Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

May 5, 2016

DATA PRIVACY

Blockchain: What Is All the Buzz About?

Blockchain technology, introduced as the magic behind Bitcoin, is being touted by many as the next major disruptive innovation—in global trade and way beyond.

At its core, blockchain shifts the accounting function from third-party financial institutions and intermediaries to thousands of nodes (computers) on the blockchain network that collectively maintain a public ledger of verifiable transactions. Another important function of the blockchain is that it validates the availability of funds or assets of each party in a transaction. These functions significantly reduce transaction costs and facilitate immediate and direct transfer of funds or assets. According to a recent report from Santander InnoVentures, banks alone could save $15-20 billion per year by 2022 by using blockchain technology in support of cross-border payments, securities trading, and regulatory compliance.

Substantial investments recently announced by the likes of Goldman Sachs, JP Morgan, and IBM make it very clear that blockchain technology is here to stay and will undoubtedly disrupt many industries besides banking. Hundreds of online articles identify existing Blockchain applications, but mostly speculate on future use cases, in areas such as: stock trading, smart contracts (legal), voting, academic records, land/property ownership records (public sector), media, insurance, etc.

Blockchain is going to affect all of us before long, so we need to understand its impact on our security and privacy. Importantly, no personally identifiable information is written to the public ledger. Instead, a very long string of characters, which represents an account or personal wallet, is recorded to ledger transactions. Blockchain's design is inherently resistant to the effects of hackers, though it is not invulnerable. In my estimation, the biggest risk comes from its "permisionless" design in which anonymous computers can participate in the collective maintenance of the public ledger. In fairness, the design is quite sophisticated and even a limited hacking would reportedly require more nodes and/or more computing power than the thousands of good nodes on the network.

It is interesting that IBM announced, just last week, it is launching its framework for using a highly secure and auditable form of the blockchain technology that uses a "permissionless" model for network nodes. Certainly, the additional security, backed by Big Blue, will accelerate adoption by their enterprise clients and other organizations and industries.

— Fernando P. Monteleone

Web Trackers: What Others May Know about Your Online Footprint

Web trackers have been a hot topic in recent news, yet most of us are oblivious not only to the extent they are used but also to the potential for misuse of our personal information currently being aggregated in countless databases around the world.

On the day of this writing, I searched for “cordless drill” on the websites of three very familiar, top-20 global retailers and counted a total of 171 trackers. These trackers are essentially programs that execute when a website page is visited or some action is taken by the user, such as performing a search or clicking on a link or an item of interest. The programs are generally written by companies that benefit financially through targeted advertising or by the sale or use of the aggregation of the data (i.e., “Big Data” – large databases typically analyzed to identify patterns or trends in human behavior). With the exception of a hijacked website, trackers that exist on any given website are the products of the website owner or their invited partners or affiliates.

Most of us have experienced a targeted ad (e.g., for a cordless drill) while on Facebook and concluded that it was in connection to a previous search for that item on another site. Some of us may generally be OK with tracking for that purpose. But would we be OK knowing that a database may contain much more personal information, such as finances, health, religious beliefs, political affiliation, race, ethnic background, or even sexual preferences? Would it concern you even more if these tracker programs were recording our Internet activity over time and establishing long-term profiles of us on an individual basis?

Many of us think that we are surfing the web anonymously, but is that really true? There have been numerous reports and research studies over the past decade that show how personal identity could be obtained by Web Trackers—even when no personal website login information was entered. As social media was becoming extremely popular, representatives from AT&T Labs and Worcester Polytechnic Institute published a research paper making it clear that default settings of many social networking applications caused personally identifiable information (PII), such as our name, location, gender, activities, employer, and even our friends list, to be accessible to tracker programs. More recently, it was discovered that simply surfing the web from a device associated with a major cellular provider exposed personal account information to trackers, essentially connecting “anonymous” web activity to an individual.

In fairness, most of the sites we visit on a regular basis publish and comply with their information privacy policies generally limiting use of the data to targeted ads and/or broad, nonpersonal categorizations of aggregated data. Google, for example, currently has only one tracker (owned by Google) that executes when a search is performed. Based on its information privacy policy, its tracker program would essentially just record the interest in a cordless drill (using the same example as above). While they would also likely record geolocation of the user and other categorical information that would be useful for data analytics and general marketing, they do not associate the activity with an individual. On the other hand, if a typical retail website has 50 or more trackers, most of which are third-party owned, how can you feel comfortable that the actual data recorded and its use will be consistent with the information privacy policy of the site owner?

While concerned end users, security researchers, and lawmakers will continue to identify unscrupulous behaviors and effect change consistent with our collective privacy interests, I would like to leave you with a few suggestions to help you take matters into your own hands. First and foremost, review and revise any available privacy settings to meet your comfort level (e.g., limit sharing of name and location information to your friend list) and know the information privacy policies of all your social network applications and any applications/websites that you use to record or share personal information. Find and install tools that make web trackers visible to you and, more importantly, allow you to selectively block them from embezzling your personal data. Consider the Ghostery Browser Extension, which is highly rated by users and free.

