February 4, 2016

EU PRIVACY

EU and U.S. Agree to New Safe Harbor Data Transfer Pact

The U.S. Department of Commerce and the European Commission announced on Tuesday that they have entered into a new transatlantic safe harbor transfer agreement, which comes two days after the deadline set by EU data protection authorities.

According to the EU Commission, the pact, known as the EU-U.S. Privacy Shield, includes stronger obligations for U.S. companies to protect the personal data of EU citizens and will require monitoring and enforcement by the U.S. Department of Commerce and the Federal Trade Commission.

The pact will allow EU citizens to complain about misuse of their data through a newly created privacy ombudsperson for national security, and there will be limitations on law enforcement and intelligence authorities' access to EU citizens' data.

The deal will be presented to the EU's College of Commissioners for approval. Separately, the Article 29 Working Party is expected to announce its plans for enforcement of transatlantic data transfers in the next few days.

— Linn Foster Freedman

DATA BREACH

UVA Notifies Employees of Illegal Access to Human Resources Information through Phishing Scheme

The University of Virginia (UVA) has notified approximately 1,400 of its employees that unauthorized individuals were able to access its HR system and the personal information of 1,400 employees of the Academic Division. The intruders launched a successful phishing attack asking for employees to provide usernames and passwords. The successful phishing attack scored the W-2 forms (including names, addresses, and Social Security numbers) of 1,400 employees and the direct deposit banking information of 40 employees from 2013 and 2014.

UVA was unaware of the intrusion, which occurred between early November 2014 and early February 2015. The FBI notified UVA following an "extensive law enforcement investigation."

UVA is offering the affected individuals one year of free credit monitoring and identity protection services.

This is another example of how important training is for employees about phishing and spear phishing attacks. The attacks have become more sophisticated, and the hackers are using social engineering to dupe employees into clicking on links and providing the keys to the company's kingdom. Companies may wish to consider intensifying employee training to effectively combat these attacks, which have been on the rise for some time.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Victoria's Secret Hit with TCPA Class Action for Text Messages

Last week, Victoria's Secret was hit with a class action in California alleging that the lingerie company sent Michael Hannegan almost 100 texts in one day in violation of the Telephone Consumer Protection Act (TCPA). Hannegan admits he did opt in to receiving promotional texts from Victoria's Secret in May of this year, but Victoria's Secret said it would only send 6 text messages per month in its confirmation text.Hannegan's complaint says, "Because the initial opt-in message that defendant sent to plaintiff stated that he would receive no more than six messages per month, any additional messages beyond the first six messages he received in any given month were unauthorized and sent without plaintiff's consent in violation of the [TCPA]." Hannegan calls Victoria's Secret's text messaging marketing campaign "misguided" and now seeks to certify a class of consumers across the country who received more than 6 text messages in one month over the past four years and seeks an injunction against Victoria's Secret as well as damages. This is a new type of TCPA claim; while Victoria's Secret appears to have obtained prior express consent in accordance with the TCPA, it also appears to have overstepped the boundaries of the consent. We will watch this case to see how far it progresses.

— Kathryn M. Rattigan

Eight District Attorneys in Oklahoma Sued for Wrongfully Disclosing Personal Information in Court Filings

Generally, court filings are public records unless sealed from public access by a judge. Vast amounts of personal information contained in public records can be, and are, accessed by criminals in order to obtain personal information of individuals, which can be aggregated with other information, to perpetrate fraud and identity theft.

For this reason, most federal and state courts have adopted local rules over the years that prohibit the filing of sensitive personal information like full Social Security numbers and driver's license numbers in court records.

But litigators don't always redact this information prior to filing documents in a court record, and it has been a recurring problem over the years. I still don't understand why every form set of Interrogatories to plaintiffs include requesting a full Social Security number. Litigators may wish to review whether they really need such sensitive information and want the responsibility of having to protect that sensitive piece of information and the consequences of its loss or misuse.

In Oklahoma, one woman is fighting back. She is suing the State of Oklahoma and eight district attorneys for wrongfully disclosing her birth date and full Social Security number in publicly available court

documents.

The suit, filed last week, alleges that DAs from 11 different counties in Oklahoma regularly file the dates of birth and full Social Security numbers of anyone involved in a civil or criminal dispute in the court system and that the information is available on the state's electronic Supreme Court Network.

In her case, she was arrested and charged with a misdemeanor. During the process, the police department obtained her personal information through the Oklahoma Department of Public Safety's electronic system. The information contained in the document from the Department of Public Safety was filed in the court proceeding and was available to the public through the electronic court system, and it included her full Social Security number.

