Privacy & Data Security:
2017 Year in Preview

real challenges. real answers.℠

POLSINELLI

Summary

Few issues keep executives awake at night more than Privacy and Data Security. New regulations and threats alike are plentiful, varied, and evolving. The rate of change for cybersecurity and information governance continues to increase, while corporate budgets to address them remain stretched.

As your organization prepares for 2017, data security, privacy compliance, and new technological threats are sure to be on your list of priorities. This guide highlights some key Privacy and Data Security trends and expectations for the new year. Organizations that are well prepared to address the issues highlighted in this guide will be better positioned to mitigate risk and strengthen compliance efforts.

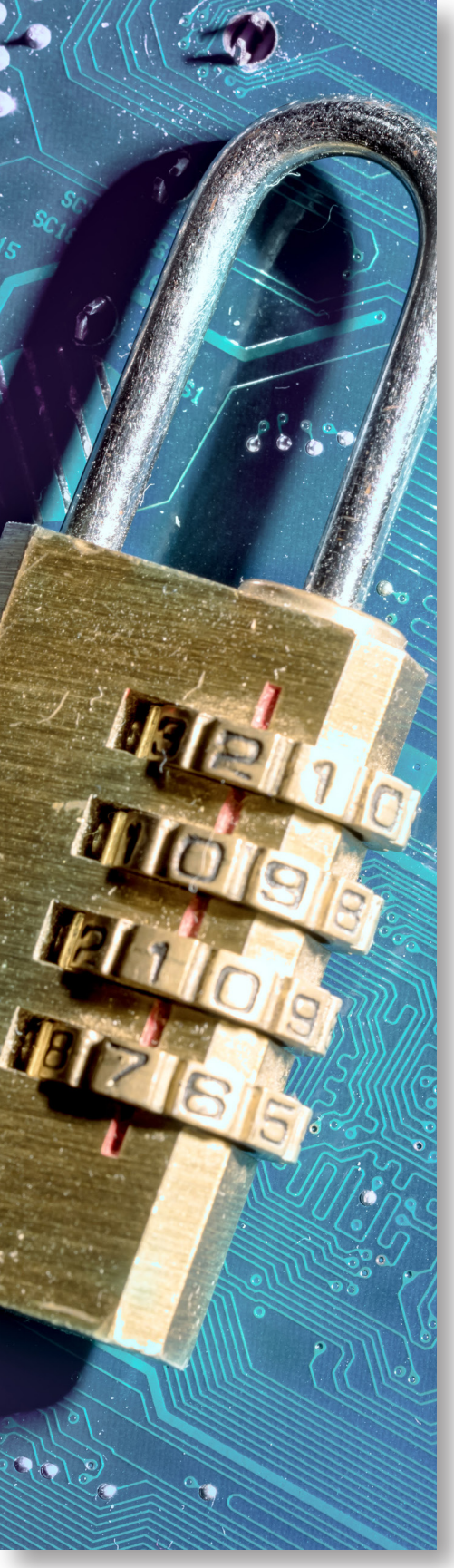


Table of Contents

GDPR:

Welcome to the New World Order

1

By: Daniel Farris, Matt Todd

The European General Data Protection Regulation (GDPR) is set to take effect in May of 2018, and if your organization has not begun preparing, it is already behind. The comprehensive 99-Article law replaces the 20 year old Data Protection Directive (95/46/EC), and establishes or expands individual privacy rights and corporate compliance obligations, and includes penalties for violations up to 4% of global revenue. GDPR's extra-territorial scope means even domestic US companies may be affected, either via business deals in Europe or through US-dealings with multinationals passing along European data.

As 2017 progresses, so too will corporate efforts to prepare for GDPR. European regulators and analysts have indicated that Member State Data Protection Authorities are expected to take a dim view of last minute attempts at compliance. Others have suggested that 2017 corporate budgets for GDPR preparation should equal the highest potential penalty – 4% of revenue. Because many GDPR obligations are enterprise-wide and operational in nature, giving your organization time to develop and launch new compliance programs is critical. Here are some steps most companies should take in 2017:

First, budget for the new compliance obligations. Under GDPR, many companies must appoint a Data Protection Officer, and may need to add technical expertise like a Chief Information Security Officer. New systems for identifying and tracking data, vendor management, training, and system or process audits may be required.

