Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

January 7, 2016

News, Trends + Predictions for 2016

ENFORCEMENT + LITIGATION

FTC Settles with Software Provider over Misleading Customers about Encryption of Patient Data

On January 5, 2016, the Federal Trade Commission (FTC) announced that it has agreed to a $250,000 settlement with Henry Schein Practice Solutions, Inc. (Schein), an office management software provider for dental practices based in Utah, in connection with its investigation into allegations that Schein falsely advertised the level of encryption it provided for patient data.

The FTC alleged that Schein marketed its Dentrix G5 software by touting that it provided industry-standard encryption and that by using the software the practice would comply with HIPAA. It further alleged that Schein was aware that the encryption standards that it used did not meet the NIST recommended standard (Advanced Encryption Standard), which meets HIPAA regulatory requirements, which violated Section 5 of the FTC Act. The advertisement of HIPAA compliance was included in marketing materials and brochures.

In addition to the payment of $250,000 to the FTC, Schein must stop misleading customers about its encryption as being "industry-standard," and in the next 60 days must notify all of its customers who purchased and use Dentrix G5 that the product does not provide industry-standard encryption. According to the FTC, this was the first settlement involving marketing claims specifically related to data security. The settlement is open for comment until February 4, 2016.

This settlement is interesting because it shows that the FTC is continuing to expand its enforcement over data security, but in this case, it concentrated on the false advertising of the company with respect to data security. We predict that the FTC will continue to expand its enforcement over data security, and this is a stark reminder to software companies (and others) to be careful when advertising their products' capabilities.

— Linn Foster Freedman

Mortgage Company Pays $7.4 Million to Settle TCPA Violations

Mortgage Investors Corp. (MIC) settled a class action this week for $7.4 million for its alleged violations of the Telephone Consumer Protection Act (TCPA) in an Oregon federal court. Plaintiffs stated in their complaint that MIC made millions of unsolicited telephone calls to veterans marketing refinancing options for their home loans. Plaintiffs also alleged that they received multiple, harassing telephone calls even though their telephone numbers were on the national Do-Not-Call Registry, and they did not provide prior consent to receive these telemarketing calls.

U.S. Magistrate Judge Janice M. Stewart said, "For the reasons stated by plaintiffs in their motion… including lack of any objection by any class member, this court concludes that all factors strongly favor final approval of the settlement agreement." Part of the settlement will cover $1.8 million in attorneys' fees and $5,000 incentive fees to the two class representatives.

— Kathryn M. Rattigan

FAST Act Loosens Financial Institutions' Privacy Policy Notice Requirements

In addition to providing long-term funding for highway infrastructure improvements and other transportation projects, the newly enacted Fixing America's Surface Transportation Act (FAST Act) seeks to reduce consumer confusion by eliminating annual privacy notice requirements for financial institutions in some circumstances.

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to provide consumers with notice of the institution's privacy policies and procedures annually. Section 75001 of the FAST Act, signed into law by President Obama on December 4, 2015, eliminates this annual notice requirement for financial institutions that satisfy two criteria:

- The financial institution does not share nonpublic personal information with nonaffiliated third parties except pursuant to certain GLBA exceptions permitting such disclosures; and
- The financial institution has also not changed its privacy policy and procedures since the most recent GLBA privacy notice sent to consumers.

Financial executives planning to send out annual privacy notices at the beginning of 2016 may no longer need to do so and may wish to review privacy practices and procedures to determine if the FAST Act exception is applicable to their institution.

Section 75001 should be considered in conjunction with a Consumer Financial Protection Bureau final rule issued in October 2014, which also allows financial institutions that meet certain requirements and limit data sharing to post privacy notices online in place of mailing notices to individuals.

Section 75001 of the FAST Act is available here.

— Norman H. Roos and Scott M. Baird

U.S. Supreme Court's Decision in *Spokeo v. Robins* Case Will Make Waves in Consumer Class Actions–One Way or Another

Back in early November of last year, Spokeo, Inc. (Spokeo) argued before the U.S. Supreme Court, seeking to overturn a February 2014 ruling from the Ninth Circuit that revived the Fair Credit Reporting Act (FCRA) lawsuit filed against Spokeo by Thomas Robins. Robins alleges that Spokeo violated the FCRA by falsely reporting his financial, marital, and educational status (for the better). He was portrayed as wealthy, married, and a graduate degree recipient when in fact he was unemployed and struggling

financially. Spokeo is asking the Supreme Court to review the Ninth Circuit's decision and overturn the prior decision in favor of Spokeo.

