Data Privacy Day: Top 10 for 2018

By Joseph J. Lazzarotti, Jason C. Gavejian and Maya Atrakchi

January 23, 2018

In honor of Data Privacy Day, we provide the "Top 10 for 2018." While the list is by no means exhaustive, it provides key issues organizations should consider in 2018.

1. Greater Focus on EU Data Protection Requirements

Many U.S. organizations mistakenly think the European Union's data protection requirements do not apply to them. However, organizations that control or process the personal data of EU residents likely are subject to the General Data Protection Regulation (GDPR), which takes effect on May 25, 2018. Therefore, U.S. companies that sell or market products over the internet to individuals in the EU, for example, should assess whether they must comply with the GDPR. The GDPR's many privacy and security compliance requirements have undergone what is considered the greatest change to EU privacy and data security law in 20 years. Key changes include a 72-hour breach-reporting requirement, the "right to be forgotten," heightened data-subject consent, and tougher fines and penalties.

While not all organizations in the U.S. will have GDPR-compliance requirements, many will and their executives and human resources, legal, and IT departments should be well-aware of their responsibilities (see our blog post, Does the GDPR Apply to Your US-based Company?). The HR department, for example, should be familiar with the provisions concerning human resources data, as well as those on employee monitoring and profiling or analytics activities (see our blog post, U.S. Employers with EU Employees Gearing Up for GDPR).

2. Biometric Data – Emerging Law and Litigation

The trend for greater immersion of biometrics and other technologies, such as GPS, into business operations continues with no shortage of related legal issues. Over the last few years, for example, the Illinois Biometric Information Privacy Act (BIPA) produced many class action lawsuits on the collection, safeguarding, or retention of biometric information. Claims against employers surged during 2017. However, a state court decision may change the landscape for biometric lawsuits in 2018. For the first time, in *Rosenbach v. Six Flags Entertainment Corp.,* an Illinois state court held that plaintiffs must claim actual harm, rather than simply a technical violation, to be considered an "aggrieved person" under the BIPA. Plaintiffs likely will continue to test legal arguments on whether an individual is an "aggrieved person" under the BIPA. Accordingly, companies that want to implement (or have implemented) technology using employee or customer biometric information (*e.g.,* for timekeeping, physical security, validating transactions, or other purposes) should be prepared.

In addition, the surge of biometric class action suits, together with the growing use of biometric data and devices, appears to have inspired states to consider BIPA-like legislation. For example, in 2017, Alaska, Connecticut, Massachusetts, New Hampshire, and Washington have initiated or passed legislation to enhance protections for biometric information.

3. Analytics in the Workplace – Privacy Vulnerabilities

The use of analytics in the workplace continues to grow. Whether to optimize marketing campaigns or measure sales, the sales, marketing, and financial fields have relied on analytics to make key business decisions. The use of analytics has moved to other business operations as well. Increasingly, organizations are using analytics for workspace optimization with in-office sensors to inform office design, supplies inventory, and lease renewals. Of course, employing analytics to improve hiring, placement, promotions, and termination decisions by analyzing interviews, quantifying individual performance, and evaluating how team dynamics and demographics affect results likely will be more widely adopted.

Organization are making more, better, and faster decisions with analytic tools. Their use raises concerns about discrimination and disparate impact, as well as questions on the handling of personal data — its source, maintaining privacy and confidentiality, and the security of data in the hands of the organization and its affiliates and vendors.

4. Enhanced Connectivity - GPS plus IoT

No longer is GPS the only option for tracking employees, company equipment, and data. Combining

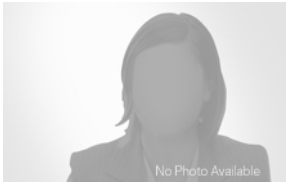
Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Jason C. Gavejian

Principal
Berkeley Heights 908-795-5139
Email



Maya Atrakchi

KM Attorney
New York Metro
New York City 212-545-4000
Email

GPS technology with "Internet of Things" (IoT) technology (*i.e.,* the growing network of internet-enabled devices that communicate with one another), including wearables and automated assistants, and video and audio surveillance, employers can significantly boost their employee monitoring capabilities. Moreover, tracking tools are readily accessible on most digital devices, particularly smartphones, contributing to their increased use. Employers can monitor employee phone calls, work email, keystrokes, internet behavior, movements, log time, location, tone of voice, interaction with colleagues, and so on. These technologies likely improve efficiency, productivity, and safety, help ensure compliance with company policies, protect employer-owned property, and provide better customer service. However, such connectivity raises privacy and security concerns.

