June 30, 2016

DATA PRIVACY

Facial Recognition Guidelines Issued by NTIA and Approved by IBIA

On June 15, 2016, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) issued its facial recognition best practices, which were developed by a multistakeholder group convened by NTIA. The best practices document, titled "Privacy Best Practice Recommendations for Commercial Facial Recognition Use," is intended to be a code of conduct for the commercial use of facial recognition technology.

The best practices are considered voluntary, but they encourage those using facial template data to:

- be transparent about the collection, storage and use of personal data;
- develop facial template data management practices;
- allow individuals the opportunity to control the disclosure and sharing of their facial template data;
- implement appropriate security measures to protect the data; and
- allow consumers to contact the business regarding its use of facial template data.

The guidelines are "intended to provide a flexible and evolving approach to the use of facial recognition technology, designed to keep pace with the dynamic marketplace surrounding these technologies."

Following the issuance of the best practices by NTIA, the International Biometrics + Identity Association (IBIA) endorsed the facial recognition best practices on June 22, 2016. IBIA is "the leading international trade group representing the identification technology industry." In its statement endorsing the guidelines, IBIA indicated that it was "proud to be part of this collaborative process.…These privacy best practices will help to assure the public that facial recognition is being used responsibly and accountably. They also demonstrate the strong commitment of the industry to protecting the public's privacy, even as new technologies and applications emerge."

— Linn Foster Freedman

DATA BREACH

Massachusetts General Hospital Vendor Patterson Dental Supply Reports Breach of 4,300 Patient Records

Patterson Dental Supply, Massachusetts General Hospital's (MGH) vendor that provides software to the hospital to manage dental practice information, has reportedly admitted that approximately 4,300 of MGH's patient records have been accessed by an unauthorized individual who "gained access to electronic files on the company's systems in early February."

The information compromised included patient names, dates of birth, Social Security numbers, and, for some patients, the type of dental appointment, provider name, and medical record numbers.

Despite the fact that the unauthorized access was to Patterson Dental Supply's system, MGH began notifying patients on June 29, 2016, and set up a call-in center to answer patients' questions.

— Linn Foster Freedman

CYBERSECURITY

Banks Embracing Biometric Technology

Passwords are a pain to keep track of, and it is well known that consumers use the same password for multiple platforms because none of us can remember multiple complex passwords. So, a hacker who gets ahold of one password, can use that password to gain access to multiple accounts.

The nation's largest banks are well aware of their customers' shortfalls when it comes to password management, and therefore, some of the larger banks are embracing biometric technology to replace the traditional password for authentication and access to banking information.

Bank of America, JPMorgan Chase, and Wells Fargo customers reportedly use fingerprint scans to log into online banking accounts with their mobile phones. More and more banks will be rolling out biometric technology for authentication in the future, including iris scans for wiring instructions and voice recognition for credit card transactions (instead of "What is your mother's maiden name?"). USAA is using facial recognition technology to identify its military customers.

The financial services industry is usually ahead of the curve when it comes to data security. Because almost a third of U.S. citizens' Social Security numbers were exposed in health care breaches alone in 2015, biometric technology is the new wave of authentication. We expect to see other industries follow the banking industry and rapidly embrace biometric technology to replace passwords in the very near future. And we thought the movie Minority Report was futuristic and creepy—it's reality now.

— Linn Foster Freedman

FBI Reports $3.1 Billion Lost by Businesses through "Business Email Compromise"

Wire fraud crime has long been a problem for financial institutions and banks. However, wire fraud through email is a completely different beast. Originally characterized by law enforcement as an extension of traditional wire fraud, wire fraud by email has become so pervasive that it now warrants its own internet crime designation: business email compromise (BEC). Under the FBI's definition, BEC scams target businesses that have international business relationships and regularly send wire transfer payments. In other words, a BEC scam is a type of wire fraud conducted through emails that are compromised because the sender's identity or email has been hacked or spoofed and/or because the recipient at the business is tricked into believing the email is legitimate. A previous blog post described some of the ways a phishing or spearphishing email targets a victim.

A recent push by global law enforcement agencies to correctly identify BEC scams, as well as concerns about increased activity, has led to a disturbing statistic: since January 2015, there has been a 1,300 percent increase in exposed losses worldwide due to BEC. This startling increase includes reports made to the FBI's Internet Crime Complaint Center (IC3) and other international law enforcement agencies. The losses come from 22,143 total reported cases from U.S. and foreign victims from October 2013 through May 2016. While the IC3 tracks other internet crimes that use email, such as ransomware, extortion, and emails targeting individuals, losses from BEC, as well as the dramatic increase in victims, clearly have the FBI's attention.