According to the complaint, this practice has been taking place since 2012, and she is seeking to represent any potential class members whose birth dates and full Social Security numbers were included in the Oklahoma Supreme Court Network since February 1, 2012.

This case illustrates how important it is for state government employees to recognize the high-risk data of citizens that they have access to and how important it is to safeguard it. Public officials are responsible to implement privacy and security measures, just as private industry is. In this case, if you follow the data, the plaintiff's full Social Security number was accessed at a minimum by the Department of Public Safety, the police, the DAs office, and then allegedly the public when it was included in the electronic court system. On the surface, it is questionable whether the number was needed at all by any of these departments, so why was it accessed and disclosed over and over without someone catching it and questioning why it should be disclosed once again?

State governments may wish to review how they are handling citizens' sensitive personal information, including limiting access to it not only in court records but between departments and third parties as well. In the present environment, it is hard enough for us to protect our own information, but we need people to work together to protect our information as if it is their own.

We expect this case is a wake-up call to those involved in Oklahoma, but it should also be a wake-up call to other state government employees and all litigators too.

— Linn Foster Freedman

FTC Files Suit against Devry University for Deceptive Advertisement from Data

The FTC filed suit against Devry University on January 27, 2016, alleging that its ads stating that 90 percent of its graduates obtained jobs in their field of study and were making 15 percent more than graduates from other colleges and universities in their first year out of school, were deceptive.

In its claim for a permanent injunction, the FTC alleges that Devry ran English and Spanish ads through paper materials, TV, and social media, including its website, about the benefits of obtaining a Devry degree.

The basis for the statements in the ads comes from manipulations of data maintained by Devry's Career Services office. According to the FTC, the actual data does not substantiate the claims.

The claims in the Complaint include the fact that students were not included in certain statistics and others who should have been excluded were not, which skewed the statistics in a deceptive way.

The FTC also found that reliance on a third-party vendor who provided an income report also did not

substantiate the higher income claim. The complaint states that the assumptions and conclusions in the report "all gave or should have given Defendants reason to question the reliability of the conclusions and information contained in the report," including the fact that the statistics in the report "differed significantly" from Devry's internal statistics.

The FTC alleges that these claims were deceptive and a violation of Section 5 of the FTC Act.

Message for higher education institutions: consider implications of mining the data, skewing the data, and relying on third-party vendors in reporting the data before it is published and advertised.

— Linn Foster Freedman

Berkeley Students Sue Google for Mining Emails for Ads Through Apps for Education

Four students attending the University of California, Berkeley, sued Google last week, alleging that it violated the Electronic Communications Privacy Act by scanning and mining their emails in order to create advertising profiles after telling the university that emails would be private. The lawsuit claims that Google told Berkeley and other colleges and universities that if the ads were turned off in the Apps for Education account, then the users' emails and personal content would not be scanned for targeted ad purposes. According to the suit, despite this assurance to Berkeley and the other colleges and universities, Google scanned the emails between November 2010 and April 2014 specifically to target the users with advertisements.

The suit further alleges that, because of Google's representations to the colleges and universities, including Berkeley, Berkeley assured students and employees who used Apps for Education that their information would be private, which was not true.

The students are requesting that Google purge their data and seek damages of $10,000 each or $100 a day pursuant to the Electronic Communications Privacy Act.

— Linn Foster Freedman

Class Action Suit Dismissed against Georgia Secretary of State for Data Breach

We previously reported that the Georgia Secretary of State's office experienced a massive data breach in October and didn't find out about it until November. The breach affected approximately 6 million Georgia voters and included their names, addresses, dates of birth, driver's license numbers, and Social Security numbers.

Following the data breach and notification to affected individuals in November after the *Atlantic Journal-Constitution* exposed the breach, the Georgia Secretary of State's office was sued in a proposed class action case.

The case was voluntarily dismissed last week by the named plaintiffs as the suit accomplished their goal of making the state acknowledge that it happened and to "make sure this doesn't happen again."

Credit and identity theft monitoring has been offered to the affected individuals through February 14, 2016.

— Linn Foster Freedman

DATA PRIVACY

The Biggest Surveillance and National Security Event of the Year: Super Bowl 50

While you are dipping chips and pulling apart BBQ wings, over 60 federal, state, and local law enforcement agencies will be combining their efforts to survey the nearly one million people who will travel to the San Francisco area for Super Bowl 50. Agencies ranging from the Department of Homeland Security, the Drug Enforcement Agency (DEA), and the Transportation Security Administration (TSA) to the Secret Service and the Coast Guard have spent over two years planning for THE game. This means that, if you are attending the game or any events before or after the game in the area, you will be watched. All eyes will be on you. Here is a list of some of the types of surveillance expected to be in use in the San Francisco area:

- cell phone surveillance devices (including fake cell phone towers called stingrays or IMSI catchers that mimic cellular towers, tricking phones into linking to them)
- video cameras (many of them)
- automated license plate readers (with geolocation tracking)
- social media monitoring software (this is new)

Of course, no federal or state officials will confirm or deny the use of any of these types of surveillance. Officer Esparza of the San Francisco Police Department (SFPD) said, “The basic bottom line is that our best eyes and ears are the public who come and participate. If someone sees something, we are asking people to say something.”

