Underwriting In An Even More Connected World

By Ron Raether and Mark C. Mao

Ron Raether
is a partner in the Cybersecurity, Info Governance and Privacy, and Financial Services Litigation practices at Troutman Sanders. Ron has assisted companies in navigating federal and state privacy laws for almost twenty years. Ron's experience with technology-related issues, including data security, patent, antitrust, and licensing and contracts, helps bring a fresh and creative perspective to novel data compliance issues. He can be reached at ronald.raether@troutmansanders.com.

Mark Mao
is a partner in the Cybersecurity, Info Governance and Privacy and Business Litigation practices of Troutman Sanders. Mark's practice focuses primarily on emerging-technology companies, with a particular interest in their intellectual property and privacy ("cyber") law needs. Mark is certified by the International Association of Privacy Professionals (IAPP), for their ISO-approved programs, as a Certified Information Privacy Technologist (CIPT), and a Certified Information Privacy Professional in the United States (CIPP/US). He can be reached at mark.mao@troutmansanders.com.

New coverage issues are coming to the world of cyber insurance, and they show how it is more important than ever for insurance organizations and the attorneys representing them to invest more time understanding emerging technologies.

Why is this important? Let's start with commonly used terminology. The insurance marketplace provides "privacy injury" coverage by defining such risks as the "unauthorized collection, use, access, disclosure, alteration, or destruction of Personal Information," and the "failure to safeguard, deploy, maintain, or comply with policies and procedures with regard to the Insured's obligations for Personal Information." Another definition of "privacy injury" might use language such as, "any unauthorized disclosure, access, or inaccuracy with respect to Non-Public Personal Information, in violation of (1) the Insured's privacy policy, or (2) any federal, state, foreign law, statute, or regulation governing the confidentiality, accessibility, or integrity of Non-Public Personal Information."

Most insurance professionals think "data breach litigation" when they think "privacy injury." However, common behavioral tracking and directed marketing practices are appearing increasingly in civil litigation and regulatory enforcement. Data breach cases have also begun debating the requisite standard of care. As the issues in these cases increasingly require a deeper understanding of the technology, underwriting and claims handling increasingly require technical competence.

Impermissible "Tracking" Cases–The Prelude to a More Connected World

Most are not aware that a much more connected world is already here. Portable technologies like fitness wearables are actually a play for the greater connectivity of all "things," which some have dubbed the "internet of things (IOT)." Personal data and related applications are already accessible by "cloud" through laptops, mobile phones, tablets, and smart-watches. IOT devices such as "smart" home thermometers, door locks, security cameras, televisions, and refrigerators are now also connected to our mobile devices. As automobiles also become automated and connected, life from wake to work to home to sleep will be constantly monitored and adjusted to "personalize" the experience wherever the user goes. Adding on "augmented reality" that one will soon be able to layer on top of his or her physical experience in the real world, our experiences with each other and businesses as we stroll down a street will truly be customized for those connected.

For such complete personalization, however, businesses need more of our personally identifiable information (PII). With more PII, businesses can enhance our life experience and direct services to when and where we need them most. It is in anticipation of this tectonic shift in technology that governance of PII becomes more important than ever. Technologists and marketers argue that leveraging PII can increase market efficiency by directing and targeting traffic to users in accordance with what they actually want and need. Privacy advocates argue that such practices mostly lead to unwanted targeted marketing, which is impermissibly intrusive. For insurance professionals, the question might instead be whether use of such marketing practices could be a covered "privacy claim."

A number of impermissible tracking cases were filed in 2015. Plaintiffs filed cases against common business practices such as the scanning of incoming emails,[1] use of persistent identifiers,[2] and tracking of user-posted hyperlinks.[3] In the cross-device tracking context, plaintiffs also filed claims against the recently popular practice of recording audio sounds.[4] As the arguments in these cases demonstrate, the theories of liability and defense are highly technical, even on basic issues such as identifiabilty and consent. It is easy to talk about the use of pseudonyms as a method of masking identity, but identifiability arguably depends on *how* each pseudonym is used. Organizations will need to have great confidence that their legal counsel can explain such technical workings of the mechanism at issue to judge and jury.