Next, undertake an assessment to understand your current level of readiness relative to the regulations. In this regard, developing a Data Map that describes how Personal Data is collected or received, how and where it is stored, how it is used, how it flows within and outside of the organization, and with whom it is shared, is a critical component to GDPR compliance (Article 30). A comprehensive and accurate Data Map is the foundation upon which companies can complete a Data Protection Impact Assessment (DPIA), which is required by GDPR to identify "high risks" to data privacy that may occur when processing Personal Data.

Reviewing and updating privacy, information governance, and security policies is another area where companies can take early action. For example, GDPR requires that companies not only provide notice of the information they collect and how they use it, but also the legal basis for processing the data, the company's data retention periods, and the recourse mechanisms available to individuals with a complaint. GDPR also requires affirmative opt-in consent for data collection and sharing, not opt-out, and individuals have a "right to be forgotten." Finally, ensure that your organization has the right procedures in place to detect, investigate, report, and remedy a data breach.

Privacy Shield:

An Uncertain Future

2

By: Amanda Katzenstein, Matt Todd

If 2016 was an exciting year for US-EU privacy relations, 2017 should be the year we learn whether our eleventh hour diplomacy worked. To recap, 2016 was a significant year for transatlantic data privacy, with the EU-US Privacy Shield becoming effective on July 12, 2016, after the prior Safe Harbor agreement was invalidated in October 2015. The US Department of Commerce began accepting self-certifications under the Privacy Shield on August 1, 2016, with the additional incentive that if companies self-certified by September 30, 2016, they would get a nine-month grace period to conform their third-party contracts with the Accountability for Onward Transfer Principle. 2017 has already proven to be eventful, as a new US-Swiss Privacy Shield Framework has been adopted and is scheduled to go into effect on April 12, 2017.

Despite Privacy Shield's acceptance by both US and EU lawmakers (including Switzerland), and despite an initial burst of 1,500 companies seeking certification, Privacy Shield programs are expected to slow in 2017 as companies anxiously await the effective date of Europe's General Data Protection Regulation (GDPR).

GDPR is Europe's new omnibus data protection law that replaces the 20-year-old Data Protection Directive (See Page 1). Uncertainty concerning new challenges to Privacy Shield similar to those which invalidated Safe Harbor, loss of the grace period to ensure Onward Transfer compliance, and the new US administration have all caused some US companies to skip Privacy Shield certification altogether – a trend that may persist in 2017 absent aggressive enforcement campaigns by European Data Protection Authorities.

Confusion over the interplay of Privacy Shield with GDPR, combined with the specter of GDPR's massive fines, may also cause companies to focus on GDPR and lose sight of Privacy Shield. Those that do, may do so at their own peril.

German and French Data Protection Agencies (DPAs), amongst others, have signaled their intention to investigate multinational compliance, and aggressively pursue Privacy Shield violations. 2017 should give US companies the first indication of how Europe intends to monitor and regulate transatlantic data flows. Political tension amongst the US and its NATO allies in Europe coupled with the future of the EU post-Brexit may trickle down to EU Member State DPAs, particularly given the high profile nature of cybersecurity and data breaches. Companies that opt out of Privacy Shield should make good use of legally available alternatives, such as Model Contract Clauses. Given the likely increase in political, regulatory, and technological risks coming in 2017, and the impending launch of GDPR in 2018, companies should dedicate resources to ensure basic levels of privacy and data security compliance.

The Internet of Things:

Momentum for Regulating Privacy

3

By: Spencer Wood, Kathryn Allen

Building privacy and data security considerations into the design, operation and management of new technologies – also known as "privacy-by-design" – is generally considered a best practice when it comes to privacy protection. To date, there has not been significant state or federal regulation around IoT devices. In 2016, however, there were signs the IoT industry could be headed toward a regulatory scheme with a privacy-by-design mandate. Due to political change, Washington will likely have less appetite for pursuing such regulations in 2017.

There were 5.5 million new consumer devices connected to the Internet each day last year. Technology giant Cisco forecasts the market opportunity for IoT devices to be as high as $19 trillion. GE anticipates investment in Industrial IoT to top $60 trillion over the next 15 year. Between connected appliances, home automation, and the semi-autonomous vehicle, the number and prevalence of IoT devices continues to grow significantly. Relatedly, serious momentum started to build in 2016 for a privacy-by-design IoT regulatory scheme. The House formed a Congressional Internet of Things Caucus, co-chaired by former Microsoft executive, Suzan DelBene, to examine the issues IoT devices create for consumers. Members of the House Energy and Commerce Committee held hearings to determine the feasibility and appropriateness of regulating IoT devices, and the FTC has recommended that Congress enact broad-based privacy legislation that will provide clear rules for companies that deal in consumer data collection. Even the Institute for Critical Infrastructure Technology (ICIT) joined in the call for lawmakers to consider regulating the security of connected devices.

