion 05/2014 on "Anonymization Techniques onto the web" (WP216).
[2] Article 29 Working Party, Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (WP217).
[3] Article 29 Working Party, Letter from the Article 29 Working Party to Vice President Viviane Reding on the actions set out by the European Commission in order to restore trust in data flows between the EU and the U.S.
[4] Article 29 Working Party, Letter from the Article 29 Working Party to Lilian Mitrou, Chair of the Council's Working Party on Information Exchange and Data Protection (DAPIX), on the One-Stop-Shop mechanism, and Annex 1: Statement of the WP29 - Main points for a one-stop-shop and consistency mechanism for businesses and individuals.
[5] Article 29 Working Party, Opinion 05/2014 on "Anonymization Techniques onto the web" (WP216).
[6] Article 29 Working Party, Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" (WP217).

> The opinion stresses the difficulty of creating truly anonymous datasets under EU data protection law

not be treated as a "last resort" for rare or unexpected situations where other legal bases are deemed not to apply. In addition, that legal basis should not be automatically chosen with the thought that it is less constraining than other legal bases.

Further, WP29 explains how to apply the legitimate interest legal basis in practice and that this legal ground requires a balancing test. The purpose of the balancing test is to review the interest of a controller (or of a third party) and to balance it with the rights and freedoms of the data subject, while taking into consideration the following:

1. The nature and source of legitimate interest of the controller or third party, and whether the processing is necessary for the exercise of a right by the controller

2. The impact on individuals and their reasonable expectations about what will happen to their data

3. Additional safeguards (e.g., data minimization, opt-out mechanism, transparency, data aggregation and anonymization, privacy-enhancing technologies, privacy by design, or privacy impact assessments)

In addition, WP29 recommends considering the following factors when conducting the balancing of interest test: the sensitivity of the data; the possible prejudice suffered by the controller or third parties if the data processing does not take place; the status of the individual (e.g., minor or employee) and of the controller (e.g., market shares); and the way in which the data will be processed (e.g., large-scale processing, data mining, profiling, disclosure to a large number of people, or publication).

Finally, WP29 provides a large number of scenarios where the legitimate interest can be used as a legal ground (however, without making determinations as to whether the rights of individuals or data controllers would prevail): direct marketing and advertisement; freedom of expression or information, including in the media; prevention of fraud, misuse of services, or anti-money laundering; employee monitoring for safety or management purposes; whistleblowing schemes; physical security, IT security, and network security; processing for historical, scientific, or statistical purposes; processing for research purposes (including marketing research).

EU-U.S. Data Transfers

On April 10, 2014, WP29 sent a letter to Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship,

> If the one-stop-shop mechanism is enacted, there will be one data protection authority responsible for all processing activities of a company at a pan-EU level

on the European Commission's 13 recommendations to rebuild trust in EU-U.S. data transfers[7] following the revelations of intelligence collection programs. WP29 welcomes the commission's initiatives but also voices some criticisms and makes further recommendations.

According to WP29, the U.S.-EU Safe Harbor program should be suspended if the European Commission's revision efforts "[do] not lead to a positive outcome." Such an outcome cannot be reached without improving the safeguards provided by safe harbor. To that end, WP29 makes a large number of recommendations relating to, among other things, applicable law, transparency, redress, fees, access by U.S. authorities, choice, access, onward transfer, security, proportionality, and accountability. It is unlikely that the European Commission will be able to incorporate all of WP29's recommendations and concerns, but this illustrates the current thinking of EU regulators regarding the future of the U.S.-EU Safe Harbor framework.

The One-Stop-Shop Mechanism

On April 16, 2014, WP29 issued a short statement supporting a compromise between the current positions in the Council Working Group on Data Protection on the one-stop-shop and the consistency mechanisms. The one-stop-shop and consistency mechanisms are two of the key principles that will likely be included in the future EU data protection legal framework.

In a nutshell, if the one-stop-shop mechanism is enacted, there will be one data protection authority responsible for all processing activities of a company at a pan-EU level. The consistency mechanism would provide the rules regarding how authorities must cooperate among themselves. These concepts and their exact scope have been at the center of intense discussions among the EU institutions involved in the legislative process,

[7] European Commission, Rebuilding Trust in EU-US data flows (COM(2013) 846 final), November 27, 2013.

Continued on page 14...