Justices were split in November on the issue of whether consumers can sue Spokeo for FCRA technical violations without any allegations of actual injury. On one hand, Justice Elena Kagan said, "People get these reports, and you don't know what they're doing with these reports. They might not have given you a job for that reason, or they might not have given you a job for some other reason." However, Chief Justice John G. Roberts said, "We have a legion of cases that say you have to have actual injury." To this point, many class actions have not proceeded past the pleadings stage for failure to show any damage or injury. If the Supreme Court rules in favor of Spokeo, it could build a strong precedent that consumers must assert actual harm before a case can proceed; if the Supreme Court rules for the government and the standard changes, it could mean more privacy and security breach litigation. The Supreme Court is expected to issue a decision on this matter in the first half of 2016.

— Kathryn M. Rattigan

DATA BREACH

Regional Income Tax Authority in Ohio Loses Info on 50,000 People

The Regional Income Tax Agency of Ohio (RITA) announced on December 31, 2015, that it lost the personal data of approximately 50,000 individuals who filed tax forms with the agency in November. RITA provides tax collection services for over 250 municipalities in the State of Ohio.

According to RITA, a backup DVD with the personal information of the individuals was unable to be located on November 10. The DVD contained the names, addresses, Social Security numbers, and dates of birth of taxpayers. It was stored off-site at a third-party vendor's facility and, when it was recalled, it could not be found.

RITA will provide notice to the affected individuals and provide one year of credit monitoring.

— Linn Foster Freedman

IRS Provides Tax Relief for Pre-Breach Identity Protection Services

The IRS released a bulletin on December 30, 2015 (Announcement 2016-02) announcing that it would extend the tax exemption issued in August to organizations that provide credit monitoring to their employees following a data breach to receive a similar exemption for pre-breach identity protection services. This means that the value of the services, both pre-breach and post-breach, should not be included in an individual's or employer's gross income for tax purposes.

The bulletin stated "…the IRS will not assert that an employer providing identity protection services to its employees must include the value of the identity protection in the employees' gross income and wages…and will not assert that these amounts must be reported on an information return filed with respect to such individuals."

The exemption does not apply to cash, services offered as part of a benefit package, or insurance proceeds.

— Linn Foster Freedman

Look for Additional Data Breach Class Action Cases, Standing Decisions, and Shareholders' Derivative Suits in 2016

2015 was a banner year for data breaches and associated class action litigation. Toward the end of the year, class action cases were filed the same day as the notification (related post here). Based upon the data breach fallout in 2015, there is no doubt that 2016 is setting itself up to be another frenzied year of data breaches.

It used to be that class actions weren't filed or didn't make it past a motion to dismiss for lack of standing, and the case law was pretty uniform until this year. Now, plaintiffs' attorneys are using new theories of liability such as benefit of the bargain or state law statutes to defeat motions to dismiss, and several cases, including *Tabata*, are considered outliers.

Not only do we predict that data breaches will explode in 2016, but the corresponding class actions filed following the breaches will be assumed and not a surprise. We also predict that more decisions will be handed down at both the federal and state level on standing to sue in a data breach case, and when you have more cases, it is inevitable that there will be more outliers. I used to comment frequently about how the case law on standing in data breach cases is surprisingly consistent. Unfortunately, I am not sure I will be able to continue to say this in 2016.

And on top of that, companies can also assume that a shareholder's derivative suit is in the mix as well. Although the derivative suit against Wyndham Worldwide was dismissed in October of 2014, these suits have been filed against Target and Home Depot following those data breaches.

Companies can learn from the Wyndham dismissal now. In that case, Wyndham was able to show that the directors discussed cybersecurity during board meetings and did not disregard the risk because the minutes of the meetings reflected the discussion of the risk. Cybersecurity is a risk that boards would do well to pay attention to and document that the board is questioning whether the organization is taking appropriate measures to protect its data in order to combat shareholders' derivative suits.

