Attorney Advertising

Robinson+Cole

Data Privacy and Security Insider

May 14, 2015

INSIGHTS FROM PRIVACY LAW STUDENTS AT ROGER WILLIAMS UNIVERSITY LAW SCHOOL

Welcome to this week's Insider. I had the honor of teaching the inaugural (and hopefully annual) Privacy Law class at Roger Williams University Law School in Bristol, Rhode Island. An interesting statistic is that only approximately 25% of law schools in the U.S. offer a course on Privacy Law. Roger Williams University is on the cutting edge (and yes, I am biased as I am a Trustee of both the University and the Law School) in also offering a joint MS in Cybersecurity/JD.

Part of the Privacy Law class requirement was for the students to prepare a mid-term paper on an area of Privacy Law that they found to be of particular interest. I so enjoyed reading the papers that I wanted to share them with our wider audience. So—let me introduce you to members of my class, and below is a compilation of their papers. I hope you find them as thought provoking as I did, and have confidence in the future of the legal profession in the hands of these bright young adults!

Enjoy this special edition. Our regularly scheduled weekly Insider will resume next week. In the interim, we will be publishing additional blog posts on the R+C Data Privacy & Security Insider, which you can subscribe to here.

– Linn Foster Freedman

WORLD WAR C: CYBER WARFARE

State-sponsored hacking occurs when a country funds cyber hacking organizations or groups in order to infiltrate a company's or government's cyber system for the sole purpose of stealing personal/sensitive information in the hope of turning a profit, gaining intelligence, or destroying mainframes. Since the first cyber attack in 1988, cyber hacking as become quite ubiquitous. Cyber hacking, once an avenue of personal exploitation, has become a militarized option which is on the forefront of every World Power's mind. Cyber attacks worldwide cause billions of dollars in losses to companies and governments every year. State sponsored hacking is also an effective method for a nation to effectuate an attack on a rival nation without having to shoulder the blame since cyber attacks are relatively anonymous.

I have termed this international phenomenon, World War C: Cyber Warfare. In order for the United States to avoid being inundated with successful cyber attacks, our cyber strategy must be threefold: develop technological advancements, factor in costs for cybersecurity into the national budget, and establish a cyber response team of white hat hackers through recruitment. Technological advancements are of paramount importance because the older a cyber system gets, the more vulnerable it becomes. Budgeting is important because each branch of the military has now established a wing of cybersecurity that requires financing and continued growth. Recruitment is necessary, because in order to train white hat hackers for a good cause, time and resources are required and should begin during adolescence.

From the first attack in 1988 to the Sony hack in 2014, cyber hacking has been growing at an alarming rate. These principals which are evidenced in my extensive research paper outline a necessary response to the international problem of state-sponsored hacking. Cyber hacking has been, and will continue to be, one of the most pressing issues of the computer age.

– Winthrop Smith, Milford, Connecticut, 3L

ISSUES CONCERNING MEDICAL IDENTITY THEFT

Whenever a large data breach occurs in the healthcare industry, such as the Anthem Blue Cross Blue Shield breach this past winter, some news stories always seem to focus on the strange medical catastrophes that could result—like going to an emergency room with acute appendicitis only to be told you had an appendectomy two years earlier. Such a situation may be attention-grabbing for the headlines, but it turns out that medical identity theft is a much larger and more diverse problem.

In addition to the potential inaccuracies in medical records, financial and credit problems can arise just like in any other case of identity theft. Because thieves may be motivated by financial gain, free medical care, or some combination of the two, medical identity theft may be more alluring to potential thieves than regular identity theft. While credit cards have alert systems to spot suspicious charges and all charges are posted to the account in a matter of days, medical billing is a much slower, labor intensive process. The length of time before the medical identity victim might have the first opportunity to learn that the crime occurred can make it harder to apprehend the medical identity thief.

Fixing records after an incident of medical identity theft is more difficult than it would be in a case of financial identity theft. Medical providers are only obligated to correct their own errors, so a victim of medical identity theft must contact every provider seen by the medical identity theft and then every provider that subsequently included any of that information in its own record for the victim. There are often fees to obtain a copy of a personal medical record as well. This is very different from the financial identity theft victim who only needs to contact three agencies and is guaranteed a free annual credit report.