BEC hackers and scammers involved are sophisticated—they monitor and study their victims for extended periods. They first identify the individuals at a business in finance, accounting, or treasury functions who may send wire transfers. Then, they study the habits of these businesses and the individuals on LinkedIn, Facebook, and other social media and wait for the right moment. Familiar BEC scams include emails from (i) a foreign supplier of a business with "new" wire transfer instructions for the next invoice payment, (ii) a travelling executive to a finance employee of the business to request an "urgent" "confidential" wire transfer, (iii) the fraudster using a spoofed email to pose as a legitimate employee, customer, or supplier of the business, or (iv) the fraudster posing as the attorney for the business requesting wire transfers relating to transactions or deals that are soon closing.

How do you protect your business from a BEC scam?

- Provide training and awareness within the business about BEC scams.
- Don't open spam, or attachments from spam, or click on links from unknown sources.
- Avoid using free web-based email accounts for the business, as it is easier to spoof emails.
- Check the sender's email by hovering over it to confirm it is not spoofed.
- Don't reuse the same or old passwords across social media and other platforms.
- Don't use your business email address to sign up for social media platforms and don't use the same password as your work email. For example, if you signed up for Linkedin using your corporate email in 2012, your username and password is probably readily available on sites such as leakedsource.com that specialize in cataloging data breaches.
- Tighten wire transfer procedures, restrict the number of individuals involved in sending wire transfers, and verify changes with the supplier or sender of the email. Don't use the phone number in the requesting emai—it may be fraudulent as well.
- Implement two-factor authorization for corporate email accounts.
- Create intrusion detection system rules that flag emails with extensions that are similar to company email. For example, legitimate email of abc_company.com would flag fraudulent email of abc-company.com.
- Be familiar with your supplier's and customer's habits, such as the details of, reasons behind, and amount of payments.
- Review email requests for transfers of funds to determine if the requests are out of the ordinary.

If you do fall victim to a BEC scam, it is important to act quickly. Contact your financial institution immediately and ask it to contact the financial institution where the wire was sent. Contact your local FBI office and legal counsel. File a complaint, regardless of dollar loss, at www.IC3.gov.

— Kathleen Porter and summer associate David Wang

IRS Shuts Down Electronic Filing PIN Program

Last week, the IRS announced that the electronic filing personal identification number tool (e-file PIN), used by taxpayers to verify their signature on their tax filings, "is no longer available."

The IRS admitted in February 2016, that cyber criminals were attacking the system and had accessed more than 100,000 taxpayers PINs. It did not shut down the system because the PINs were used in commercial tax return software programs, and it would be disruptive.

Apparently, the IRS detected additional attacks on the system by cyber-attackers and decided enough was enough and shut the system down. It is not much of a surprise that hackers continue to try to get into the IRS system and steal taxpayer information, as the information in tax returns includes names, addresses, Social Security numbers, and financial information—the treasure trove of personal information. When will the IRS use the same security measures as the Department of Defense?

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

FTC Warns Telemarketers about Prohibition of Certain Payment Methods

The Federal Trade Commission (FTC) issued an alert this week reminding businesses that the Telemarketing Sales Rule (TSR) amendments, which went into effect in November 2015, prohibit telemarketers from using three types of payment methods that have been used by con artists and scammers.

According to the FTC, "as of this month, it is illegal for telemarketers to ask consumers to pay for goods or services using cash-to-cash money transfers, such as MoneyGram and Western Union provide, or by providing PIN numbers from cash reload cards such as MoneyPak, Vanilla Reload, or Reloadit packs. It also is illegal for telemarketers to use unsigned checks called 'remotely created payment orders' to withdraw money directly from consumers' bank accounts."

The FTC has provided business guidance for telemarketers to use to comply with the new rule, as well as guidance that warns consumers that "any telemarketer requesting payment using these methods is a scammer because the payment method is illegal."

Telemarketers—be aware of the new rules that go into effect this month. Consumers—beware of any telemarketers that attempt to use these methods as they are illegal.

— Linn Foster Freedman

Facebook Wins Appeal over Storing Nonuser Data In Belgian Court

The Belgian data protection authority has lost its legal battle with Facebook over whether the social network could track the online activities of non-Facebook users in Belgium who visit Facebook pages.

Belgium's data protection regulator took Facebook to court a year ago, accusing it of breaking EU privacy law by tracking people without a Facebook account without their consent.

At the heart of the case was a so-called 'Datr' cookie, which Facebook said it uses to protect its platform and the data of its users against "malicious attacks." Facebook places the function on people's browsers when they visit a Facebook.com site or click a Facebook 'Like' button on other websites, allowing it to track the online activities of that browser.

The lower court ruled in favor of the regulator and ordered Facebook to stop storing the data or face a daily fine of 250,000 euros ($277,800). After the ruling, Facebook said it would comply and stop using the 'Datr' cookie to track nonuser activity. Shortly thereafter, Facebook appealed the ruling to the Brussels Court of Appeal.

The Court of Appeal disagreed with the lower court's decision, and the case was thrown out because the social media network's European servers are in Ireland, not Belgium.