— Linn Foster Freedman

CYBERSECURITY

Extension Given to DOD Contractors to Comply with Cybersecurity Requirements

The U.S. Department of Defense (DOD) issued an interim rule on December 30, 2015, that extended the deadline for DOD contractors to comply with security requirements for protecting nonclassified, but sensitive, government information until December 31, 2017. The rule followed a public meeting where contractors expressed concern and need for additional time to implement the requirements.

With the extension comes a requirement that contractors notify the DOD CIO of any unimplemented cybersecurity requirements within 30 days of being awarded a DOD contract. This means that the DOD can assess whether the contract will be awarded to a company based upon its implementation of the requirements, depending on the nature of the information that will be available to the contractor.

Even though an extension has been granted, DOD contractors may want to consider expediting compliance in order to be in the best position to win DOD contracts.

— Linn Foster Freedman

Comment Period for NIST Guide "Model Device Security" Coming to a Close

The National Cybersecurity Center of Excellence (NCCoE) has announced that the comment period for the draft NIST Cybersecurity Practice Guide "*Mobile Device Security: Cloud & Hybrid Builds*" will close on January 8, 2016.

The Guide addresses the cybersecurity challenge of allowing employees to access information resources despite security controls to address the risk. This guide is an example of a mobile device security solution for businesses. According to NCCoE, the guide "demonstrates how commercially available technologies can meet an organization's needs to secure sensitive enterprise data accessed by and/or stored on employees' mobile devices." Comments can be submitted via email to mobile-nccoe@nist.gov.

If you don't follow NIST's great work, we recommend that you may want to start. The NIST folks will be busy in 2016 helping private companies and the government implement industry standards to protect data. We will be following them closely.

— Linn Foster Freedman

Sanction Rules Adopted for Cyber-Attackers

The federal government issued The Cyber-Related Sanctions Regulation on December 31, 2015, which allows the freezing of assets of suspects who aid in cyber-attacks. The regulation follows an Executive Order from April 2015, which allows officials to determine that money transfers by individuals suspected of playing a role in a cyber-attack targeting national security, foreign policy, or the economic health or financial stability of the United States to be "null and void."

The Office of Foreign Assets Control can also deny licenses to those covered by the Executive Order and keeps a list on its website of individuals who have been determined to have played a role in cyber-attacks and who are subject to the sanctions.

— Linn Foster Freedman

INTERNET OF THINGS

Self-Driving Cars, Mood-Controlled Lighting and Fitbits: More FTC IoT Enforcement

Almost one year ago, the FTC released its "*Internet of Things (IoT): Privacy and Security in a Connected World*" report urging companies to implement best practices for consumers' privacy and data security and, shortly thereafter, introduced the new Office of Technology Research and Investigation unit to protect consumers from IoT failures. Since the FTC's release of its report, and the start of its new IoT unit, we have yet to see any enforcement actions against companies for their IoT failures. While the FTC's case against TRENDnet in 2013 is known as the first (and only) IoT action to date, in 2016, we will likely see an increase in the FTC's IoT enforcement actions, as well as an increase in privacy litigation (in particular, a rise in class action plaintiffs) against IoT companies and manufacturers for failure to properly

utilize the FTC's IoT privacy and security recommendations when these individuals attempt to claim losses and sue for damages related to IoT data breaches. A new year's resolution for IoT companies and manufacturers? Maintain reasonable security measures, update your privacy policies, and freshen up on the requirements of the Fair Credit Reporting Act (FCRA) when using IoT data for credit, employment, insurance, or other types of eligibility.

— Kathryn M. Rattigan

Ford Motor and Henry Ford Health System Co-Sponsoring Technology Challenge for Connecting Wearable Devices with Automobiles

The Connected Health App Challenge (Challenge), co-sponsored by Ford Motor Company and Henry Ford Health System, launches on January 20, 2016, and is open to employees of both entities. What is it? It's a challenge that seeks to find technology that will expand patient monitoring and management to their cars.

The concept is that people are in their cars for a significant amount of time every day and that time could be spent monitoring and managing drivers' health conditions. The questions posed in the Challenge include how being connected to your car can manage your health condition, how knowing your vital signs can improve your driving, and whether being connected to your car can save lives. Our cars will now have our vital signs? That's fodder for another post later, but connectivity through technology is not going away in 2016!

