Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

November 19, 2015

ENFORCEMENT + LITIGATION

LabMD Vindicated in FTC Row

We have been following the fight between LabMD and the FTC for years. It has been a story of high emotions, principles, standoffs, aggression, lawsuits, court decisions, Congressional hearings and accusations, all outlined in a book entitled "The Devil in the Beltway" (admittedly a one-sided account by LabMD CEO Mike Daugherty about the details of the case).

In an over 90-page decision issued last Friday, the administrative law judge (ALJ) presiding over the FTC's case against LabMD (which alleged that LabMD had insufficient security to protect patient lab results, which were allegedly accessible by others through a file sharing network) stopped the FTC in its tracks by decidedly finding in favor of LabMD.

The ALJ found that there was no evidence that any third party had access to any patient information and no evidence that any consumer had been harmed. He further identified that Section 5 of the FTC Act requires that there be evidence that consumers have suffered substantial harm. In this case, the FTC was unable to show that the information had actually been accessed by anyone and certainly was unable to show that any consumer had been harmed. The ALJ dismissed the case against LabMD.

Mike Daugherty enthusiastically forwarded the decision to his network, including this writer, noting that it was bittersweet for him. Understandable, because LabMD was forced to dissolve during the investigation, which Daugherty directly attributes to the time and resources dedicated to fighting the crushing weight of the FTC investigation.

Daugherty commented to me following the decision, "It's bittersweet but a big victory for the legacy of LabMD as the administrative law judge smacked the FTC down but good, dismissing the FTC's bully case for the smoke and mirrors revenge mission that it was. Relying on unreliable witnesses, not verifying evidence, and punishing LabMD into insolvency, this win won't bring back LabMD or wash the blood of the government's hands, but hopefully will raise awareness of the true tactics of the FTC and all who enable their behavior. The battle continues."

The FTC has not publicly stated what its intentions are with regard to an appeal, but it will be interesting to see whether it decides to pursue this case.

Although the FTC was recently successful in the Wyndham case (see related post), the facts in that case were quite different than the LabMD case. Although this provides companies with some hope that they can be successful in pushing back against the FTC, the road for LabMD was long and bloody. Going forward, the facts of each case will no doubt be the deciding factor for the FTC to pursue cases, and for companies to push back. Either way, this is a bump in the road for the FTC's recent aggressive

enforcement over data security practices of companies that may (or may not) suffer a data breach.

— Linn Foster Freedman

PSQIA Held to Preempt Florida Constitutional Right to Access Adverse Medical Incident Reports

On October 28, 2015, the District Court of Appeal in the First District of Florida held in *Southern Baptist Hospital, Inc. v. Jean Charles, Jr. et al.* that the federal Patient Safety and Quality Improvement Act of 2005 (PSQIA) preempts a provision of the Florida Constitution that provides patients with a broad right of access to records of adverse medical incidents.

In this case, the plaintiff sought documents pertaining to adverse medical incidents at Southern Baptist Hospital pursuant to Article 10, §25 of the Florida Constitution (commonly referred to as Amendment 7). Amendment 7 establishes a constitutional right of access for patients with respect to any records made or received in the course of business by a health care facility or provider in relation to an adverse medical incident (which term includes medical negligence, intentional misconduct, or any other act, neglect, or default of a health care facility or provider that caused or could have caused injury to or death of a patient). Amendment 7 is commonly used to compel discovery in medical malpractice actions filed under Florida law.

Southern Baptist Hospital refused to produce certain requested documents that were potentially responsive — primarily occurrence reports compiled by the hospital that were not specific to the circumstances of the plaintiff's case — on the basis that such documents were privileged and confidential patient safety work product (PSWP) under the PSQIA. The PSQIA established a voluntary reporting system that incentivizes the creation of patient safety evaluation systems (PSEs) by hospitals and other health care providers by providing broad confidentiality and privilege protections for PSWP collected or maintained within a PSE for reporting to a recognized patient safety organization (PSO). The PSQIA defines PSWP to include, in pertinent part, any documents or reports that could improve patient safety, health care quality, or health care outcomes and are collected by a provider within a PSE for reporting to a PSO.

After the trial court rejected Southern Baptist Hospital's arguments against producing the occurrence reports, the hospital sought *certiorari* from the District Court of Appeal to review the discovery orders. The District Court of Appeal found that Southern Baptist Hospital's occurrence reports met the definition of PSWP because they were placed into the hospital's PSE for reporting to a PSO, and they did not exist outside of the hospital's PSE. The District Court of Appeal thus quashed the trial court's discovery orders and further held that Amendment 7 is both expressly and impliedly preempted by the PSQIA under the Supremacy Clause. In reaching its conclusion, the District Court of Appeal noted that allowing broad discovery under Amendment 7 of documents constituting PSWP would be "contrary to Congress's intent to cultivate a culture of safety to improve and better the healthcare community as a whole."