And although the impermissible tracking cases seem to be focused against Silicon Valley giants for now, the practices at issue are generally very common business practices. Organizations that use the internet have been scanning incoming traffic, using persistent identifiers, and tracking incoming URL requests since the beginning of the internet. Thus, if such practices really become common "privacy injury" risks, underwriters will need to do even deeper technical dives into the insureds' technology.

User Profiling–Yes, It Is Already Here

The regulators have already declared that they will aggressively police this new connected world. All are impatiently waiting for the Supreme Court's decision in *Spokeo v. Robins*.[5] Spokeo is a data aggregator that advertises itself as having collected data from a number of "untraditional" sources, such as social media. Prior to the filing of the *Spokeo* case, the FTC had filed a complaint against Spokeo, arguing that it was a "consumer reporting agency (CRA)" issuing "consumer reports," as covered by the Fair Credit Reporting Act (FCRA).

On June 12, 2012, the FTC reported that Spokeo had agreed to pay $800,000 to settle charges that it violated the FCRA, without taking the required steps to protect consumers on issues such as accuracy, making sure that consumer reports would only be used for permissible purposes, and for deceptive advertising.[6] Many critics saw the FTC's move as a bold and expansive one, as data aggregators employing new data technologies like *Spokeo* were not previously dealt with as a CRA covered by the FCRA. The FTC's analysis was viewed by some as turning the FCRA's logic on its head, by redefining "consumer reports" and making Spokeo a CRA.[7]

Although the Supreme Court is considering *Spokeo v. Robins* on a different issue, it is unlikely that the FTC timed the release of its report

entitled, "Big Data—a Tool For Inclusion or Exclusion (Jan. 2016)," by accident. The FTC reminds organizations that it has powers to regulate e-commerce pursuant to the Fair Credit Reporting Act (FCRA), various equal opportunity laws, and the Federal Trade Commission Act (the "FTC Act"). The FTC reiterated its position that aggregators and marketers compiling "non-traditional" information gathered from social media to profile users for the purposes of credit, employment, insurance, housing, or other similar decisions about the users' eligibility may be deemed CRAs, and parties using such information may be deemed to be using "consumer reports." Quietly recognizing the limitations of the FCRA, the FTC also reminded businesses of equal opportunity laws and its powers under Section 5 of the FTC Act.

Perhaps even more importantly, the FTC discussed how an organization using *anonymized* consumer data directly in combination with demographic data from an aggregator to make a covered decision regarding consumers (e.g., on creditworthiness) "likely" implicates the FCRA.[8] This was inconsistent with its own prior finding regarding data anonoymization in its "40 Years (of) FCRA" Report (FTC 2011)," wherein it stated, "[i]nformation that does not identify a specific consumer does not constitute a consumer report even if the communication is used in part to determine eligibility." The FTC recognized its reversal of position and stated in a long footnote that its prior statements therein encouraging de-identification were "(not) accurate."[9]

Attempts to pigeonhole data aggregators as CRAs will be imperfect, however, especially since the data aggregation models of new technology will substantially differ from one to another. For example, faced with allegations similar to *Spokeo*, LinkedIn successfully argued that the claims against it for FCRA violations should be dismissed because, unlike Spokeo, LinkedIn aggregates data provided by its users, even if reports pulled from LinkedIn can be used as credit reports for employment purposes.[10]

And as we had discussed previously, in the new age of connectivity, the world will only be more personalized, and hence more "profiled." It is clear that the FTC's report is meant to signal that it will aggressively police such profiling. Defending against such regulatory actions for covered "privacy injuries" will require high technical competence. As the FCRA provides statutory damages of $100 to $1000 for a willful violation, these issues also will likely appear in courts soon.

Defending The Standard of Care

Data breach litigation is also requiring increasing technical competence, as cases have finally begun debating the requisite standard of care. Defendants are increasingly willing to defend against allegations on the basis of the standard of care to which they believed that they had adhered. In *Lozano v. Regents of the University of California*, Los Angeles Super. Ct. Case No. BC55419, for example, the plaintiff alleged that her medical records were improperly accessed by the current romantic partner of her ex-boyfriend, who allegedly used the identification and password of a doctor to access her personal health information (PHI). Plaintiff alleges that her PHI was then texted to others, revealing that she had a sexually transmitted disease. The UCLA health system disagreed, arguing that it used security protocols consistent with existing standards and that it should not be held responsible for "inside jobs." On Sept. 3, 2015, a jury found that UCLA was not legally liable for the breach.