— Linn Foster Freedman

Toyota Announces 'Data Communication Modules' for Its 2017 Models

Connected cars are on the verge. And they are already on our roads. This week, Toyota announced that it will add more connected cars to our roads with some of its 2017 vehicle models, which will have Data Communication Modules (DCMs) installed to allow for uploading and downloading of information from the vehicles to Toyota's big data base. No pun intended. This will be a BIG database. All of the vehicles will be connected to the Toyota Big Data Center, and the system will "analyze and process data collected by DCMs, and use it to deploy services under high level information security and privacy controls." What is high-level exactly? Without any specific regulation of connected cars at this point, data collection from cars will likely become an even more pressing issue in the coming years. Toyota has not yet revealed which models will have this DCM option (or how the cost of their vehicles will change due to the installation of these DCMs), but they have confirmed that the deployment of these vehicles will start with 2017 models. The DCM will allow for standard emergency notification in a crash (which is already offered by other car manufacturers via Wi-Fi and Bluetooth connections), but Toyota will be bringing the cellular connection to the car to make the transmission of data even easier.

— Kathryn M. Rattigan

HIPAA

HHS Issues Proposal to Allow Covered Entities to Report Background Check Information to NICS

In a press release issued on January 3, 2016, the Department of Health and Human Services announced that "as part of President Obama's continuing efforts to reduce gun violence…HHS…issued a Notice of Proposed Rulemaking (NPRM) to remove unnecessary legal barriers under…HIPAA…that may prevent states from reporting certain information to the National Instant Criminal Background Check System (NICS)."

The press release indicates that states are under-reporting information to NCIS, which "helps to ensure that guns are not sold to those prohibited by law from having them," and cites a 2012 GAO report that found that only 17 states had submitted fewer than 10 records of individuals prohibited from owning a gun, including felons, those convicted of domestic violence, and individuals involuntarily committed to a mental institution.

The NPRM intends to modify the HIPAA Privacy Rule to allow HIPAA-covered entities to disclose the identities of persons prohibited from possessing or receiving a firearm because of reasons related to mental health to NICS. Basically, it will allow providers to disclose that someone has been involuntarily admitted to a mental institution or is a danger to themselves or others.

The proposed rulemaking would not allow the disclosure of mental health visits or routine mental health care, including clinical or diagnostic information to NCIS. However, it would allow providers to disclose "the minimum necessary identifying information about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs."

Comments to the NPRM can be submitted here.

— Linn Foster Freedman

Healthcare Cloud Services Vendors Accredited for HIPAA Compliance

The FedRamp federal government program governing cloud security has accredited three healthcare cloud computing vendors for meeting best business practices and complying with the privacy and security requirements of HIPAA.

The accreditation comes from the Electronic Healthcare Network Accreditation Commission (EHNAC), which has 19 accreditation programs. EHNAC provided the accreditation to FIGmd, HealthcarePays Network, and MedicaSoft.

We expect that more healthcare providers will utilize cloud service vendors in 2016, and knowing that there are accreditation programs like EHNAC is comforting.

— Linn Foster Freedman

Increased OCR Investigations and Fines Predicted in 2016

The Office for Civil Rights (OCR) had another strong year of investigations and enforcement actions against covered entities. It also has made it abundantly clear that it will not back down from aggressive enforcement in 2016. What's different this year is that we will see more investigations and enforcement actions against business associates.

The OCR has publicly announced that its audit program for business associates will start in 2016. I would believe the OCR. Business associates may wish to review their HIPAA compliance programs and shore up that program now before they get that knock at the door.

— Linn Foster Freedman

INFORMATION GOVERNANCE

Corporate Board Governance of Data Privacy and Security

If 2015 was the year that corporate boards started to stay up at night thinking about cybersecurity like their IT guys, 2016 will be the year that they will take action to work with their C-Suite and CIO and/or CISO to get a handle on data security in the organization and take control of risk management.

We are seeing corporate boards put data security on their agendas for risk management more frequently, and that trend will continue throughout 2016.