In light of the ruling of the Brussels Court of Appeal, Facebook can now start showing its pages to Belgians who aren't signed up to its service.

— Kelly Frye Barnett

HEALTH INFORMATION

Connecticut Legislative Update: Public Act 16-77: An Act Concerning Patient Notices, Designation of a Health Information Technology Officer, Assets Purchased for the State-Wide Health Information Exchange and Membership of the State Health Information Technology Advisory Council

This legislation (P.A. 16-77) makes substantive and technical changes related to Public Act 15-146, a major public health and health care bill passed by the Connecticut legislature during its 2015 legislative session.

Connecticut Health Insurance Exchange Consumer Information Website

Under current law, Connecticut's Health Insurance Exchange (HIX) is required, within available resources, to establish and maintain a consumer health information website by July 1, 2016. The HIX website must include price and cost information for the most common inpatient diagnoses and procedures, outpatient procedures, and surgical and imaging procedures, listed by health care provider and categorized by third-party payer, based on a list published by the Department of Public Health (DPH) and the Insurance Department (CID) on their websites (Joint Report).

Current law provides that, starting January 1, 2017, hospitals will be required to inform a patient of the patient's right to request cost and quality information at the time of scheduling a diagnosis or procedure for nonemergency care listed on the Joint Report. If the patient requests such information regarding the diagnosis or procedure, a hospital must, within three business days, provide the patient information on (1) the amount the patient will be charged if uninsured, including the amount of a facility fee; (2) the Medicare reimbursement amount; (3) if the patient is insured, the allowed amount and the insurer's contact information so that the patient may obtain additional information regarding charges and out-of-pocket costs; (4) the hospital's Joint Commission composite accountability rating and Medicare star rating; and (5) the website addresses for the Joint Commission and Medicare hospital compare tool. If the patient is insured and the hospital is out-of-network under the insurance policy, the hospital's notice must also state that out-of-network rates may apply.

P.A. 16-77 delays the implementation date for requiring hospitals to provide patients with notice of their right to request cost and quality information. Under this legislation, hospitals will not be required to provide such notices until 180 days after the CID and the DPH issue the Joint Report on their websites. Additionally, in the event a patient's diagnosis or procedure has no corresponding Medicare reimbursement amount, this legislation requires a hospital to instead notify the patient of either the approximate amount or the percentage of the hospital's charges that Medicare would have paid for the services. P.A. 16-77 also clarifies that the location or setting of scheduled nonemergency care is immaterial for purposes of implicating the notice requirement.

Health Insurer Consumer Information Websites

Current law requires health insurance carriers in Connecticut to maintain a website and toll-free telephone number to allow consumers to obtain insurance cost and network information related to specific procedures and providers by July 1, 2016. P.A. 16-77 delays the deadline for establishing this website until January 1, 2017, and also exempts all health insurance carriers with less than 40,000 covered lives in Connecticut from having to maintain such a website.

— This post was co-authored by Stephen W. Aronson, Lisa M. Boyle, Leslie J. Levinson, Brian D. Nichols, Lisa M. Thompson, Theodore J. Tucci, Pamela H. Del Negro, Meaghan Mary Cooper, Nathaniel T. Arden, Conor O. Duffy, and Erica S. Youngerman and is being shared from our Health Law Pulse publication. If you're interested in getting updates on developments in health care, we invite you to subscribe to our publication.

PRIVACY TIP #41

Tape Over Your Laptop Camera and Microphone

When I train clients' employees on data privacy and security, I always mention the microphone on smartphones. They are powerful and if you allow apps access to your microphone, they can listen to every one of your conversations [see related privacy tip]. Do you want every one of your conversations to be accessible by someone who is not part of the conversation? I find that people still don't understand how the microphone on their phone can pick up virtually every conversation if the microphone feature is on all the time. Take a look at the microphone setting on your phone and turn it off when you are not using the particular application that has requested access to the microphone.

News broke this week that the CEO of Facebook "tapes over his camera and microphone" on his laptop. Let's just admit that the CEO of Facebook is pretty tech savvy.

Security experts say that hackers are able to gain access to devices, including laptops and smartphones through the use of remote-access Trojans—a process known as "ratting." They gain access to the camera of your device and can literally watch you while you are at your computer. That's pretty creepy. They then try to use the images for everything from voyeurism to extortion. And it is a growing problem--especially for women.

Security experts say that taping over the camera and microphone of your device is a good security practice and will keep hackers from being able to spy on you. It is a cheap and effective security tool.

It is reported that not only does the CEO of Facebook tape over the camera and microphone, but also the head of the FBI does too. Hmmm….going to find some tape...

Of course, I couldn't find any masking tape or electrical tape in our home, but I found weather stripping, which did the trick. The camera and microphone on my laptop are now weather stripped against hackers.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

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

- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)
- September 12 - 15 – ASIS 2016: 360° VISION in Orlando, FL (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)

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.