On the regulatory side, the FTC announced in August 2015 that it would not take any enforcement action against Morgan Stanley for an insider data incident disclosed in January 2015. Morgan Stanley apparently satisfied the FTC, which noted that: "it [Morgan Stanley] had a policy limiting employee access to sensitive customer data without a legitimate business need, it monitored the size and frequency of data transfers by employees, it prohibited employee use of flash drives or other devices to download data, and it blocked access to certain highrisk apps and sites." In its closing letter, the FTC implied that it might not pursue further action if an organization suffers a "human error," but had reasonably appropriate policies in place. As with *Lozano v. Regents of the University of California, supra*, the case of Morgan Stanley establishes that companies can and should assert it did not necessarily breach a standard of care.[11]

To successfully make such arguments in the future, the defense must necessarily understand how to properly present the technical issues to the regulators and finders of fact. They also must understand generally accepted cyber security practices, and thus the standard of care. Setting aside the imminent technological evolution, proving that an insured adhered to the requisite standard of care will require solid understanding of the technologies involved.

Conclusion

In response to the ongoing technological and legal changes, insurers must decide whether they will continue to so define "privacy injury," or simply forego underwriting provisions that would cover the new type of claims that are emerging. Even if carriers merely continue to underwrite cyber risks more closely associated with hacks and direct data loss, it appears that they will need to invest substantial resources to constantly learn about the ongoing changes in technology.

Endnotes

1 *See* Order, *Holland v. Yahoo*, No. 13-cv-4980, ECF No. 105 (N.D. Cal. May 26, 2015) [allowing claims under the Cal. Invasion of Privacy Act and the Stored Comm. Act to survive against Yahoo for its scanning of incoming non-subscriber emails].

2 *See* Order, *In re Google, Inc. Cookie In Placement Consumer Privacy Litigation*, No. 13-4300 (3rd Cir. Nov. 10, 2015) (request for rehearing on motion to dismiss was denied on December 11, 2015).

3 See *In re Facebook Privacy Litigation*, No. 10-cv-2389,(N.D. Cal.) [involving Facebook's use refer header URLs containing user information, from users clicking on advertisements]; see Notice of Vol. Dismissal, *Raney v. Twitter, Inc.*, No. 15-cv-4191, ECF No. 51 (N.D. Cal. Jan. 14, 2016) [alleging that Twitter altered and redirected user's posted hyperlinks in direct user-to-user messages]; see *Campbell v. Facebook, Inc.*, No. 13-cv-5996 (N.D. Cal.) [accusing Facebook of mining URLs and other information in user private messages]; and see *In re Google, supra*, note 2 [holding that scanning referrer URL headers can constitute scanning content in some cases].

4 See *Reed v. Cognitive Media Networks, Inc.*, No. 15-cv-5217 (N.D. Cal.)(suing Vizio and its software partner); *Hodges v. Vizio*, N.D. Cal. Case No. 15-02090; *Mason v. Vizio Holdings*, No. 15-cv-11288 (N.D. Ill.}; and *Ogle v. Vizio*, No. 15-cv-754 (N.D. Ark.).

5 No. 13-1339 (U.S. S. Ct.).

6 FTC, *Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA* (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

7 Law360, Case Study: US v. Spokeo (July 11, 2012).

8 p. 16-18

9 FTC, 40 Years of Experience with the Fair Credit Reporting Act, 20 (July 2011), https://www.ftc.gov/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations

10 Order, *Sweet v. LinkedIn Corp.*, No. 14-cv-4531 (N.D. Cal. Apr. 14, 2015).

11 See also *Krystel v. Sears Holding Corp.*, No. BC486354 (Los Angeles Super. Ct.) (peeping Tom case where jury found Sears not liable for the intruder's viewing of over 1,000 women, including by using secret cameras).