What’s trending on NP Privacy Partner

Target and several others are embroiled in privacy and data breach litigation, resulting in one $8.4 million TCPA settlement. And electric power infrastructure companies receive new smart grid cybersecurity guidelines from NIST. Here’s what’s trending in data privacy and security.

Enforcement & Litigation

Target files Motion to Dismiss in multidistrict data breach litigation, financial institutions respond to Target’s Motion to Dismiss claims relating to reissuing payment cards, and a federal court won't approve a proposed junk fax settlement

The Target multidistrict litigation has been heating up. Target filed its Motion to Dismiss, the putative class action suit, alleging that the plaintiff/consumers lacked standing to sue alleging that there is no evidence that the consumers suffered a compensable harm, relying on Clapper v. Amnesty International USA.

In addition, as a result of the massive data breach, financial institutions had to cancel and reissue millions of payment cards. The financial institutions are seeking reimbursement from Target for the costs associated with the issuance of the new cards, and rely in part on the Minnesota Plastic Card Security Act (the “Act”). The financial institutions allege that Target was negligent in protecting consumers’ data, that its practices were deficient and that they were maintaining customer financial data anywhere between 60 and 90 days, which violates the Act.

Target claims that it has not violated the Act, that the banks lack standing and that it owes no duty of care to the financial institutions.

Finally, on Wednesday, a federal judge refused to approve a settlement that would resolve a proposed class action against Target that claims it violated the Junk Fax Prevention Act when it sent unsolicited faxes to approximately 458 pharmacies. Target proposed to settle the case for $183,375. The settlement requires the pharmacies to submit a form to get a portion of the settlement proceeds, which the judge found concerning because the reply rate is typically low in those types of settlements. In addition, the settlement includes a provision that any unclaimed settlement funds revert back to Target. The judge stated that he “harbored doubts whether the settlement was adequate and should be approved.”—Linn Foster Freedman
Comenity Bank settles TCPA class action for automated telephone calls to mobile phones for a whopping $8.4 million

On October 2, 2014, U.S. District Court for the Southern District of California approved Comenity Bank’s $8.5 million Telephone Consumer Protection Act (TCPA) class action, which consisted of over four million class members. From August 2010 to May 26, 2014, Comenity Bank allegedly made automated telephone calls to consumers’ mobile phones. The lead plaintiff, Carrie Couser, filed the class action back in October 2012, alleging that Comenity Bank had called her mobile phone four to five times per day to collect an alleged debt. Now, with the Court’s final approval, almost $2 million of the $8.4 million will be used to pay for attorneys’ fees, while class members will get only a tiny portion. Each individual can only claim up to one call per cell phone number. What does this mean for the payout to consumers? Each individual will receive between $0.98 and $32 depending on the percentage of class members who actually submit a claim. The settlement motion stated, “Although the TCPA provides for statutory damages of $500 for each negligent violation and $1,500 for each willful violation, it is well-settled that a proposed settlement may be acceptable even though it amounts to only a small percentage of the potential recovery that might be available to the class members at trial.” Does that seem fair? I think not, but with more and more TCPA class action settlements, businesses should be aware that even if the consumers don’t get a large payout, these actions are going to keep coming.— Kathryn M. Sylvia

Twitter files declaratory action against the USAG, Department of Justice and the FBI

On Tuesday, Twitter filed a Complaint for Declaratory Judgment against Eric Holder in his official capacity as Attorney General of the United States (DAG), the United States Department of Justice (DOJ), James Comey, in his official capacity as the Director of the Federal Bureau of Investigation (FBI) and the FBI requesting a declaratory judgment that: 1) its draft Transparency Report submitted to the FBI be published in part or in whole; 2) that the letter forwarded to Twitter by the DAG violates the Administrative Procedures Act; 3) that the nondisclosure provision of the Stored Communications Act, review mechanisms and secrecy provisions of the Foreign Intelligence Surveillance Act are unconstitutional under the First Amendment; and 4) the DAG’s prohibition of reporting receipt of zero requests and ranges of national security process requests are unconstitutional.