The only other time this type of surveillance is used is for Presidential Inaugurations and for the Super Bowl that occurred right after 9/11, back in February 2002.

But where will they put all this data? How will they sort it? Well, right next door to the field is the Northern California Regional Intelligence Center. The name of the game is coordination. Federal, state, and local agencies will use this intelligence center to share information in hopes of thwarting and preventing any acts of terrorism. For those of you visiting San Francisco for the game, remember, they’re watching. For those of you sitting at home, enjoy the dip.

— Kathryn M. Rattigan

How Far Have We Gone with License Plate Photos and Location Tracking? Too Far...

Vigilant Solutions is a company that takes photographs of cars and trucks using its network of cameras. What’s the big deal? Traffic cameras are always recording our plates. Well, not only is Vigilant Solutions taking photos of your license plate, they are also retaining your vehicle’s location data along with the photo of your license plate, AND they are selling it. To date, Vigilant Solutions has taken approximately 2.2 billion license plate photos in almost every major city across the United States. Among Vigilant Solutions customers (i.e., those buying your license plate numbers and location data), 300 of them are law enforcement agencies. You might think to yourself, "Well, don’t the police need to get a warrant to put a GPS tracking device on my car." The simple answer is yes, but to get years of data on your vehicles location, all the police have to do is pay Vigilant Solutions.

Vigilant Solutions subsidiary's website, Digital Recognition Network, says, "All roads lead to revenue with DRN's license plate recognition technology. Fortune 1000 financial institutions rely on DRN solutions to drive decisions about loan origination, servicing, and collections. Insurance providers turn DRN's solutions and data into insights to mitigate risk and investigate fraud. And our vehicle location data transforms automotive recovery processes, substantially increasing portfolio returns." Is this reminiscent of George Orwell's 1984? With this type of tracking technology becoming more and more affordable, we are sure to see an increase in its use. As consumers (and individuals with constitutional rights), we should all be aware of this and speak up for our privacy rights.

— Kathryn M. Rattigan

NIST Seeks Comments on Randomness to Protect Sensitive Information

The National Institute of Standards and Technology (NIST) announced last week that it is seeking comments on its draft publication Recommendation for the Entropy Sources Used for Random Bit Generation. What does this mean in layman's terms?

Basically, in order to protect private messages, cryptography is used to encrypt the messages into a form that cannot be accessed or understood without using a random number that allows access. This is often used in two level authentication.

This publication provides recommendations that are designed to make sure the random numbers used are sufficiently unpredictable. According to NIST, "When you're accessing your process for generating randomness, you want to make sure nothing is broken and that it is performing consistently. We would like the public's input on ways we can improve these tests."

A public workshop to address these and other security issues will be held at NIST on May 2-3, 2016.

— Linn Foster Freedman

Backdoors to Encryption Protocols vs. Cybersecurity: Weighing Priorities in The U.S. and Abroad

With the revelation that the Paris and San Bernardino attackers used encrypted communications to recruit, communicate, and plan their attacks, the U.S. government is again pushing the tech industry to provide it backdoor access to encryption protocols. Bypassing security mechanisms through a backdoor, law enforcement believes, permits it to more effectively track users and content, providing a powerful tool to investigate terrorists and criminals. Proponents of backdoor access argue that it simply allows them to inspect a computer in the same way they can search a home. Without a backdoor, the government cannot access encrypted data, even with a warrant.

For security and other reasons, the tech companies are refusing the government's demands for backdoor access to the data. Rather than provide access, tech companies' priority is ensuring the everyday security of data against criminals. Most recognize that the sensitive nature and amount of information shared in Internet and mobile transactions makes keeping the information secure even more critical than providing government access to it. This means that most tech companies have built more recent versions of products and services so they have no access to encrypted data, let alone the ability to provide access to law enforcement. Last summer, this theory was tested as the Department of Justice obtained a court order against a tech company to turn over real time text messages between suspects using the company's phones. The company said it could not comply, as its messaging system was encrypted, and the real time texts were unavailable to it. Ultimately, the company turned over some of the stored messages, which were saved in an unencrypted fashion to the cloud.