"Technology giant Cisco forecasts the market opportunity for IoT devices to be as high as $19 trillion."

With the new administration in Washington and a Republican-controlled Congress, the momentum around new legislation impacting IoT may slow overall in 2017. If a regulatory scheme were to gain a foothold this year, we anticipate it would be measured and probably would involve industries that are already heavily regulated. Healthcare, consumer products, and transportation, for example, are early adopters of IoT technologies, and all are highly regulated by various state and federal agencies. So while companies might see privacy by design incrementally regulated for products like health-monitoring wearables, we doubt there will be a broader regulatory mandate on the horizon in 2017. On the other hand, if the Federal government is slow to address privacy-by-design, an uptick in litigation based on theories of product liability would not be unexpected. In particular, when consumer information is obtained by hacking, or safety and security is compromised, we may see more lawsuits in 2017 asserting that the failure to build privacy-by-design into IoT devices is a product defect.

Whether privacy-by-design considerations in IoT devices are compelled by the legislative or the judicial branch in 2017, one thing is certain: a risk-based approach to identifying digital vulnerabilities in order to close privacy gaps will become a necessity in the IoT field, both for the manufacturer, the seller/reseller, and the consumer.

Russia and China:

Emergence of New Privacy Regimes

4

By: Amanda Katzenstein, Karen Dickinson, Jarno Vanto, Ajay Sharma

China and Russia both expanded their protectionist policies in privacy and data protection in 2016. In 2017, those trends will likely continue, as both economic and geopolitical forces impact government policies in both countries.

Recent events point towards increased data localization enforcement by Russia in 2017. On November 17, 2016, for example, Russia's federal agency for telecom, information technologies and mass communications (its data protection regulator), *Roskomnadzor*, blocked access to LinkedIn within Russia for violating Russia's Federal Law No. 242-FZ (No. 242), which, among other things, requires that data operators store personal data of Russian citizens on servers located within Russia's borders. In early 2017, Russian authorities demanded the LinkedIn app be removed from Apple and Google Russian app stores. Most US companies operate in violation of No. 242, and it is safe to expect that Russia will carry out similar enforcement actions against non-Russian companies in 2017.

China will also remain active regarding data privacy. President Xi's effort to protect China's "cyber sovereignty," combat hacking, exercise control over China's Internet, and protect personal information, resulted in many new laws, regulations and administrative guidance in 2016, that affect everything from telecommunications and Internet service providers, to website operators, ridesharing and mobile apps, and online payments. In 2017, China will likely pass new laws, implement new/existing regulations, and provide administrative guidance. Importantly, China's new overarching Cybersecurity Law (effective June 1, 2017), as well as Draft Regulations, codify previous requirements for the protection of personal data. Companies operating websites in China will soon be subject to a number of new obligations, such as providing notice of use of personal data, following the principles of legitimacy, rightfulness, and necessity in collection of personal data, obtaining consent for data transfers, and providing "technical support" and assistance to the authorities in investigations.

Operators of "critical information infrastructure" (CII), such as the public communication and information services, energy, transportation, water resource utilization, finance, and public service sectors, have additional obligations, including data localization and annual government network safety assessments. The new requirements could result in CII operators and their suppliers needing to disclose source code or other secret information to the government, and Chinese standards becoming trade barriers for US exporters. Companies should monitor regulations and administrative guidance relating to the Cybersecurity Law as these are published, to determine whether and how the companies may be impacted.

Health Care:

Data and Uncertainty Reign Supreme

5

By: Lisa Acevedo, Lindsay Dailey

In 2017, no industry may have a more uncertain future than the healthcare industry. Notwithstanding the change in Administration and potential repeal of the Affordable Care Act, three recent trends are likely here to stay. First, the acceleration of population health utilizing data and technology will continue. Second, cybersecurity threats will disproportionately target healthcare organizations. And third, increased enforcement action by OCR and state attorneys general can be expected.

Despite potential changes to policy out of Washington, the shift in health care delivery and payment models from fee-for-service, to a quality of care, clinical outcomes-based model, is here to stay. Healthcare organizations will accelerate efforts to collect data about patients, including capturing health data directly from patients through technology. Healthcare providers and payors will increasingly attempt to predict health outcomes and assess financial risk under the new reimbursement paradigm through data analytics. To that end, 2017 will see increased efforts to capture and analyze patient data, including collecting data directly from patients through wearable devices.