The crux of the Complaint is that Twitter may receive requests for information about users from the government under the authority provided to it to protect against international terrorism or “clandestine intelligence activities” known as FISA requests. Following the Edward Snowden leaks about the U.S. government intelligence collection and surveillance programs and the concern raised by the public, the government released limited information about the programs. However, the government has refused to allow Twitter (and other communications providers) to respond to government statements and provide information to the public about the actual facts, including the number of surveillance requests and responses by Twitter.

Twitter alleges that it is “entitled under the First Amendment to respond to its users’ concerns and to the statements of U.S. government officials by providing more complete information about the limited scope of U.S. government surveillance of Twitter user accounts, including what types of legal process have not been received by Twitter…”

Previous Complaints filed by other services providers were dismissed when the DOJ agreed to allow the companies to disclose information about the government’s surveillance through two preapproved formats. Since Twitter’s information did not fit within the preapproved formats, the government refused to allow it to publish its surveillance information. It will be interesting to see
how the government responds to this Complaint and if a resolution will be reached before it gets too far down the litigation path.—Linn Foster Freedman

**Wyndham argues again against the FTC’s authority to regulate data security practices**

We wrote back in August that the U.S. Court of Appeals for the Third Circuit would hear the case between Wyndham Hotel & Resorts LLC (Wyndham) and the Federal Trade Commission (FTC). Now, on October 7, 2014, Wyndham pled with the Third Circuit, arguing once again that the FTC does not have the authority to regulate businesses’ data security practices and procedures. This argument comes after Judge Esther Salas ruled in April of this year that the FTC did, in fact, have authority to regulate data security practices and bring enforcement actions against businesses that have lax data security practices under Section 5 of the FTC Act. Wyndham reiterates its argument that Congress did not intend for the FTC to have the power to regulate a business’ data security practices under the Section 5 “unfairness” prong because security breaches not only harm individual consumers but the business itself as well. Wyndham said during its argument, “If Congress had intended to give the FTC vast powers over cybersecurity (or other forms of business security), it could and would have done so much more clearly than allowing the commission to regulate ‘unfair’ business practices. And because the statutory term ‘unfair’ cannot be stretched so far, the FTC is not entitled to any deference on this score.” Wyndham also continued to argue that even if the FTC has the power to regulate data security practices, the FTC has failed to provide any guidelines as to what qualifies as reasonable data security practices, and therefore, cannot enforce its action against Wyndham. Wyndham calls this disconnect “the very antithesis of the rule of law.” Without any guidelines to follow how can businesses conform their conduct to the law? On procedural grounds, Wyndham also argued that the FTC failed to satisfy federal pleading standards. This is the case to follow. Continue to watch how this decision pans out.—Kathryn M. Sylvia

**Judge dismisses $116M medical data theft class action against Alere**

Alere Home Monitoring Inc. (Alere) suffered a data breach in 2012 when a password protected laptop containing the names, addresses, dates of birth, Social Security numbers and diagnosis codes of 116,000 patients receiving home monitoring was stolen from an employee’s vehicle. As a result of the breach, a putative class action case was filed against Alere on behalf of a potential class of 116,000 persons alleging negligence, unjust enrichment, violations of the Fair Credit Reporting Act (FCRA), the Unfair Competition Law and the California Medical Information Act.

The Judge dismissed the FCRA claim because the plaintiff was unable to prove that Alere is a credit reporting agency, the unfair competition and unjust enrichment claims based upon the fact that release of the information did not constitute a loss of property.

Alere asked the Court to dismiss the case because the only damages alleged were for risk of identity theft and risk of wrongful use of medical information, and invasion of privacy, and all of these claims are “speculative.” This decision is consistent with many other similar cases, so it appears that this area of the law is becoming more and more well settled.—Linn Foster Freedman

**Cybersecurity/Smart Grid**

**NIST Interagency Report on Revised Guidelines for Smart Grid Cybersecurity published**

The National Institute of Standards and Technology (NIST) Revised Guidelines for Smart Grid Cybersecurity was recently published, updating the 2010 initial three-volume report published in 2010.
The initial guidance provided a voluntary framework to be used by organizations to develop effective cybersecurity strategies applicable to smart grid technology, including assessing risk and identifying and applying security standards.