The District Court of Appeal's decision in this case is likely to spurn further litigation over the permissible scope of discovery in medical malpractice cases under Florida law and the PSQIA.

— Conor Duffy

Lab Tech Indicted for Identity Theft

A lab tech working at a Las Vegas pediatric cardiology practice has been indicted on one count of illegal use and disclosure of patient health information and one count of aggravated identity theft. The lab tech had previously been convicted of Medicaid fraud for submitting false Medicaid claims and was sentenced

to serve 12 to 48 months in prison and pay approximately $10,000 in restitution, penalties and costs.

According to prosecutors, the lab tech in this case accessed a patient's information without authorization and then used it to apply for credit cards without the patient's knowledge. The lab tech has pleaded not guilty to the charges.

This case underscores the importance of performing background checks of employees who will have access to high risk and sensitive data in your organization.

— Linn Foster Freedman

DATA BREACH

Over 70 Million Prison Phone Records Leaked

Securus Technologies (Securus), which provides phone services for many of the country's prisons, experienced a breach of over 70 million phone records from over 37 states. The data leaked includes downloadable recordings of inmate calls from December 2011 through Spring 2014. The data was provided to *The Intercept*, an online media outlet, in a 37-gigabyte file, which contained the recordings as well as spreadsheets of prisoners' first and last names; phone numbers they called, the date, time, and duration of the call, and the inmates' Securus account numbers. While many argue that much of this information is not private, in the context of incarceration, because the right of privacy is diminished once incarcerated, individuals on the other end of the phone call may be losing some of their civil liberties in this mass recording conducted by Securus. However, the individual receiving the phone call does hear the following: "This call is from a correctional facility and may be monitored and recorded."

However, the bigger problem with some of the other calls is that they are between inmates and their attorneys, meaning that these calls are confidential and privileged, and probably shouldn't have been recorded in the first place. This is a potential constitutional violation, including a violation of the right to effective assistance of counsel and access to the courts.

David Fathi, Director of the ACLU, said, "This may be the most massive breach of attorney-client privilege in modern history." Inmates should be able to speak freely and honestly with their attorneys, and while Securus promised in its contracts with state prisons that each "call will be recorded and monitored, with the exception of privileged calls," they clearly didn't keep that promise and didn't secure the data to keep it out of the wrong hands.

After the announcement of the breach by *The Intercept*, Securus made a statement to explain that they "have seen no evidence that records were shared as a result of a technology breach or hack into our systems. Instead, at this preliminary stage, evidence suggests that an individual or individuals with authorized access to a limited set of records may have used that access to inappropriately share those records," and that "it is important to note that we have found absolutely no evidence of attorney-client calls that were recorded without the knowledge and consent of those parties." We will keep you updated once any further details are released.

— Kathryn M. Rattigan

CYBERSECURITY

Beware of Version 4.0 of Cryptowall Ransomware

Security experts are warning that a new version of the notorious and nasty ransomware Cryptowall, dubbed Cryptowall 4.0, has hit the scene. The difference with the new version is that it is able to encrypt specific file names, on top of data.

What this means is that it can infiltrate your network, encrypt specific files and make them unintelligible to the user. So if you have a file entitled "travel," it will be encrypted and masked so you can't locate it. Very frustrating.

The message from the Cryptowall developers is that they are making "the Internet a better and safer place," but they are running all the way to the Bitcoin bank.

Cryptowall 4.0 is still sent to users primarily through a zipfile with an attachment that looks like a resume. So warn all of your employees to beware of zipfiles and contact IT if they are suspicious. Security experts are recommending to continually back up data to be able to retrieve data in the event of an intrusion.

— Linn Foster Freedman

DATA SECURITY

NIST Issues Draft IT Asset Management Special Publication

The National Cybersecurity Center of Excellence (NCCoE) has issued its draft practice guide entitled "IT Asset Management," designed for the financial sector.

The comment period for the guide is open through January 8, 2016, and comments can be submitted online or via email.

The guide, developed by NCCoE engineers, "allows an organization to centrally monitor and gain deeper insight into their entire IT asset portfolio with an automated platform." The example solution "gives companies the ability to track, manage, and report on information assets throughout their entire life cycle. This can ultimately increase Cybersecurity resilience by enhancing the visibility of assets, identifying vulnerable assets, enabling faster response to security alerts, revealing which applications are actually being used, and reducing help desk response times."

We are all fortunate to have these bright NCCoE engineers working for us. If you are a CIO or CISO in the financial services industry or a contractor to the financial services industry, consider taking a look at the guide and offering your comments.

— Linn Foster Freedman

Increased Risk of 'Medjacking' Calls for Better Security Measures on Medical Devices

Did you know that right now we have about 5 billion connected smart devices in use? Is it surprising that it is predicted that by 2020 that number will skyrocket to 25 billion? Of all these connected devices, a significant portion of these devices will be medical devices such as pacemakers, in-home monitoring systems and drug pumps. The risks associated with these connected medical devices are plentiful. The biggest concern is medjacking. Medjacking is short for medical device hijacking.