Providers, payors and their vendors will likely enter into increasingly complex data sharing arrangements that may not be contemplated under HIPAA, state, or other privacy laws. Increased collection and analysis of patient data will heighten risks for data breaches. The ability to truly de-identify these data sets will be an increasing challenge, as vast amounts of data are connected and data analytics tools become even more powerful. Notwithstanding the regulatory risks and increased breach liability, patient data collection and analytics will continue to accelerate in 2017.

> “...companies should implement a more proactive approach to mitigating cyber risk.”

The rapid adoption of new technology and vast amounts of sensitive data will continue to make healthcare companies a primary target of cybercriminals. Accordingly, healthcare entities should prioritize and budget for cybersecurity risks, including investing in key resources (IT staffing, risk analysis and assessment tools, encryption technology) to defend against and respond to constantly-evolving cyber threats. Increasingly sophisticated ransomware attacks targeting health care providers are likely to accelerate (see Page 8), so companies should implement a more proactive approach to mitigating cyber risk.

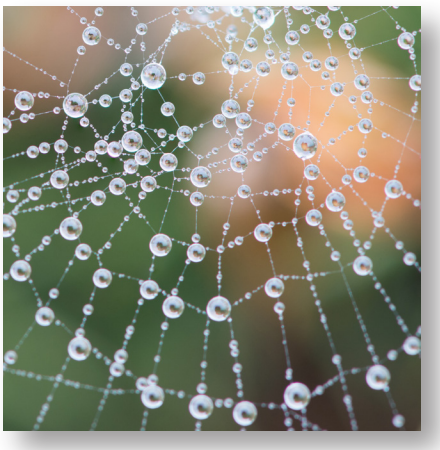
Finally, the Office for Civil Rights (OCR) will continue its pattern of heightened enforcement in 2017, building on a record year of settling 11 cases in 2016 (including the first action against a vendor Business Associate). OCR has also announced an initiative to more widely investigate breaches affecting fewer than 500 individuals, so anticipate increased investigation and enforcement of incidents that traditionally were not as highly prioritized. Similarly, state Attorneys General (AGs) will likely increase their own enforcement activity under state breach notification laws. Several states recently expanded the definition of “personal information,” changed their approach to encrypted information, and adjusted the timing requirements to notify affected individuals and AGs (see Page 6). Concurrently, companies should expect to see AGs exercise their authority under the HITECH Act to bring civil actions on behalf of their residents for violations of the HIPAA Privacy and Security Rules.

No State Left Behind:

How Privacy Law is Trending Stateside

By: Nicole Poulos, Daniel Farris

2016 saw at least a dozen states enact amendments or new statutes respecting privacy and data security. Today, forty-seven states (plus D.C., Guam, Puerto Rico, and the Virgin Islands) have enacted laws governing data breach notification. More than half of US states have data disposal statutes (statutes governing how a business must dispose of personally identifiable information). In 2017, states will continue to move beyond breach notification statutes, instead addressing the collection, storage, security, and disposal of data containing personal information. New and proposed legislation requires affirmative corporate action, not just a timely response when faced with a breach. The breadth of such statutes is widespread, regulating the private sector across multiple industries and various state agencies.



The number and variety of state privacy laws should continue to keep US companies on their toes. About half of US states, for example, now have laws regulating an employer's access to the online account username or password of employees. Other similar state laws apply to educational institutions and their access to students' online accounts, or to landlords for similar purposes. As social media becomes a more integral part of people's lives, more states are likely to adopt comparable statutes. Illinois, for example, added provisions in 2016 regulating the actions of employers and prospective employers with respect to online accounts of employees or job applicants (see the Illinois Right to Privacy in the Workplace Act).

As technology continues to advance in the age of IoT and "smart" everything, companies should expect increased state legislation in transportation, home automation, and e-commerce. California, for example, has enacted laws governing smart TVs. With existing assistive technologies progressing to full autonomy, particularly in the auto industry, state legislatures are taking notice. A number of states have passed, or are actively pursuing, legislation regulating automated driving. The US Department of Transportation and National Highway Traffic Safety Administration have also issued guidance on automated vehicles, with an update last year, that may influence how states approach new autonomous vehicle laws.