According to the revised guidelines, “cybersecurity must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition.”

The revised Guidelines are the culmination of comments from the industry, users’ experience deploying the systems and updates to technology. New sections have been added to address outstanding issues such as cyber-physical attacks. In addition, the revised Guidelines discuss new laws and regulations that have been enacted in several states applicable to smart grid technology.

The Guidelines are dense and technical, but an imperative read for those stakeholders responsible for electric power infrastructure, “including utilities, providers of energy management services and manufacturers of electric vehicles and charging stations.”—Linn Foster Freedman

Social Media

California enacts bill protecting student information posted on social media
California Governor Jerry Brown signed into law a bill that requires school districts to notify students and their parents in advance if they collect information that their students post on social media. The Student Online Personal Information Protection Act requires districts to only gather and maintain information that pertains directly to school safety or to pupil safety, provide a student with access to any information about the pupil obtained from social media, and requires school districts and their third party vendors who have access to the information to destroy any information collected on the students within one year of the student leaving the district or turning the age of 18.—Linn Foster Freedman

Did a Twitter parody cross the line?
The figure of speech “Will it play in Peoria?” applies to a civil rights lawsuit in an Illinois Federal Court, where the plaintiff alleges that the City of Peoria, its Mayor and other municipal officials violated his First and Fourth Amendment rights in its response to his Twitter parody account. The Peoria defendants deny liability and claim that the lawsuit does not plead legally viable causes of action.

As alleged in plaintiff’s complaint, on or about March 9, 2014, Jonathan Daniel (“Daniel”) created a Twitter account spoofing Peoria Mayor Jim Ardis. The account’s avatar was a picture of Mayor Ardis. Daniel intended the account to be seen only by his friends. A few days after creating the account, Daniel added the words “parody account” to its biography. Daniel posted crude tweets attributing illegal acts to the Mayor, including the use of narcotics and patronizing of prostitution.

Peoria officials responded promptly to the depiction of the Mayor. In Illinois, it is a crime to impersonate via the Internet another person if the person making the posts acts with the “intent to intimidate, threaten, injure, defraud, or obtain a benefit from another.” The Peoria police secured warrants to learn the account holder’s identity from Twitter and search Daniel’s premises and seize evidence. Twitter suspended the account on March 20, 2014. After seizing Daniel’s computers and other electronic devices, the Peoria police arrested Daniel for falsely impersonating a public official. Ultimately, the city did not prosecute Daniel under the False Impersonation Statute. The Mayor has defended the municipality’s response and described the parody account as “absolute filth.”
In June, Daniel filed a civil rights lawsuit alleging violations of his free speech rights and freedom from unlawful searches and seizures due to Peoria’s response to his satirical Twitter parody of the Mayor. City officials contend that they had probable cause to believe that there was a violation of the False Impersonation Statute justifying the municipality’s response, searches and arrest.

This litigation poses interesting constitutional questions as to how far satirical speech may go on the Internet and remain protected by the First Amendment. Similarly, the federal court will examine whether the city’s response was justified and within the scope of the Fourth Amendment’s provisions governing searches and seizures. The determination of these issues should be watched closely as online satirical postings proliferate on social media.—Steven M. Richard

Courts address the use of instant messages and a social media profile page as evidence
Recently, we issued E-Discovery Alerts analyzing two important appellate decisions regarding the proper authentication of electronic evidence at trial. In each case, the electronic evidence had a dispositive impact upon the jury’s verdict.

In one, the Massachusetts Appeals Court upheld a conviction based upon the admission of incriminating instant messages sent under a false name that were attributed to the defendant. The Appeals Court ruled that the prosecution properly authenticated the messages through the testimony of the recipient who described “confirming circumstances” tying the electronic confession to the defendant.