Tech companies also argue there is no “law enforcement only” backdoor in encryption. Once created, backdoors weaken everyone’s security, as they can be detected and exploited by law enforcement, as well as by terrorists, hackers, criminals, and foreign intelligence officials. Creating a backdoor makes everyone more vulnerable.

In addition, the tech companies are leery about cooperating with the government because of Edward Snowden’s revelations about the role of the tech industry in the U.S. government’s mass surveillance programs. The tech industry lost business from foreign customers concerned about buying systems accessible to the U.S. government and its surveillance operation. Even if the tech companies agreed to mandated backdoor access, foreign companies and governments would look for alternative products and services that didn’t include backdoor access. Lastly, Snowden’s leaks drove the terrorists to go dark. They frequently use encrypted applications to hide their communications from law enforcement.

So what are the current proposals on encryption and access in the U.S. Congress? There are several current proposals, mostly bipartisan. None really address the concern about ensuring security. Some U.S. lawmakers want to mandate backdoors for law enforcement generally or at least when compelled by court order. Others recognize that there is no current solution, so they are pushing legislation to bring together the tech industry, privacy advocates, academics, law enforcement, and the intelligence community to study and come up with a solution that provides law enforcement access without weakening security. There are also proposals pending in California and New York to mandate backdoor access to data. Those against these proposals say any effort to weaken encryption only makes data more vulnerable to criminals.

Meanwhile, foreign governments and organizations are also considering the balance between ensuring security and having access. Recently, the UK government's encryption protocol for voice communications has been found to have a backdoor that enables security services to intercept and listen to all past and present calls. Another piece of UK legislation would give the government powers to compel companies that operate in the UK to decrypt data with a warrant. In January, the French Parliament considered legislation that would have required tech companies to configure their systems so that police and intelligence agencies could always access encrypted data. While the legislation was rejected, just the fact that such a measure was even considered in France suggests that some there are willing to consider prioritizing the security of citizens against terrorism over individual privacy concerns. There was even a panel discussion on this topic at the recent World Economic Forum, which discussed the various viewpoints but did not achieve any general consensus on solutions.

— Kathleen E. Porter

Super Bowl Sunday: No Drone Zone

The Federal Aviation Administration (FAA) released a YouTube video on Wednesday letting drone operators know that the air above Levi’s Stadium in San Francisco is off limits on Super Bowl Sunday. Labeled a “No Drone Zone,” the FAA has instituted temporary flight restrictions within a 32-mile radius of the stadium from 2:00 to 11:59 p.m. on Sunday. In the 20-second video released by the FAA, the agency tells football fans to bring their jerseys, face paint, and team spirit but to leave their drones at home. The FAA said, “We’re working closely with our safety and security partners to spread this message as widely as possible.”

— Kathryn M. Rattigan

PRIVACY TIP #20

FTC Releases New Online Tools for Identity Theft Victims—Take Advantage of Them!

As one who is frequently asked, “What happens when I become the victim of identity theft?” or “How do I prevent myself from becoming the victim of identity theft?,” I am a pretty big fan of the FTC’s website and refer people to it often. FTC statistics indicate that it received more than 490,000 complaints from consumers about identity theft in 2015 alone, which was a 47 percent increase from 2014. This issue is just not going away any time soon.

When companies experience data breaches and provide notification letters to affected individuals, the FTC website is often included in the notification letter to provide individuals with additional information on how to protect themselves following a data breach of personal information.

The website has always been pretty good, but now it’s even better.

On January 28, 2016, which just happened to be International Privacy Day, the FTC released additional “significant enhancements” to its IdentityTheft.gov website.

The site now allows individuals to file an identity theft complaint with the FTC. After filing the complaint, a “personalized guide to recovery” for users is generated that will respond to the details of the complaint. It is intended to be unique to each complaint.

Each guide to recovery provides consumers with the tools necessary to inform law enforcement, credit bureaus, the IRS, financial institutions, and governmental agencies of the fact that they have been the victim of identity theft, including form affidavits and letters to send. It makes the process more streamlined and easy for consumers to take action after they have been victimized.

If you have ever been the victim of identity theft, you understand how complicated and difficult it can be to restore your identity. Any help from the federal government to assist consumers in this process and to make it easier for us is great.

So if you have been the victim of identity theft, and don’t know what to do—check out www.IdentityTheft.gov now. It is one-stop shopping for victims to obtain a personalized identity theft guide to recovery. Take advantage of it! It is available through mobile devices and in Spanish. Kudos to the FTC for launching this site to help consumers.

— Linn Foster Freedman