The fundamental conflict between employers' right to monitor and employees' right to privacy has sought clarification from the courts. More courts are addressing GPS tracking in the workplace (see our blog post, Employer Denied Access to GPS Data), and several states (*e.g.,* California, Minnesota, Texas, and Tennessee) are limiting when and how GPS and related technologies can be utilized (see our blog post, GPS Tracking and Smartphone Apps – Get Consent!).

Consider a policy that includes notifying employees of any monitoring activities and other features related to the associated technology. For example, if a system also has audio and video surveillance capabilities or other functionalities (such as tracking speed, gas consumption, and driving behaviors), the organization should consider whether employees or other individuals in the vehicle should be on notice. When the tracking device should stop tracking the employee is another consideration.

5. Ransomware and Phishing Attacks Continue

Ransomware. Ransomware erupted into a billion-dollar industry in 2016. Attacks increased in 2017 by up to 250-percent, according to some estimates, and damage costs estimated to top $5 billion. Forecasters anticipate these numbers to continue to rise in the coming years. Ransomware attacks are becoming more widespread — infiltrating companies globally and across multiple sectors. At the start of 2017, ransom payouts averaged approximately $15,000. Over the last few months, demands of $250,000 to $500,000 became a weekly occurrence, according to Kivu Consulting and Navigant Consulting, a third-party specialist that facilitates cryptocurrency payments and investigates perpetrators.

Accordingly to McAfee:

> The profitability of traditional ransomware campaigns will continue to decline as vendor defenses, user education, and industry strategies improve to counter them. Attackers will adjust to target less traditional, more profitable ransomware targets, including high net-worth individuals, connected devices, and businesses.

The 2017 "WannaCry" ransomware attack brought ransomware international attention. On May 12, 2017, some hospitals in the UK's National Health Service reported being locked out of their computer systems until they complied with ransomware demands. The attack on 300,000 computers across 150 countries exploited a vulnerability in Microsoft's file-sharing mechanism. Microsoft discovered the vulnerability and issued a patch weeks before, but companies affected had not installed the patch in time. The White House concluded that North Korea was responsible for the WannaCry attack. This is even more worrisome, as, unlike other cybercriminals, nation-states have economic and political backing.

In addition, while many organizations trust and rely on cloud service providers to store their data, believing, in part, that the providers can better safeguard their data, Computer Weekly recently reported the Massachusetts Institute of Technology's prediction that cloud services may turn out to be ransomware's favorite targets in 2018. For these reasons, organizations should continue to develop and refine their plans to be prepared to effectively respond to an attack.

Phishing Attacks. HR professionals can expect constant, surreptitious attacks from hackers seeking employee tax information, particularly Forms W-2, in January and February. Watch for spearfishing emails targeting HR and payroll personnel likely to have access to this information and who are apt to respond to requests from management for that information. Of course, the emails are not from management, but are artfully disguised as such. The results of successful attacks are that fraudulent tax returns are filed in employees' names and employers must provide breach notifications to affected employees and, possibly, state agencies. *Trust but verify.* Employees should be advised to trust the source, but call to confirm the request verbally.

Phishing attacks also have spiked in the healthcare industry. Malware easily can be distributed with a link or infected attachment and delivered to healthcare employees by email. Hackers then can access a healthcare provider's database containing hundreds, if not thousands, of patient records.

6. Insider Threats

Ransomware, phishing, and other cyberattacks by external hackers often are the main focus of a

cybersecurity plan. However, malicious insiders, such as disgruntled employees, with access to areas of the employer's system external hackers cannot easily reach often result in the most costly data breaches.

Examples of situations in which internal threats can arise include:

1. An employee leaving a company and taking customer, patient, or client data that includes personal information. The information is used by the former employee or the former employee's new company to solicit business from those individuals (see our blog post, Healthcare Worker Gives New Employer Patient Records, Old Employer Pays $15,000 to NY Attorney General for HIPAA Violation);
2. Fearing of losing his or her job, an employee removes files with personal information about customers, patients, or clients in preparation for challenging the termination and related litigation; and
3. A former employee hacks the payroll system to inflate his pay, accesses proprietary files, and hijacks the company website (see our blog post, Company Awarded Damages after Former Employee Hacks Its Systems and Hijacks Its Website).

More innocent, but equally concerning, are threats such as inadvertent loss of credentials due to clicking spam links with malicious viruses attached, losing a laptop, unknowingly bringing an infected device to work, sending sensitive files to the wrong address, and the like.

According to a 2017 Insider Threat Report by ipswitch, 53 percent of companies estimate remediation costs of at least $100,000, with 12 percent of companies estimating a cost of more than $1 million. The same report suggests that 74 percent of security breaches originate from within the extended global enterprise, including a current or former employee, contractor, or business partner with access to company data.