In the other, the United States Court of Appeals for the Second Circuit ordered a new trial and vacated a defendant’s conviction for sending a forged document via email. The prosecution introduced at trial a social media profile page to tie the defendant to the email address from which the forged document was sent. The Second Circuit held that the prosecution did not properly authenticate the profile page by merely accessing it on the Internet and admitting a printout into evidence. Instead, the proper authentication required evidence that the defendant and not someone else actually created the profile page.—Steven M. Richard

Mobile Technology

Is the future of business collaboration the future of corruption concerns?
In today’s fast-paced environment, businesses rely on technology to provide employees with quick, organization-wide communication tools. Recently, businesses began using instant messaging (“IM”) services to promote broad collaboration with internal and external personnel. Many programs function seamlessly with personal instant messaging services. As a result, employees often intertwine their business and personal communications. Although IM offers an effective communication tool, the fast-paced environment tends to elicit unguarded responses and potentially devastating evidence in a civil or criminal investigation.

Because, on IM, employees often talk more freely, multinational corporations must be aware that their employees’ IM logs might contain information critical to an effective internal or governmental investigation. Impulsive responses can be particularly devastating for companies investigating violations of the Foreign Corrupt Practices Act (“FCPA”). While large, domestic companies have likely read headlines touting multimillion-dollar FCPA settlements and corporate executives sentenced to federal prison, many small and mid-sized companies are inexperienced with the FCPA. Of course, the recent $2,000,000 settlement of Massachusetts-based Smith & Wesson proves that mid-sized companies should pay attention.
Business leaders with overseas branches should prepare to grapple with allegations of corruption. Today, investigating corruption means analyzing large amounts of private data such as e-mails, calendars and—most recently—IM communication logs. Securing electronic communications during any investigation is itself a sensitive matter, but the global nature of FCPA investigations often forces investigators to confront the privacy laws of multiple countries. For instance, investigating an EU-based subsidiary requires additional resources and time due to strict EU privacy laws. Because IM tools allow employees to reach beyond their borders and contain a mix of personal and business communications, leaders and investigators will be forced to weigh the costs and benefits of accessing private data and have competent counsel capable of advising them on multiple fronts.—*Eric Walz*

**International Privacy**

**EU Advisory Body Hopes to Implement a Consistent Approach for Addressing Complaints Related to “Right to be Forgotten” Refusals**

EU regulators’ support for data privacy reform continues. And now, as link removal requests under the so-called “Right to be Forgotten” continue to pour in to search engine operators, users whose requests have been rejected are wondering: What next?

The Article 29 Working Party on the Protection of Individuals (“WP29”), an independent advisory body set up under the EU Data Protection Directive, recently discussed the effects of the high court’s ruling and how complaints about refusals to “de-list” are now making their way to data protection authorities in the EU. The WP29 remarked that these complaints demonstrate “that the ruling has addressed a genuine demand for data protection from data subjects.” But what happens now? The construction of a “tool-box” to help regulators evaluate rejected “de-listing” requests.

After a summer of meetings, discussion and grilling of search engine operators, the WP29 determined that the EU needs a common case-handling approach, including a network of dedicated contacts to handle complaints. The proposed “tool-box” for handling complaints will include: “a common record of decisions taken on complaints” and “a dashboard to help identify similar cases as well as new or more difficult cases.”

The WP29 spent its summer with media companies and search engine operators. During its meeting with the search engines, in particular, the members of WP29 were critical and curious about how the operators implemented the ruling’s requirements. The planned “tool-box” may give some comfort to EU citizens seeking appeal from a refusal to “de-list.” What remains to be seen is whether the “tool-box” and the resulting determinations by EU officials could eventually help search engine operators have a clearer understanding of how they should act upon such requests in the first instance. As these issues and the discussion of how to handle them develops in the EU, users and search engine operators are left to make their own determinations until they can see some actual guidance.—*Kate A.F. Martinez*

For more information, please contact:

— Linn Foster Freedman, Privacy & Data Protection Group Leader, at lfreedman@nixonpeabody.com or 401-454-1108
— Kathryn M. Sylvia at ksvlia@nixonpeabody.com or 401-454-1029
— Kate A.F. Martinez at kmartinez@nixonpeabody.com or 585-263-1332
— Steven M. Richard at srichard@nixonpeabody.com or 401-454-1020
— Eric Walz at ewalz@nixonpeabody.com or 617-345-1029

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team.