Corporate boards should already be engaged in managing data security risks for their organizations in 2016 and need to become more educated so the gap between data security and the board room can be bridged. If you are a corporate board member and you don't understand what malware or phishing is, get engaged, ask questions, and become educated. If the organization doesn't have an information governance or data privacy and security program, find out why and get it in the budget. Learn about cybersecurity and take action to protect your organization in the coming year of anticipated increased data breaches.

— Linn Foster Freedman

Information Governance Outlook in 2016

The purpose of an information governance program is to provide insight into information that is the most valuable to the organization, while minimizing associated risks and costs. Until recently, organizations focused less on the latter and heavily on gaining insight into the most valuable information. The reason for this change is largely due to the increasing number of data breaches happening in various industries all across the globe. It is a risk that simply can't be ignored.
We expect this year to be the year of stakeholder collaboration. Gone are the days of the information technology, business units, and legal teams working in silos. All should be working together for the organization's information governance to be a success.

Some projects we expect organizations to focus on in 2016 include:

- Undergo inventory of unstructured and structured data repositories and document access control permissions
- Reduce digital footprint by defensibly disposing of information that is no longer needed according to corporate policy and legal requirements
- Undergo inventory third-party vendor agreements for compliance with your organization's data privacy and security requirements
- Understand where sensitive data (SSNs, credit card, driver's license, passport, tax identification, etc.) is stored in the organization and implement measures to protect it

- Create and implement a data privacy and security awareness policy and program

This list is just the tip of the iceberg. What information governance projects is your organization focusing on in 2016?

— James Merrifield

DATA PRIVACY

Password Authentications Should Become More Obsolete

The username/password method of authentication is dying, albeit more slowly than many of us would like. In 2016, we should see a continued trend of replacing password authentication as the primary method for navigating through cyberspace.

We all know the challenges of password authentication. The number of access points that require passwords is growing, making it impossible for anyone to remember a specific password for each site. This requires us to regularly use the "Forgot My Password" link or dangerously use the same or similar password for all sites. While password management applications are available, they have not garnered wide acceptance.

What alternatives should we expect to see? Biometric authentication (e.g., Apple's Touch ID) allows users to access their devices and certain applications using just a fingerprint. While this is the most readily identifiable alternative at present, it is not the only replacement. Geolocation authentication relies upon a user's unique Internal Protocol (IP) address. Bluetooth proximity authentication permits users, for example, to automatically log in to his/her desktop computer by virtue of the close proximity of their mobile phone. Finally, one should expect pictograph authentication to become more prevalent wherein users select pictures as opposed to characters which are easier to remember.

Of course, the hope is that these alternative authentication methods will not only make site access less cumbersome but also reduce the number of unauthorized attacks. Only time will tell whether replacing password authentication will achieve the remedial objective.

— Brian J. Wheelin

DRONES

Is the FAA Registration Process Really the Best Thing for the New Year?

Under the new Federal Aviation Administration (FAA) drone registration requirements, all drone operators who use drones weighing more than 0.55 pounds and less than 55 pounds must register their drones with the FAA. Seems like a great idea for 2016, but the FAA has received extensive criticism for its inability to protect the information that registrants provide. Critics argue that the FAA does not have proper security measures in place to protect drone registrants' data. Registrants must submit their name, home address, and e-mail address (along with the $5 registration fee), and the FAA will issue a Certificate of Aircraft Registration/Proof of Ownership. Now, if that information is ONLY available to the FAA, no harm. However, once the database is searchable, it is a whole different story.

— Kathryn M. Rattigan

FAA Sued over Drone Registration Rules

In a move applauded by model airplane buffs, the validity of the Federal Aviation Administration's (FAA) new drone registry is being challenged in the U.S. Court Appeals for the D.C. Circuit.

John Taylor filed suit against the FAA on December 24, 2015, alleging that the registration is prohibited by Section 336 of the FAA Modernization and Reform Act of 2012 (Act) because the Act prohibits the FAA from promulgating any new rules or regulations applicable to model aircraft if they are flown for hobby or recreational purposes. As presently promulgated, the registration would be required of model aircraft flyers.

Mr. Taylor, an avid model aircraft flyer, sought an emergency stay of the registration requirement until the case is resolved, but it was denied by the Court. We will be watching this case closely as it proceeds.