7. Privacy and Data Breach Class Actions

In May 2016, the U.S. Supreme Court held in *Spokeo v. Robins* that plaintiffs must allege a tangible or intangible concrete injury to establish Article III standing to sue. This confused the lower courts. How are they to apply this standard in a range of data breach and statutory privacy class actions (such as under the Telephone Consumer Protection Act, Fair and Accurate Credit Transaction Act, and Video Privacy Protection Act)? Different standards have developed and, even within the same circuit, separate panels have reached conflicting conclusions. For example, paying for data security protections he did not receive was sufficient to confer standing on a customer, a panel in the U.S. Court of Appeals for the Eighth Circuit had ruled. However, a separate Eighth Circuit panel ruled the threat of future identity theft from a data breach was insufficient for standing.

The company in *Spokeo* has re-petitioned the U.S. Supreme Court to review the panel decision finding standing in its case. If the Court provides clarity on this issue in 2018, organizations can better navigate class action suits following a data breach or a statutory privacy violation.

8. Data Breach Readiness

In 2017, a surge of massive data breaches affected more than one-half of the U.S. population. Cyberthreats in the coming year are expected to affect even more people, as hackers develop new attack methods (while IT departments charged with protecting a company's sensitive information try to keep up). Many hope that advanced machine learning and artificial intelligence technologies can help organizations become better at detecting and remediating attacks. However, hackers also have access to these tools, and they will use them to strengthen their attacks to overcome organizations' defenses. The battle will continue.

Companies of all sizes and in all industries are expanding their cybersecurity programs and incident response plans. It is important for cybersecurity programs to be flexible, improving and evolving with the shifting tactics of hackers.

9. Increased Data Privacy and Security Legislation

Following massive data breaches in 2017, data privacy and security legislative proposals were introduced at the federal and state level. Senate Democrats introduced the Consumer Privacy Protection Act of 2017, geared toward protecting Americans' personal information against cyberattacks and ensuring timely notification and protection when data is breached. Subsequently, three Democratic Senators introduced the Data Security and Breach Notification Act, which would require companies to report a breach within 30 days of becoming aware of it and any person may face a penalty of up to five years in prison for concealing a breach.

New York Attorney General Eric T. Schneiderman proposed the SHIELD Act, which would heighten data security requirements for companies and better protect New York residents from data breaches of their personal information. Similar legislation have been proposed in Ohio and Vermont and are being contemplated in other states. State data breach notification laws also continue to develop.

Maryland amended its Personal Information Protection Act to expand the definition of personal information, modify the definition of security breach, and provide a 45-day timeframe for notification, among other changes. New Mexico enacted the Data Breach Notification Act, becoming the 48th state with a data breach notification law.

10. Vendor Management

Virtually all businesses interact with third-party vendors for a variety of reasons that involve all kinds of confidential company information. Increasingly, to derive efficiencies and control costs, vendors are linked directly to their customers' information systems. Cloud service providers, benefits brokers, medical billing services, debt collection companies, consultants, accountants, law firms, staffing services, shredding/data destruction services, cleaning service providers, and other businesses utilize third-party vendors to provide an array of services. In the course of providing their services, vendors, like their clients, use technologies and devices (such as mobile devices, wireless networks, and flash drives) that pose risks to information they handle. Moreover, there may be legal obligations associated with a company's use of vendors, such as requirements in third-party service provider contracts.

In certain states (including California, Illinois, Maryland, Massachusetts, Nevada, Oregon, and Texas), companies must obtain a written agreement with all third-party vendors handling personal information of state residents in order to provide services to the company. Similar requirements exist elsewhere. For instance, HIPAA imposes expansive requirements for any "business associate" or "subcontractor" that handles protected health information. The Payment Card Industry (PCI) standards have similar requirements, and law firms in many states (*e.g.,* Maine, Missouri, New Jersey, New York, Oregon, Vermont, and Wisconsin) are subject to specific state ethical mandates to have written assurances from vendors handling client data. Finally, a company that must adhere to the looming EU GDPR will have to reassess its relationship with any third-party vendor that processes personal data. Vendor management should be part of an overall strategy to safeguard company and personal information.

Bonus: Be Vigilant and Watch for Changes

Organizations constantly should be assessing their privacy and data security risks and implementing policies and procedures to protect the personal information and data they maintain. This is particularly important as the law and industry guidance change and evolve to keep up with technological advancements. Organizations need to be vigilant to remain compliant and competitive.

Please contact a Jackson Lewis attorney if you have any questions about these and other legal developments.