Medjacking is becoming more and more prevalent as more medical devices get connected. In June 2015, TrapX Security released a report that detailed incidents of medjakcing in three hospitals:

1. Passwords were stolen to the hospital's network and confidential data transmitted to computers in Eastern Europe via a blood gas analyzer infected with two different types of malware.
2. Unauthorized entry into the hospital's network to send sensitive data to China via the radiology department's image storage system.
3. Unauthorized access to the hospital's network to access confidential data through a back door that hackers installed in a drug pump.

More of these types of incidents are likely to occur as more and more medical devices are connected to sensitive, confidential networks.

Why is this happening? What can we do? Currently, the U.S. Food and Drug Administration (FDA) has only released security "recommendations" for medical devices. But with this real-time operating system, the security flaws are being discovered by hackers and exploited faster than the security failure can be patched. The FDA will hopefully require medical device manufacturers to implement security features that meet a set standard; solve the problem of lagging security fixes and security patches; segment sensitive, confidential data from the networks that these medical devices are connected to; and train patients and health care staff on how to use medical devices in the most secure way they can. For now, be aware of these vulnerabilities and be sure your patients' medical devices are not being exposed to medjackers.

— Kathryn M. Rattigan

Massachusetts Develops a Remote-Controlled Contraceptive Chip

Ladies and gentlemen, introducing the remote-controlled contraceptive computer chip. Releasing measured doses of the levonorgestrel hormone, these computer chips can be implanted under a woman's skin as a new form of birth control, presumably starting in 2018. While there are certainly other types of contraceptives that can be implanted under a woman's skin, the only way to "deactivate" those contraceptives is to have an outpatient procedure. This new computer chip, developed by the Massachusetts Institute of Technology (MIT), is set to release the hormone for up to 16 years –*but,* it can be stopped anytime using a wireless remote control and then reactivated when desired.

However, the big question is the security of the chip. The team at MIT is working to ensure that the chips cannot be hacked, which could lead to activation or deactivation of the chip without the woman's knowledge. To address this concern, as of now, the chip can only be reprogrammed at "skin contact level distance." The team will also ensure that the communications between the chip and the remote are transmitted via secure encryption.

The team hopes that this type of technology can be used to administer many other kinds of drugs as well. The computer chip will be submitted for preclinical testing starting next year.

— Kathryn M. Rattigan

DATA PRIVACY

EU Data Transfer Update

On November 6, 2015, the EU Commission released its guidance for businesses relating to the EU safe

harbor.

The commission indicated that since the invalidation of the safe harbor framework, it has "stepped up" talks with the U.S. regarding transfer of data from the EU to the U.S. but acknowledged that global companies were seeking guidance on how to proceed.

The guidance follows the statement made by the Article 29 Working Party (see related post) and acknowledges the goal of having a new framework in place by January 31, 2016, but indicating that the DPAs have authority to enforce improper data transfers.

Meanwhile, the Polish DPA issued a statement last week that referred to the Statement of the Article 29 Working Party indicating that, in the event that no appropriate solution is found with the U.S. authorities by the end of January 2016, and depending upon an assessment of the transfer tools by the Article 29 Working Party, the EU data protection authorities will take all necessary and appropriate actions, which may include coordinated enforcement actions.

— Linn Foster Freedman

WEEKLY PRIVACY TIP #10

What Are Digital Assets and Why Should I Care?

Your digital life and assets can include online music, photos, social media accounts, gaming winnings, and the like. But most of us don't look at these items as assets that we should think about and plan for when we pass away.

But when you pass away, your heirs and/or executor has to deal with digital assets just like any other assets. They can't just get into your Apple account to retrieve your music or credit or take down your Facebook account. They don't have the user name and password, so they can't access it, and companies, including social media companies, will not allow you to access the deceased's account without going through a lengthy process (rightfully so).

Because this has become such an issue, the Uniform Law Commission has implemented a model law to allow fiduciaries to have access to digital assets. Delaware became the first state to adopt the law.

Additionally, 19 states have passed their own laws to protect people's digital assets and give the heirs/executor the right to access and manage online accounts after death, but again, there are processes that must be followed by the family members before they can get access to the accounts. If you have ever been an executor of an estate, you will want to make the job easier for your executor.

How can you help your heirs? Just as you should plan for your death and consider having a will, a health care power of attorney, and a durable power of attorney, you should also plan for the transfer of digital assets to your heirs and work with your estate planning attorney to include these assets in your estate plan. It is important to include the information necessary for your heirs to access these accounts after your death, which would include user names and passwords for each account. It is not recommended that the user names and passwords be attached to any legal documents that may be filed in court, as they could potentially become public. But work with your attorney to gather the information necessary and be able to provide it to your heirs and family members to make the process easier for them. You will be gone, but it will make a big difference for them.

— Linn Foster 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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com