— Linn Foster Freedman

Homeland Security Issues Best Practices for Drone Use by Government Entities

On December 18, 2015, the Department of Homeland Security (DHS) group Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group, issued a set of 15 best practices to help government agencies think about civil rights and civil liberties when using drones. DHS states in its publication that is does not intend to regulate any government entity, but instead seeks to share best practices that have been identified to help sustain privacy during drone operation.

Specifically, the best practices include:

1. Consult Your Legal Counsel, Privacy, Civil Rights, and Civil Liberties Experts to Ensure Legal Authority and Compliance;
2. Clearly State the Purpose of the Unmanned Aircraft Program;
3. Stay Focused on the Purpose of the Unmanned Aircraft Program;
4. Designate an Individual Responsible for Privacy, Civil Rights, and Civil Liberties Compliance;
5. Stay Involved from Conception Throughout Deployment and Thereafter;
6. Conduct a Privacy Impact Assessment and Document Privacy Compliance;
7. Limit Collection, Use, Dissemination, and Retention of Unmanned Aircraft System Recorded Data;
8. Respect Constitutionally Protected Activities;
9. Have a Redress Program for Individuals that Covers Unmanned Aircraft System Activities;
10. Ensure Accountability in Management of Unmanned Aircraft Program;
11. Properly Secure and Store Unmanned Aircraft System-Recorded Data;
12. Review Agency Procurement Solicitations;
13. Provide transparency and Outreach;
14. Train Personnel; and
15. Develop Procedures to Handle Unmanned Aircraft Systems Support Requests.

While these best practices are specifically for federal, state, and local agencies, private sector companies may also find these suggestions useful and helpful as a roadmap for their own privacy compliance when operating a drone.

— Kathryn M. Rattigan

CHILDREN'S PRIVACY

More Child Identity Theft, but More Protections for Children's Data

It seems that 2016 will mean MORE child identity theft. Why? Because with the increased amount of data collection from children and young adults at schools, health care facilities, retailers, and by advertising companies, hackers can gain access to centralized data systems with a plethora of high-value information from children. However, perhaps 2016 is also the year in which more states will implement statutes to protect children's information and identities. As of today, only California has a robust regulation to protect children's privacy, the Privacy Rights for California Minors in the Digital World Act, and only 21 states have laws to protect student data. This year, states may start to follow the lead of not only other states' laws, but also the federal children's privacy protections (under the Children's Privacy Protection Act or COPPA), and present measures such as parents' and guardians' ability to place security freezes on their children's Social Security numbers, and the ability to take proactive measures with more choice before collection of children's data. As the year progresses, we will follow legislature initiatives to see if perhaps more states decide to take a stronger stance on children's privacy.

— Kathryn M. Rattigan

DATA SECURITY

Increased Focus on Third-Party Risk Assessment, Audits and Oversight in 2016

For vendors or suppliers or other companies providing outsourced services or components or supplies, and for the customers of such services or suppliers, 2016 means an increased demand on your limited time and manpower to respond to or review risk information security assessments, host or perform audits, and generally oversee or be subject to oversight.

Companies often hire third parties to perform a range of on-site or remote services, from landscaping, security, plant care or cleaning, HR screening, onboarding payroll or benefits, and product development to office, treasury or IT services. In addition, many companies have component or material suppliers with whom they share proprietary information and trade secrets. Leveraging the talent and resources of an experienced niche developer, vendor, or supplier can often be the key to a company's success. And while working with or as a vendor or supplier frequently reduces a company's costs and provides it flexibility, these relationships can also create information security risks for both parties, including the risk that a data security incident involving the vendor or its employees will result in a loss or theft of the company's critical valuable information or adversely affect deadlines, deliveries, or lead times. A company experiencing these delays or losses could also be in breach of its contracts with its customers, or at odds with its shareholders or regulators.

The growing realization that "*outsourcing the project or the function does not mean outsourcing the risk*" has prompted companies (as the customer) to increasingly focus on assessing, minimizing, and managing these information security risks. The focus begins with information security assessments when initially selecting a vendor or supplier, and continues throughout the relationship through audits, site visits, and periodic review. We expect to see an even heightened focus on information security risks in 2016. For the company (as the customer), this focus is usually just an extension of a company's larger quality control or risk management group. For many niche vendors and suppliers, where people wear multiple hats, this focus can be an unexpected unbudgeted cost. Additionally, without some planning, an outsourcing organization working with multiple accounts can find itself in constant audit mode in response to these requirements.