– Lena Thomas, 3L

PRIVACY POLICY OF MOBILE APPS: NO STANDARD FOR TRANSPARENCY

In the standards set by the California Online Privacy Protection Act (CalOPPA) to developers of websites and mobile applications, websites and apps have to have their privacy policy clearly labeled, properly displayed, easy to read, and transparent for the user. All of these properties make an easy way to know why the website or app is using personal information, who is collecting it, and where the information is going. However, there is no industry standard for how transparent a privacy policy has to be. Some websites use broad terms to describe the information, where others are very clear and precise. The questions that need to be looked at in the law are: what privacy practices are being used for apps and websites and how transparent should website and app developers be with the consumer?

Developers such as Rovio, the company that created “Angry Birds,” have a privacy policy that tells users exactly what they want to know. They display where the user’s data is going, who is getting access to it, and what is being accessed. They set up their policy to let the user know that everything is being used for their personal experience and this applies to geo-location services as well. Rovio is clear in saying that their app is used to bring them ads and experiences that are local to the user. However, this type of privacy police is not standard.

In a smaller company like Ustwo, the company that made “Monument Valley,” there is no real way to access their privacy policy easily. One has to Google search for their policy, which can be found in a blog

post that states, “We will not sell your data to anyone or do anything bad in any other way.” This is a dramatic difference from Rovio. Users paid for this app and even though they say they are not using one’s data, can it be trusted? It’s a short line and leaves a lot of questions as to what the developer is doing with the information.

There needs to be some transparency regulation with website and app developers. A stricter rule of what can be said in broad terms and what should be properly displayed for the consumer. In this modern age where everything can be accessed on a smartphone, there should be no chances taken when it comes to the privacy of those that keep the app and website developers in business, the consumer. CalOPPA is working to protect personal information and there should be a standard for what needs to be said and done by developers.

– Evan D’Abrosca, West Warwick, Rhode Island, 3L

THE DATA BREACH NOTIFICATION THAT CRIED WOLF: HOW CONNECTICUT’S OVERBROAD DATA BREACH NOTIFICATION STATUTE UNDERMINES THE EFFECTIVENESS OF CONSUMER PROTECTION

Connecticut’s data breach statute is a wolf in sheep’s clothing. That statute’s definition of “breach of security” is overbroad, encourages over-notification, and undermines the goal of protecting consumers from identity theft. In Connecticut, notification is triggered by mere access of personal information, a statutory feature that encourages over-notification. Over-notification refers to a Boy-Who-Cried-Wolf-like phenomenon. Specifically, when consumers receive many notices of breaches that do not result in identity theft, notices of high-risk breaches will be ignored because the “average” data breach poses no risk of harm – a result that clearly undermines the statute’s consumer protection goals.

Importantly, Connecticut’s data breach law only applies to Connecticut businesses. Therefore to the extent that data breach notices damage a business’s reputation (which they surely do) Connecticut businesses are placed at a disadvantage to similarly situated businesses in other states due to the greater frequency of required disclosure of breaches. Under Connecticut’s regime of over-notification consumer backlash ceases to be a free market force that rightfully punishes businesses that have exposed their customers to identity theft, thus making consumer backlash in this context an artificial, ineffective, and frankly unfair market force. While fully in line with Connecticut’s well-earned reputation as anti-business, this negative effect is likely unintended and certainly does not further the statute’s consumer protection policy goals.

Connecticut’s regime of over-notification fails to apprise consumers to notices of true threats to their financial security, which at best makes the statute ineffective and at worst puts consumers at greater risk of identity theft. The policy goal should be to provide more effective notice in the form of less volume and more substance. Such legislation needs to be re-drafted to optimize consumer protection while minimizing unnecessary harm and cost to Connecticut businesses. Until then, breach notices will continue to cry-wolf to Connecticut’s consumers, and Connecticut businesses will suffer under a law that is, in its effect, anti-consumer and anti-business.

– Jackson Raymond Schipke, Connecticut, 3L

LIMITED LEGAL REMEDIES FOR INJURED CONSUMERS: A CRITICAL VIEW OF HOW PRIVACY LAWS HAVE FAILED THOSE THEY CLAIM TO PROTECT

A common motif in privacy law is the overarching concern for “consumer protection.” Curiously, these laws offer extremely limited avenues of recovery for individual consumer-victims of a data breach. Generally, most state data breach laws (and overlapping sector-specific federal laws) require commercial entities to merely notify consumers in a timely manner to avoid liability. If the commercial entity fails to timely notify consumers, it faces potential sanctions to individual states and federal agencies rather than the consumer-victim.