— Fernando P. Monteleone

CYBERSECURITY

Chubb Advisory Warns Construction Industry of Increased Risk of Cyber-Threats

In its advisory entitled "New Business Models, Technology Raise Professional Liability Risks for Contractors," Chubb has outlined the risks of cyber-threats associated with new technologies being used by the construction industry.

As with other industries, the construction industry is increasingly utilizing the Internet and technology in its day-to-day operations. This includes building information modelling (BIM) software, customer data, personal information, critical infrastructure designs, and industrial control systems information.

The increased use of technology and software in design and building, and storing the data in the cloud, increases the risk of data exposure for contractors. For instance, BIM software programs include designs, building plans, and project files, all of which are valuable to hackers. As such, they are targeted by hackers and at risk.

According to Chubb, "Hackers have reportedly shown interest in building designs in recent years, and sophisticated malware that targets computer-aided design programs has been identified."

Critical infrastructure and industrial control designs are at particular risk, for obvious reasons. Designers, builders, and construction companies don't always recognize the importance of the information they generate and maintain, and when the data is digital, it is targeted by cyber criminals. The Chubb advisory is a good reminder that the construction industry is at risk of cyber-threats and may wish to consider assessing the security practices used to protect its design, BIM, and construction data.

— Linn Foster Freedman

DATA BREACH

American Dental Association Inadvertently Mails USB Drives Infected with Malware to Its Members

The American Dental Association (ADA) recently mailed 37,000 credit card-sized flash drives to its members that included new billing codes, entitled 2016 CDT Manual. Unfortunately, also included on the USB drive was malware used by criminals to infect users' systems that allows full access to the system. So when the 37,000 dentists put the USB drive into their computer, thinking they were getting the new billing codes, they were directed to a known web page that distributed malware, which presumably infected their systems.

Apparently, the USB drives were manufactured in China by one of the ADA's vendors. China is obviously notorious for being a source of cyber-attacks.

When the ADA found out about the problem through "a handful of reports," it sent an email to its members, saying, "Your anti-virus software should detect the malware if it is present. However,if you haven't used...the flash drive, please throw it away." It then provided instructions on how to download a pdf version. Not sure why they didn't send the pdf version the first time.

The ADA stated that it will review whether to continue to distribute products through physical media.

I am thinking we will hear more about this story from the dentists whose antivirus software did not detect the malware. All you dentists out there: beware.

— Linn Foster Freedman

Stolen User Credentials Account for Over Half of All Data Breaches in 2015

Verizon recently released its yearly Data Breach Investigations Report, and as always, the report is a very informative read. The report gathered information from more than 64,000 security incidents worldwide in 2015, 2,260 of which were actual data breaches.

One of the report's most alarming statistics reveals that legitimate user credentials were used in most 2015 data breaches. Particularly, Verizon reports that legitimate user credentials were used in the majority of 2015's data breaches, with some 63 percent of users using stolen, weak, or default credentials.

"I knew credentials were a thing, obviously. What I wouldn't have thought was that over half [of breaches] involved credentials," says Marc Spitler, senior manager at Verizon Security Research and co-author of the report. "I knew it was a significant issue and knew we wanted to talk about it in the report, but I didn't quite know it would be that high."

Stolen credentials tops the list of threat actions associated with attacks involving legitimate credentials, followed by C2 malware, exporting of data, phishing, and keyloggers.

These findings underscore the importance of awareness among businesses and government agencies on password management controls to combat this attack mechanism.

— Kelly Frye Barnett

ENFORCEMENT + LITIGATION

Trump Campaign Sued for Sending Spam Texts in Violation of TCPA

Donald J. Trump for President, Inc., which is the official campaign committee for candidate Donald Trump, was named in a putative class action case on April 25, 2016, for sending unwanted text messages to individuals. The case was filed in federal court in the Northern District of Illinois.

The suit alleges that the text messages were sent to the individuals in violation of the Telephone Consumer Protection Act. The content of the text requested that the individual subscribe to the campaign and that if they did, it would "help make America Great Again!"

The suit alleges that the texts were sent without express written consent, which is required by TCPA. The suit alleges willful violation of the TCPA, which carries statutory damages of up to $1,500 per text.

— Linn Foster Freedman

Pennsylvania Transit Sued for Fair Credit Reporting Act Violation

Last week, the Southeastern Pennsylvania Transportation Authority (SEPTA) was hit with a class action alleging violations of the Fair Credit Reporting Act (FCRA) for not sufficiently notifying job applicants of its use of credit checks, as well as violations of the Pennsylvania Criminal History Record Information Act by discriminating against applicants convicted of drug felonies. Class representative, Frank Long, claims that he (along with thousands more) did not receive the required written disclosures under the FCRA and was subject to a blanket policy of rejecting all applicants with a felony job conviction if the position applied for involved operating a vehicle. Long was convicted of drug possession and manufacturing in 1997; however, Long argues that the conviction should not have had any effect on the bus driver position he applied for because of the nature of the crime and the length of time that had gone by without any further convictions. The suit seeks to represent all SEPTA job applicants denied consumer report disclosures within the last two years and all applicants denied vehicle maintenance or non-paratransit driving jobs based on drug convictions more than seven years old. The lesson here is to know FCRA requirements and to keep up to speed on your state's laws, too.