EU Data Protection Regulators . . . *(continued from page 13)*

including the EU data protection authorities, and are still highly debated. The statement describes what WP29 considers to be effective one-stop-shop and consistency mechanisms and will certainly be taken into account in the upcoming political discussions.

Conclusion

It has been a busy time for WP29 and EU privacy practitioners keeping up with the various developments in EU data protection law. The opinions on anonymization and legitimate interest are key documents under EU data protection law and will certainly prove useful for companies seeking to comply with EU data protection law. However, it remains to be seen how these opinions can actually be applied in practice, as they set the bar extremely high.

The letter on the EU-U.S. data flows and the one-stop-shop mechanism touches upon several difficult issues and makes important recommendations, but it is unclear whether the European Commission will be able to incorporate all of the WP29 demands when negotiating the U.S.-EU Safe Harbor framework with its U.S. counterpart, or the text of the future EU Data Protection Regulation with the other EU institutions. In any event, the recent intensity of the WP29 activities demonstrates that it is determined to play a central and proactive role regarding both interpreting the current EU data protection legal framework and defining the future of U.S.-EU data transfers and the key principles of the upcoming EU data protection framework.

FCC Clarifies That Consent May Be Provided by Intermediary for Informational Text Messages

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

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

Joseph Molosky
Associate, Washington, DC
jmolosky@wsgr.com

On March 27, 2014, the Federal Communications Commission (FCC) addressed an outstanding petition[1] seeking guidance for compliance with the "prior express consent" requirement of the Telephone Consumer Protection Act (TCPA) for informational text messages.[2] In a declaratory ruling, the FCC provided clarification of this requirement, and specifically addressed whether an intermediary may provide such consent. The FCC agreed with group texting service GroupMe, Inc. that, consistent with the TCPA, intermediaries may convey consent provided by others to receive informational text messages.[3] However, the FCC made clear that companies ultimately remain liable where intermediaries fail to obtain the required consent. The ruling demonstrates a current trend at the FCC to allow businesses communicating with consumers by text message some flexibility while navigating the TCPA's increasingly complex requirements.

Background

The TCPA was enacted to protect consumers from unwanted telemarketing communications without inhibiting communications from businesses that consumers want or that do not otherwise implicate the harms that the TCPA was intended to prevent. It generally prohibits calls and text messages[4] to wireless numbers made using an "automatic telephone dialing system"[5] (often referred to as an "autodialer") or an artificial or prerecorded voice message without the prior express consent of the called party.[6] Recently, consumer communication preferences have shifted to more text-based, mobile communications facilitated by technological developments such as social

---

[1] On March 27, the FCC also granted Cargo Airline Association's request for an exemption from TCPA restrictions for free-to-end-user delivery notification cell phone calls and text messages subject to several conditions. *See* Order, *In the Matter of Cargo Airline Association*, FCC 14-32 (March 27, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0327/FCC-14-32A1.pdf.

[2] 47 U.S.C. § 227.

[3] Declaratory Ruling, *In the Matter of GroupMe, Inc./Skype Communications S.A.R.L.*, FCC 14-33 (March 27, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0327/FCC-14-33A1.pdf.

[4] Although the statute refers to "calls," the FCC has concluded that a "call" includes the transmission of a text message. *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd. 14014, 14115 (July 3, 2003). Numerous courts have adopted this interpretation. *See, e.g., Saterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 954 (9th Cir. 2009).

[5] The TCPA defines "automatic telephone dialing system" as equipment that has the "capacity" to both "store or produce telephone numbers to be called, using a random or sequential number generator; and . . . to dial such numbers." 47 U.S.C. § 227(a)(1). Despite this very specific definition, plaintiffs have argued that any equipment that has the capacity to automatically dial numbers from a list or database without human intervention is an "automatic telephone dialing system" for purposes of the TCPA. Thus, many putative TCPA class actions have been filed based on text messages allegedly sent to users of a service using a computerized or otherwise automated dialing system.

[6] 47 U.S.C. § 227(b)(1)(A).

network messaging applications. As a result, businesses are increasingly using text messages to communicate with consumers and facing new challenges complying with TCPA restrictions. The rise in the number of text-based services and methods of customer communications has led to an onslaught of TCPA putative class actions. The incentive for plaintiffs' lawyers to file such claims is great because the TCPA provides a private right of action and statutory damages of up to $1,500 per text message without requiring the plaintiff to show any actual damages.[7] The business challenges of obtaining prior express consent in the myriad contexts in which text messaging is now utilized, as well as the epidemic of putative class actions based on the receipt of a single text message confirmation, invitation, notice, or other non-telemarketing communication, have led many companies to petition the FCC over the past few years for rulings that make clear that these types of text messages do not violate the TCPA.