Finally, unlike in years past, 2016 also saw an increase in regulations and rule-making on the federal level. Congress passed the Support for Rapid Innovation Act (H.R. 5388) and the Leveraging Emerging Technologies Act (H.R. 5389), and President Obama issued a Policy Directive on United States Cyber Incident Coordination. 2017 may well see a rise in the number of states adopting similar statutes mandating a proactive stance on privacy and data security, or that further refine corporate obligations in response to a breach. US companies should implement or amend privacy programs to ensure compliance with the evolving state and federal legislative privacy and data security landscape.

Privacy Litigation:

Consumer Advocacy Dominates the Litigation Landscape

7

By: Rockwell Bower, Zuzana Ikels, Rodney Lewis, Gina Caya

In 2017, litigation will likely focus on the growing discord between consumers' right to privacy and efforts by advertisers and other service providers to collect and use personally identifiable information. Consumers will continue to advocate for their individual privacy rights, both in traditional courts and in administrative tribunals, most notably before the Federal Trade Commission (FTC).

The US Supreme Court's decision in *Spokeo v. Robins* may have a moderate chilling effect on new consumer class actions in 2017, although plaintiffs will undoubtedly continue to assert new, creative theories and other statutory violations for actual or perceived privacy violations. The *Spokeo* decision held that a "technical" violation of a statutory violation without evidence of concrete harm to the plaintiff was not sufficient to find standing. Many privacy class actions have since been dismissed by lower courts, but several other circuits have reversed dismissals involving data breach and theft of personal information lawsuits, finding that allegations of credit card and/or identity theft were sufficient to establish standing, even where there was no direct evidence or existing damages.

Two recent privacy class actions that should be closely monitored are *Smith v. Facebook*, Case No. 16-cv-01282 (N.D. Cal 2016) and *Martinez v. Snapchat*, Inc., Case No. BC-621391 (Cal. Sup. Ct. 2016), both consumer class-actions seeking redress for connecting individuals' identity and private information with on-line activity, without the user's consent or knowledge. *Smith* alleges that Facebook obtained its users' web-searching history of health-related conditions through "scraping" and cookies, and then facilitated targeted advertising to medical providers. *Martinez* alleges that Snapchat's retention of biometric information, including users' faces, violates their privacy and Illinois' Biometric Information Privacy Act.

Federal and state regulatory enforcement actions are also expected to remain active. The FTC has brought several actions against organizations that allegedly violated consumer privacy rights or misled consumers by failing to adhere to published security protocols and mishandling sensitive information. In 2016 alone, the FTC settled 9 suits for privacy violations for millions of dollars in fines and issued several Final Orders against entities charged with unfair data security practices. Although the effect of the presidential administration is unclear, the FTC's enforcement efforts are predicted to grow in 2017.

Ransomware, Phishing, and the Cloud:

8

Distributed Threats to Privacy and Data Security

By: Joe McClendon, Dov Scherzer

The use of phishing attacks to access personal data and the use of ransomware to extract money from unwitting victims have both been profitable for cyber criminals for years – so much so that the number of attacks has been climbing exponentially. That trend is not likely to change in 2017.

Ransomware is a type of computer malware that blocks access to a user's computer files, usually in one of a number of ways. Currently, the most successful variant is "crypto ransomware," a technology that encrypts files on an infected computer or network, thereby rendering them unusable until a ransom is paid. Crypto ransomware is increasingly being used by cybercriminals because a large number of users do not back up their data (so applying unbreakable encryption is a nearly guaranteed way to extract ransom payments). Companies should expect to see ransomware infections continue to hit home in 2017. Although many businesses have increased user training and improved IT practices, the cyber skills gap amongst employees continues to grow. Privacy-oriented companies should educate end users about ransomware through comprehensive training, be vigilant about IT practices and security, and stay abreast of new malware variants that exploit unknown vulnerabilities (or that can self-propagate across networks). Deterrence and detection are of critical importance, as malware that exploits unknown vulnerabilities and can autonomously spread to other systems has the potential to create catastrophic results as IT departments struggle to keep non-infected systems online while also allowing access to user data.

Phishing remains the most effective means for cyberattacks (and the distribution of malware), so companies should not anticipate any decrease in phishing activity in 2017. Despite all of the time and money spent on corporate training, users simply cannot stop themselves from clicking on links and opening documents from unknown senders. Spear phishing, the type of phishing directed to a specific person or group of people, has also continued to be effective as cyber criminals have become more savvy in how they spoof trusted senders. Obtaining account passwords and distributing malware through fraudulent password recovery emails is the oldest trick in the book, but cyber criminals continue to rely on it simply because it works.