— Kathryn M. Rattigan

Georgia Couple Prosecuted for Filing Fraudulent Tax Records

The filing of fraudulent tax returns continues to be a serious problem in this country. Last year alone, the IRS has admitted that up to 720,000 taxpayers were victims.

Last week, a Georgia couple pled guilty to filing fraudulent tax returns by using the IRS "Get Transcript" site. The couple used the personal information (including Social Security numbers) of five individuals that they obtained from another source to file fraudulent tax returns in those individuals' names and obtain a refund from the IRS on prepaid debit cards. They then bought money orders with the debit cards.

The husband admitted to one count of conspiracy to commit money laundering, which carries a maximum sentence of 20 years in prison, and the wife admitted to one count of withdrawing money to evade bank reporting requirements, which carries a maximum sentence of 10 years.

The case was investigated by the IRS and is being prosecuted by the Department of Justice in the federal district court of Northern Georgia.

Although this case only represents fraud against five individuals, prosecuting these cases will hopefully be a deterrent against future fraudulent schemes.

— Linn Foster Freedman

HEALTH INFORMATION PRIVACY

Telemedicine Nursing Licensure Compact Legislation Enacted in Six States and Seven More Right Behind

In another case of technology outpacing the law, telemedicine has continued to push the limits of state medical professional licensure laws.

Generally, physicians and nurses must be licensed in the state in which they are practicing; yet technology has become so sophisticated that telemedicine is allowing those medical providers to provide access to medical care beyond the boundaries of an individual state.

To break down barriers of state lines, six states have enacted legislation that would adopt a licensure compact to allow nurses to practice telemedicine across state lines. The states are Idaho, Wyoming, Virginia, Tennessee, Florida, and South Dakota. These states allow licensed nurses to practice telemedicine for patients in any of these states utilizing their home state license, with conditions and restrictions.

The idea has caught on, and seven more states are considering similar provisions.

Opponents to nursing telemedicine and the licensure compact say that different licensing requirements could negatively affect patient care, as some state licensure agreements are more stringent than others.

On a similar note, New York has introduced regulations that would allow psychiatric providers to use telemedicine to consult with patients through live video conferencing, providing additional opportunities for patients to have greater access to psychiatric care.

— Linn Foster Freedman

PRIVACY TIP #33

Shopper Tracking Billboards

I have commented before on the use of location-based services on mobile telephones and that apps (and your telecommunications provider) use and sell your location data for all sorts of purposes without your knowledge. The choice is yours as to whether or not you allow apps to have access to your location. The same is not true if you use an E-ZPass. Have you ever seen those signs on the side of highways that say "20 miles and 22 minutes to…?" They look like construction signs but are electronic tracking devices that are tracking E-ZPasses to determine how fast it takes to get from one of those digital signs to the next. If you don't like that idea, your only option is to wrap your easy pass in foil and take it out when you need it. Yes, people really do that.

There is also no consumer choice when it comes to shopper-tracking billboards. Huh?? What in the world is a shopper-tracking billboard?

Earlier this week, Senator Chuck Schumer requested that the Federal Trade Commission investigate Clear Channel Outdoor America's RADAR initiative, which he allegesis about "spying billboards."

According to Senator Schumer, the Clear Channel Outdoor RADAR campaign "has tens of thousands of mobile and digital billboards across the United States and plans to provide advertisers with data on individuals who pass its billboards—some of which are equipped with small cameras that collect information" that the company will use to determine personal characteristics of individuals such as age and gender.

Senator Schumer argues that the "unsuspecting individuals" whose information is being captured by these spying billboards should be able to opt out of having their data collected in this manner. Clear Channel says its "RADAR campaign measurement solution is a partnership with privacy-compliant third-party data providers who are already collecting mobile data and have verified that they adhere to consumer-friendly business practices." I am not sure what "consumer-friendly business practices" are, but

I am pretty sure consumers have no idea that their telecommunications provider is tracking their location through billboards and selling it.

At any rate, Senator Schumer is on the pulse of new technology and data collection and use, and this is another reminder of how your location-based service can be used. Check your location settings again and take control of how your data is accessed and used. To each his own but be in control of the choice.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team regularly serve as presenters at topic-related seminars, and participate on panels that discuss developments in the area. Several speaking engagements at scheduled events are featured below:

Upcoming

- May 12 – Construction Risk Partners in New York City (Linn F. Freedman)
- May 20 – Annual Massachusetts Bar Association Health Law Conference (Linn F. Freedman & Kathryn M. Rattigan)
- June 7 – The Quorum Initiative Cyber Intrusions event in Washington D.C. (Linn F. Freedman)
- June 8 – The Quorum Initiative Cyber Intrusions event in New York City (Linn F. Freedman)
- June 22 – National Scholarship Providers Association in Farmington, CT (Linn F. Freedman)
- June 23 – MCLE: Data Security 2.0: The Cloud, Mobile Devices & Encryption Webcast Panel (Kathleen M. Porter)
- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + 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 + Security Team.