In March 2012, GroupMe filed such a petition asking the FCC to clarify that, consistent with the TCPA, GroupMe and other companies may rely on an intermediary's representation that it obtained the requisite prior consent from the text recipient to be sent the text at issue. According to the FCC's ruling, the GroupMe app provides a free text messaging service that allows users to create messaging groups of up to 50 people. GroupMe users can invite their friends, family, and other people whose cell phone numbers they have to a group by providing GroupMe with the individuals' wireless numbers. GroupMe then sends up to four informational text messages to those wireless numbers. The messages contain information about the group and its members, instructions to stop receiving messages associated with the group, and instructions for downloading the GroupMe app.

Because it would be impossible for GroupMe to directly obtain the necessary express consent from the individuals being invited to join a GroupMe group, GroupMe relies on the GroupMe users' (i.e., an intermediary's) representations that they obtained prior express consent from the invitees. The GroupMe users make the representation when creating a group and agreeing to GroupMe's terms of service, which include a representation that any individuals invited to the group consented to be added to the group and receive text messages. In its petition, GroupMe asked the FCC to clarify that such consent, obtained by an intermediary, satisfies the TCPA's prior express consent requirement for informational calls or texts to wireless numbers.[8]

GroupMe Declaratory Ruling

In the declaratory ruling responding to GroupMe's petition, the FCC agreed with GroupMe. Specifically, it clarified that for informational (i.e., non-telemarketing) texts, "a consumer's prior express consent may be obtained and conveyed by an intermediary, such as the organizer of a group using GroupMe's service." In making this clarification, the commission noted that neither the TCPA nor the FCC's rules or orders require a specific method for obtaining prior express consent for non-telemarketing calls. This lack of a required method for obtaining consent allowed the commission to exercise its discretion to interpret the prior express consent requirement by looking at the intent of the TCPA. It concluded that the informational messages were "normal business communications" and "expected and desired by consumers who gave prior express consent to participate in a GroupMe group" and receive associated text messages.[9] It further concluded that allowing consent to be conveyed by an intermediary in this context was consistent with the goals of the TCPA, because the person conveying the consent already has an established relationship with the called party and is required to represent that such party has consented to the communications.

The FCC stressed, however, that GroupMe and other businesses that are sending the informational text messages remain liable if the intermediary did not in fact obtain consent from the recipient for the messages to be sent. Further, the scope of the consent is limited to messages about the particular group the text recipient consented to join. The commission also encouraged GroupMe to ensure full disclosure to its user-intermediaries of the requirement to obtain prior express consent and their representation to GroupMe of obtaining it, even though GroupMe's terms of service include applicable language.

Implications

The FCC's clarification in the GroupMe declaratory ruling that prior express consent may be obtained through an intermediary is a welcome development for many businesses. Numerous group messaging, mobile social network, and other communication apps and services exist that allow users to invite people they know and whose cell phone numbers they possess to join the service. Although ultimately such services may still face lawsuits if their users do not actually obtain consent from the people whose cell phone numbers they are sharing, the clarification enables these services to comply with the TCPA's prior express consent requirement. Companies that send text messages at the direction of users of their services should especially take note of the ruling and consider its impact on their business practices. It may provide such organizations with more flexibility for complying with the TCPA's consent requirement.[10]

---

[7] 47 U.S.C. § 227(b)(3).

[8] The FCC's new TCPA rules, which took effect October 16, 2013, require prior express *written* consent for all marketing or promotional calls or text messages to wireless numbers made using autodialers or artificial or prerecorded messages. Under the rules, the written consent must include specific authorization language and a "clear and conspicuous" disclosure. See our WSGR Alert discussing the new TCPA rules at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-TCPA-changes.htm.

[9] Declaratory Ruling, *supra* note 3 at ¶ 8.

[10] *Id.*

Continued on page 16...