This appears to be a flaw in the overall scheme of privacy law—the same legal scheme that is built around a pillar of consumer protection. Accordingly, some consumers have sought recovery in the form of state tort and contract actions. (See *Walgreen, Co. v. Hinchy* 21 N.E.3d 99 (Ind. Ct. App. 2014)). The infamous *Hinchy* decision temporarily sent a chill down the collective back of the private sector, yet this case is confined to its riveting but very extreme set of facts. On the whole, it does not appear that state common law actions—absent egregious factual circumstances—are a true avenue for individual recovery.

The current patchwork quilt of American privacy law appears to offer only an illusory remedy to consumer-victims of data breaches. The only way to truly combat this flaw is to re-write significant portions of privacy law to provide adequate remedy for the actual consumers harmed by data breaches. Wholesale changes are admittedly politically unrealistic and raise counter policy concerns such as a sudden burden on the judiciary or the enigmatic "flood gates" concern. From the perspective of the consumer, rewriting privacy law to allow for private lawsuits may do more harm than good. Hypothetically, the cost liability of these lawsuits would likely be pushed on the consumer in the form of increased prices. Similarly, these lawsuits could deplete the coffers of a defendant-business and render it insolvent before more serious injuries to consumers manifest themselves. In sum, it is incumbent on policy makers to ensure that the consumer is, in fact, adequately protected. Allowing an avenue for individual lawsuits in the event of a data breach is potentially a rather axiomatic solution to the consumer protection hypocrisy in privacy law policy. Yet, if implemented, this solution must be appropriately tapered to preemptively address the various nuances and counter policy concerns that undermine such an approach.

– William C. Burnham, Monmouth County, New Jersey, 2L

DAMNED IF YOU DO, DAMNED IF YOU DON'T: WHY THE FTC'S LACK OF PRIVACY REGULATIONS MAY LEAD SOME BUSINESSES TO ABANDON BEST DATA PROTECTION PRACTICES

I chose to write my privacy law paper on the FTC and its seemingly limitless enforcement authority. Specifically, I argued that the FTC's lack of clear regulations makes it difficult, if not impossible, for companies to be sure that their data protection systems are sufficient to protect them from FTC enforcement actions and the related penalties. I likewise asserted that the FTC's failure to promulgate such regulations could ultimately prompt some companies to abandon best data protection practices altogether, as such practices can be expensive to implement, and they still do not seem to shield businesses from unwanted FTC involvement.

I was inspired to pursue this topic after we discussed the FTC's recent enforcement actions against Wyndham Hotels and LabMD, both of which have since contested the FTC's enforcement authority in the areas of data and privacy protection, and have argued that the FTC's lack of enforceable regulations infringes on companies' right to due process. Interestingly enough, these are the first two companies to challenge the FTC in such a manner, and though it is still unclear whether they will prevail, it is my sincere hope that these two cases will at least prompt the FTC and/or the federal government to implement more structured, workable privacy regulations that companies can follow, and in doing so, can be sure that they will not be subject to FTC enforcement actions.

– Kayla O'Connor, Middleboro, Massachusetts, 3L

WARRANTLESS SEARCHES OF TEXT MESSAGES: BIG BROTHER IN 160 CHARACTER INSTALLMENTS

The modern Fourth Amendment jurisprudence surrounding warrantless searches of text messaging is varied and evolving, including issues currently facing Rhode Island and the rest of the nation. My paper focused primarily upon comparing the reasoning of the Rhode Island Supreme Court in *State v. Patino* to

that of the United States Supreme Court in *California v. Riley* (the seminal case on warrantless searches).

In addition, the paper discusses the wide-ranging implications of privacy in text messages with a focus on current events in Rhode Island. Such concerns include incidents of police misconduct, such as the assault and battery of John Prince as detailed here by Samuel Esther Adler-Bell. The versatility of text messages and other online communications may invoke statutory (e.g. HIPAA) as well as Constitutional rights. See, e.g., Rhode Island House Bills 15-5177, 15-5597 (allowing health insurance billing for services conducted via telemedicine).

– Jeremy Rix, Warwick, Rhode Island, 3L

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy and Security Team.