On the flip side, while there are costs and resources required, strengthening or adopting better information security practices often comes with several benefits. Vendors and suppliers often reduce their risk of a data security incident or breach by making some changes as part of a customer's risk assessment process or as part of a third-party certification process such as ISO 27001, which is designed to help organizations keep information assets secure. Vendors and suppliers who have taken these steps can market their efforts and certifications in RFP responses and proposals, which may help them obtain even more business. Additionally, vendors and suppliers who play a particularly strategic role in a customer's services or product development, and/or who share their own proprietary information with a customer, also may want to know more about the customer's information security practices.

As there is little chance the increased focus on information security will go away anytime soon, taking the time early in 2016 to strategize about how to better respond to the increasing focus on information security risks will undoubtedly benefit vendors, suppliers, and their customers.

— Kathleen M. Porter

2016 Year of Peak Phishing Attacks?

Early studies on the causes of data breaches found many occurred after laptops, flash drives, or other mobile devices were lost or stolen. But in recent years, data breaches have largely resulted from organized online-targeted phishing, scanning, or skimming attacks against individuals and companies. The attackers sought personal and financial data to use or sell for identity and credit card theft, but also sought proprietary information or illicit or embarrassing personal data to steal, to use for blackmail, or to publicly shame the individuals involved. Whether the attackers seek social security or credit card information, salaries and internal emails of Hollywood executives, or individuals seeking sexual partners, or intellectual property or negotiating strategies, in 2016, many predict we will see more of these targeted online attacks against companies and their employees.

In particular, we expect to see more "spear-phishing" attacks on employee email accounts rather than home accounts. Spear-phishing is when the attacker sends targeted emails to recipients, inviting them to click on a domain name link to verify their login credentials, to check their account, or obtain an important new document. Once clicked, the malware is deployed, allowing hackers to collect login names and passwords. If sent to an employee's email, a hacker can often remotely access the employer's IT system with these credentials, where they rummage around, gather, and export sensitive customer and employee data for weeks or months before being detected. Even then, detection is often accidental, such as when an employee notices an unknown query being run with her credentials. Using a practice known as "typosquatting" or "spoofing," the domain names used in the links, while bogus, are frequently confusingly similar to legitimate domain names known to the employees. For example, they may be service providers used by the company for HR, benefits, office services, or IT support. In other cases, they may be similar to the prior name of the company or to the company's virtual private network (VPN) or other remote server access. In what also seems to be a trend predicted to increase in 2016, once hackers are successful at a target, they repeat the same style of attack on companies and employees within the same particular industry until they are detected.

These types of breaches are very damaging to a company because the hacker is usually in a company's IT system undetected for an extended period of time and can export massive amounts of records, which increases their value on the dark web. Second, there are reportedly at least two cases since 2000 where these types of attacks have caused physical damage, first when an Iranian centrifuge was reportedly damaged and more recently, when a German steel mill furnace failed to shut down. Additionally, these attacks are damaging because the attackers are often foreign, in some cases state-sponsored and frequently not accountable. In 2016, expect to see the U.S. government take more public and potentially forceful positions regarding state sponsored attacks. Also expect to see the U.S. charge more foreign individuals for attacks on U.S. based companies.

Perhaps with increased awareness of phishing attacks and avoidance training for employees, coupled with anti-phishing software and stronger enforcement efforts, online phishing attacks will begin to peak in 2016.