FCC Clarifies That Consent . . . *(continued from page 15)*

Companies that deliver informational text messages to consumers via cell phone numbers may also wish to consider seeking an exemption from the TCPA. If a company moves to a free-to-end-user service when sending informational text messages, it may be able to obtain a ruling from the FCC exempting the messages from compliance with TCPA restrictions. Cargo Airline Association recently obtained such an exemption, subject to several conditions, for free-to-end-user package delivery notifications.[11]

The recent ruling addresses only a small portion of the backlog of petitions regarding TCPA compliance. As the FCC works through the remaining petitions, it will provide additional guidance on many uncertain areas, including "what it means to initiate a call, whether there is liability for calls made to reassigned phone numbers . . . whether consent can be inferred from consumer behavior or social norms, whether devices including smartphones could be considered automatic telephone dialing systems, and what types of faxes are actually unsolicited."[12] Hopefully the FCC will continue to recognize that many companies are now using text messaging for "normal, expected, and desired business communications" that do not implicate the harms addressed by the TCPA and provide additional welcome guidance on the pending issues consistent with such recognition.

[11] *See* Order, *supra* note 1.
[12] Michael O'Rielly, FCC Commissioner, "TCPA: It is Time to Provide Clarity," Official FCC Blog (March 25, 2014), http://www.fcc.gov/blog/tcpa-it-time-provide-clarity.

The *Wyndham* Rulings and the FTC's Leadership in Data Security Enforcement

Edward Holman
Associate, Washington, DC
eholman@wsgr.com

Joseph Molosky
Associate, Washington, DC
jmolosky@wsgr.com

Despite reaching settlements with more than 50 organizations on data security issues since the late 1990s, no organization seriously challenged the Federal Trade Commission's (FTC's) authority to bring such cases until *FTC v. Wyndham Worldwide Corp.* made headlines in 2012.[1] The case brought rampant speculation from the privacy and data security community on the likely outcome and potential impact on a number of issues, ranging from the FTC's enforcement authority to national and state data security laws. Recent rulings rejecting Wyndham's motions to dismiss may not break new ground for the FTC, but the commission's ability to overcome the first challenges to its data security enforcement authority are significant and continue the agency's trajectory as the country's leading data security enforcer.[2]

Background

The FTC's complaint alleged that Wyndham Worldwide Corporation (WWC) and three affiliated companies, Wyndham Hotel Group, LLC (WHG), Wyndham Hotels & Resorts, LLC (WHR), and Wyndham Hotel Management, Inc. (WHM) (collectively, Wyndham), made misrepresentations regarding, and failed to maintain, reasonable and appropriate data security practices.[3] The FTC claimed that the failures resulted in three data breaches that allegedly compromised payment card information for more than 619,000 consumer accounts and caused $10.6 million in fraud loss.

The Wyndham defendants filed two separate motions to dismiss the FTC's complaint. The first motion only included WHR and made three main arguments: (1) that the FTC's unfairness authority did not extend to data security; (2) that the FTC failed to provide fair notice by not promulgating data security requirements; and (3) that federal laws and card brand policies eliminated consumer injury from the breaches and any associated consumer losses. The second motion included the remaining entities, WWC, WHG, and WHM. That motion argued that the FTC's complaint did not allege direct liability against WWC, WHG, and WHM, and that WWC, WHG, and WHM, as separate corporate

[1] Press Release, Federal Trade Commission, "FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumers' Personal Information" (June 26, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect.
[2] Opinion, *FTC v. Wyndham Worldwide Corp.*, No 2:13-cv-01887-ES-JAD (April 7, 2014), *available at* http://epic.org/privacy/big-data/ftc-v-wyndham-opinion.pdf [hereinafter Opinion 1]; Opinion, *FTC v. Wyndham Worldwide Corp.*, No 2:13-cv-01887-ES-JAD (June 23, 2014), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?filename=0&article=1763&context=historical&type=additional [hereinafter Opinion 2].
[3] Complaint, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-SPL (June 26, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf.

entities, cannot be held derivatively liable for WHR's alleged violations of Section 5.

Rulings on the Motions to Dismiss

In its ruling on the first motion to dismiss, the U.S. District Court for the District of New Jersey rejected all of Wyndham's arguments. First, the court found that the FTC's broad authority under Section 5 includes data security enforcement and rejected Wyndham's argument for a data security exception to Section 5. Wyndham had argued that other regulations containing data security requirements preclude the FTC's general data security authority.[4] The court was not persuaded, however, and found that those regulations and data security requirements complemented, rather than precluded, the FTC's data security authority. The court also found that three statements made by the FTC between 1998 and 2001 regarding its ability to bring data security cases did not limit the commission's authority.

In addition, the court rejected Wyndham's second argument that it did not receive fair notice of data security requirements because the FTC had not issued data security rules and regulations prior to bringing an enforcement action. The court noted that other courts have affirmed FTC unfairness actions without preexisting rules or regulations in many contexts by relying on notice provided by the FTC's case-by-case enforcement approach. Thus, the court found that the FTC's previous data security enforcement actions, public statements, and business guidance brochures provided sufficient notice. The court also explained that Wyndham's fair notice argument was not limited to data security, and as such, accepting it would result in the FTC stopping all unfairness actions until proscribing specific requirements for each context, an outcome contradictory to the "flexibility necessarily inherent in Section 5 of the FTC Act."[5]

Finally, the court rejected Wyndham's third argument that consumers did not suffer substantial, unavoidable financial injury because federal laws and card brands effectively protect consumers from fraud loss caused by payment card data breaches. The court held that the FTC's allegations of unreimbursed fraud charges, the loss of access to funds, the temporary loss of access to credit, the cost of reasonable mitigation, and the time, trouble, and aggravation of dealing with unwinding the alleged fraud were enough to overcome the motion to dismiss. The court also held that the FTC adequately pled that the alleged injuries were unavoidable and that Wyndham's alleged security failures caused the injuries.

In its ruling on the second motion to dismiss, the court rejected both of Wyndham's contentions. The court held that the FTC's allegations of specific facts relating to common control of the companies and sharing of office space and employees were sufficient to support a claim for common-enterprise liability. In doing so, the court dismissed Wyndham's argument that the FTC did not allege other factors that would support a common-enterprise finding, explaining that "no one factor is controlling" and courts routinely consider a variety of factors.[6] The court also noted that the FTC specifically alleged that WWC and WHG had responsibility for and oversight over some of Hotels and Resorts' business functions including information security during certain time periods.

Implications

The judge qualified the first ruling, noting that it "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked."[7] Further, the ruling does not mean that the U.S. Court of Appeals for the Third Circuit will sustain the FTC's authority on appeal or that the FTC will prevail against Wyndham at trial. The judge granted Wyndham's request to certify for interlocutory appeal of the order, so the Court of Appeals may provide additional clarification on the FTC's authority in the near future.[8] The second ruling is also limited, as a determination of common enterprise sufficient for liability for WWC, WHG, and WHM will depend on the evidence rather than the FTC's allegations.

The rulings as they stand, however, are likely to make organizations more reluctant to challenge the FTC's data security enforcement, continuing the settlement trend of the vast majority of the commission's data security cases. The rulings may even increase the FTC's recent heightened focus on data security, with five companies already settling allegations in the first quarter of 2014. The FTC also may take this opportunity to continue advancing its agenda to expand its enforcement powers. In recent testimony before the Senate Homeland Security and Governmental Affairs Committee and the Senate Commerce, Science, and Transportation Committee,[9] FTC Chairwoman Edith Ramirez again called for authority under new federal data security and breach notification laws to seek civil penalties to help deter unlawful conduct, rulemaking authority under the Administrative Procedures Act, and jurisdiction over non-profit entities. Even without these advancements in enforcement power, the rulings provide organizations clear notice of the FTC's authority to be a leader in data security enforcement.

---

[4] Wyndham identified the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as regulations establishing data security requirements. Opinion 1, *supra* note 2 at 8.

[5] *Id.* at 25.

[6] Opinion 2, *supra* note 2 at 12

[7] Opinion 1, *supra* note 2 at 7.

[8] Memorandum Opinion and Order, *FTC v. Wyndham Worldwide Corp.*, No 2:13-cv-01887-ES-JAD (June 23, 2014), *available at* http://digitalcommons.law.scu.edu/historical/755/.

[9] Prepared Statement of the Federal Trade Commission on Data Breach on the Rise: Protecting Personal Information From Harm before the Committee on Homeland Security and Governmental Affairs of the United States Senate (April 2, 2014) (statement of E. Ramirez, Chairwoman, Federal Trade Commission), *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf; Prepared Statement of the Federal Trade Commission on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches before the Committee on Commerce, Science, and Transportation of the United States Senate (March 26, 2014) (statement of E. Ramirez, Chairwoman, Federal Trade Commission), *available at* http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf.