— Kathleen M. Porter

E-DISCOVERY

Predictions (and Hopes) for E-Discovery in 2016

While 2015 will likely be remembered as the year the Federal Rules of Civil Procedure were substantively overhauled to resolve many persistent issues related to e-discovery, 2016 quietly marks ten years since the Federal Rules were amended to expressly recognize, for the first time, that electronically stored information (ESI) was equally as discoverable as its paper counterpart. In 2006, it is unlikely that anyone could have predicted the exponential growth of e-discovery as a litigation niche or the game-changing impact it would have on civil litigation. What will 2016 bring to e-discovery? Here's some predictions…and a few hopes:

- As record retention policies continue to lag behind the generation of data, garden variety commercial cases, not just the bet-the-company matters, will involve data sets that are measured in terabytes.
- With burgeoning collections, use of Technology Assisted Review (TAR) will become the default for first round document review, leaving contract attorneys out in the cold.
- Following the amendments to the Federal Rules and the publicity surrounding the opinion of the State Bar of California Standing Committee on Professional Responsibility, attorneys everywhere—from solos to big firms to in-house counsel—will (hopefully!) begin to treat their duty of technological competence with the seriousness it warrants.
- The parties' planning conference required by Federal Rule 26 will (hopefully!) no longer be treated as a meaningless task to be checked off a list, but utilized to its fullest by attorneys who recognize that it provides a valuable opportunity to negotiate a road map for the entire discovery process.
- Companies and their attorneys alike will (hopefully!) recognize that e-discovery compliance starts with sound information governance, including a thoughtful record retention policy that provides for regularly scheduled destruction of extraneous data as well as protocols to suspend those provisions in the event a litigation hold is issued.
- Savvy companies moving to the Cloud will demand that Cloud providers integrate e-discovery functionality into their platforms or, at least, provide contractual mechanisms for compliance with discovery requests or subpoenas.
- The Internet of Things will continue to expand and will become the next battleground for data collection disputes.
- The impact of the European Union's stringent data privacy rules will be felt more widely as the marketplace continues to globalize and U.S. entities doing business abroad struggle to deal with the complexities of cross border e-discovery.

Although nothing is certain, it seems a safe bet that 2016 will be an interesting year in e-discovery as litigants, counsel, and the courts all grapple with the impact of the new rules and the continual march of technology.

— Andrea Donovan Napp

SOCIAL MEDIA

Reading the Fine Print… What Happens to Your Social Media Presence after Death?

When an individual signs up for a new online account, the process typically requires an agreement to the provider's terms of service. While service providers often have policies controlling what will happen on the death of an account holder, individuals rarely read the terms of service. Nevertheless, the user is technically informed of these policies before gaining access to any service and has likely clicked on a box next to an "I agree" statement signifying consent to the provider's terms of use.

Ever wonder what is in the fine print? At the end of its terms of service, Yahoo! explicitly states that an account cannot be transferred: "You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted." Similarly, Twitter is very clear that it will not give anyone access to a deceased user's account. However, they will accept a request from an immediate family member, or estate representative, to deactivate the account. Facebook permits someone to "Report a Deceased Person," which will allow an immediate family member, upon verification, to memorialize the account of the deceased user, delete the account, or remove it altogether. Through Facebook's "legacy contact" function, a user can designate a contact with authority to respond to new friend requests, update cover and profile photos, and archive Facebook posts and photos after the death of the user.

There's plenty you can do now to ensure you get to determine the fate of your online life. If you did not read the fine print when you signed up for a new online account; you may want to read it now. Don't assume your heirs and family members will have easy access to these accounts after your death. It is important to set up a plan to eliminate as much red tape as possible for when the unexpected happens.

— Scott N. Seidor

DATA PRIVACY TIP #17

Educating K-12 Students on Privacy

I am obviously a big advocate of teaching kids about privacy at a young age. Luckily, I am not alone. There is a new privacy curriculum that educators can use to help their students learn about privacy issues, their right to privacy, and safe online usage that I want to share with our educator and school clients and friends.

The Privacy Curriculum Matrix K-12 BEaPRO™ by IKeepSafe can assist educators in setting forth a curriculum that is suited to the age of the student.

The curriculum outlines the objectives of a privacy curriculum, including awareness about data collection, why privacy matters, online terms and privacy policies, protections from identity theft, online impersonation, collection of data and respecting others' rights to privacy, and finally about sharing their personal data and the data of others, including cyberbullying, online harassment, and sexting.

The curriculum is easy to understand even if you aren't a privacy pro, and provides practical guidance for incorporating the curriculum into your classroom. The curriculum can be accessed here: www.IKeepSafe.com.

If you are an educator, make your new year's resolution to give your students tools to protect themselves

for the rest of their lives.

— 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

---