Privacy & Data Security Risk Assessments: An Overview

Wendell Bartnick
Associate, Washington, DC
wbartnick@wsgr.com

Joseph Molosky
Associate, Washington, DC
jmolosky@wsgr.com

Recent large-scale data breaches provide a stark reminder of the risks and challenges associated with today's data-driven economy. The exploding number of devices connected to the Internet and amount of information collected about people by organizations make it increasingly important for officers, directors, and senior management to fully understand the privacy and data security risks faced by their organizations.

One of the most effective techniques for managing those risks is conducting a comprehensive privacy and data security risk assessment. Organizations use such risk assessments to maintain appropriate risk profiles based on the organization's contractual, regulatory, and governance obligations. Regulatory schemes in some industries, including health[1] and finance,[2] may require risk assessments for compliance. Organizations that collect payment information to process payments as merchants or payment processors[3] or deal with data collected about individuals residing in specific states[4] may also have risk assessment obligations. Organizations commonly tailor risk assessments to meet these types of obligations for their risk tolerance and profile. A comprehensive risk assessment may include considerations of scope, documentation, timing, management, and oversight.[5]

Scope

The most effective assessments begin by defining the scope appropriately. The scope will vary depending on an organization's regulatory and contractual compliance obligations, data practices, and risk tolerance. A particular risk assessment may cover only certain business areas, functions, and/or products or services. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires an assessment covering the "confidentiality, availability, and integrity of all electronic [protected] health information a covered entity creates, receives, maintains, or transmits."[6] The HIPAA-required assessment does not cover data that is not "electronic" protected health information, although organizations commonly include all protected health information in an assessment because of its potential sensitivity and the potentially high costs of a failure to protect such information.

An organization may also consider including employee human resources information or other personal information collected from consumers in its assessment based on the organization's risk profile.

Key Elements

A privacy and data security risk assessment typically includes the identification and analysis of the following key elements:

- *Policy and Contract Obligations.* Promises made in contracts and privacy policies
- *Data Flows.* Data collected, used, processed, maintained, and disclosed by the organization and the locations where it is maintained
- *Third Parties.* Any applications or third parties using or accessing the data
- *Threat Analysis.* Potential threats to and vulnerabilities of the data and the organization, including their likelihood and potential impact on the organization
- *Safeguards Review.* Administrative, physical, and technical measures in place to protect the data and the organization

Documentation

Documenting the risk assessment process and findings helps to ensure the consistency of repeated assessments, effective oversight, successful remediation of potential issues, and a reduction of risk to the organization.

Timing

Risk assessments provide more value when conducted on a regular basis. Organizations often determine the specific frequency based on the scope of the assessments, the nature of the data, and the risks to the organization. Many organizations conduct assessments on an annual basis. Organizations also perform ad hoc assessments after any material changes to the internal operations of the organization or to the external business, regulatory, economic, or legal environments in which the organization operates.

---

[1] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Administrative Safeguards, 45 C.F.R. § 164.308(a)(1)(ii)(A).
[2] *See* Gramm-Leach-Bliley Act (GLBA), Standards for Safeguarding Customer Information, 16 U.S.C. § 314.4.
[3] *See* PCI Security Standards Council, *Information Supplement: PCI DSS Risk Assessment Guidelines* (November 2012), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf.
[4] *See* Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. § 17.03(2)(b).
[5] Standards are available that provide details for specific activities involved with each of the fundamental areas, including the recent *Framework for Improving Critical Infrastructure Cybersecurity. See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* 22-23 (February 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (providing a list of risk assessment activities and links to the treatment of risk assessments by other standards such as ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4).
[6] Department of Health & Human Services, *Basics of Risk Analysis and Risk Management*, 2 HIPAA Security Series 6 (March 2007), available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

Management and Oversight

Organizations can assign a specific individual or group of individuals with responsibility for implementing the risk assessment process, conducting the assessments, and managing any resulting remediation. The risk assessment process may also necessitate reports to senior management about the results and subsequent remediation activities.

In addition to the fundamental elements discussed above, many organizations engage outside counsel when conducting assessments due to increasing litigation and regulatory investigations resulting from privacy and data security issues. Besides offering added expertise, the engagement of outside counsel provides for the potential availability of attorney-client privilege and work-product protections.

High-profile data breaches and government investigations have brought privacy and information security risks to the attention of boards of directors, investors, and consumers like never before. Risk assessments can be a valuable tool for organizations to reduce the risks associated with these increasingly complex issues.

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

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