Cloud adoption rates will continue to grow in 2017 and, in particular, businesses in highly regulated sectors, such as healthcare and banking, will continue to deploy cloud-based solutions at a an even higher rate. With the appeal of moving data and infrastructure to the cloud, however, and despite advances in cybersecurity, the increasingly distributed nature of corporate networks is likely to continue to give way to a significant number of high profile data breaches. As data moves to outsourced data centers, one chink in a company's proverbial armor can lead to a significant breach. Companies must not only have their cyber response plans up-to-date, but also be prepared to deal with situations in which access to their data is impossible because of unplanned outages related to cyber attacks. Employee training, exercising, and audits should also be part of any company's privacy compliance program.

Privacy and Data Security Practice

The firm's data privacy and security team is experienced in industries ranging from health care to banking, and telecommunications to retail. Our lawyers advise clients on internal vulnerabilities and compliance, and regularly assist with vendor management, cybersecurity insurance evaluation, and employee education and compliance training initiatives. Polsinelli's team includes former software and systems engineers, network administrators, and information privacy professionals certified by the International Association of Privacy Professionals. Whether ensuring appropriate data security standards in a vendor agreement or ensuring compliance with the European Union's Data Protection Directives, Polsinelli provides practical and timely advice tailored to a company's specific data privacy needs.

Services to our clients include:

- Compliance and Security Counseling
- Transactional Support
- Data Breach and Rapid Response
- Breach Litigation and Counseling

Visit our online blog at
polsinellionprivacy.com

our clients say

direct and practical

"There is a definite distinction in style that you can identify from firm to firm. Some firms are shrouded with exceptions, caveats and legal speak. I want direct statements, practical help, and I get that at Polsinelli."

understanding clients' real world situations

"Polsinelli is excellent at that. They do a great job at deeply understanding what we do and are trying to accomplish. When negotiating, they know what's important to us and the right trade-offs, and they apply their legal knowledge based on that."

About the Firm

Polsinelli is an Am Law 100 firm with more than 800 attorneys in 20 offices, serving corporations, institutions, and entrepreneurs nationally. Recently ranked #17* for client service excellence among firms servicing Fortune 500 clients, the firm has risen more than 50 spots in Am Law's annual firm ranking over the past five years. Polsinelli attorneys provide practical legal counsel infused with business insight, and focus on health care, financial services, real estate, intellectual property, mid-market corporate, labor and employment, and business litigation. Polsinelli attorneys have depth of experience in 100 service areas and 70 industries.

**2017 BTI Client Service A-Team Report*, Nov 2016

About the Authors

Daniel Farris
Shareholder
312.463.6323 | dfarris@polsinelli.com

Daniel co-chairs Polsinelli's Data Center & Infrastructure and Data Privacy & Security team. As a former software engineer and network administrator in the telecommunications industry, Daniel offers his clients real-world experience in fiber optic networking, data center operations, cloud computing, mobile app development, and data privacy and security matters including data privacy and security compliance, counseling, and audits and breach counseling, notice, and response.

Lisa Acevedo
Shareholder
312.463.6322 | lacevedo@polsinelli.com

Lisa Acevedo has decades of experience in HIPAA and health information privacy and security. As the Health Information Privacy and Security Co-Chair, Lisa provides strategic counsel in the areas of federal health privacy laws and regulations, as well as state laws governing the confidentiality of health information, mental health records, and records containing other highly sensitive information.

Karen Dickinson
Shareholder
602.650.2328 | kdickinson@polsinelli.com

With a background in negotiating multimillion-dollar global contracts, Karen acts as outside general counsel for United States companies and for companies investing in the United States from other countries. She negotiates technology transactions, from simple software licenses to complicated research and development agreements. She has extensive experience advising on joint ventures and alliances, product distribution, intellectual property protection, and anti-counterfeiting strategies.

Zuzana Ikels
Principal
415.248.2114 | zikels@polsinelli.com

Zuzana's litigation practice focuses on handling complex commercial disputes, with particular emphasis in the healthcare, health tech and technology, and telecommunications industries. She has an in-depth familiarity with IT and Big Data infrastructures, from advising on electronic records and retention programs, privacy and customer consent policies, devising strategic, e-discovery plans, database discovery and Big Data analytics.

About the Authors

Rodney Lewis
Shareholder
312.873.3686 | rlewis@polsinelli.com

Rodney has assisted corporate clients in complex commercial litigation matters, including privacy and data security issues, consumer class action defense under the Fair Credit Reporting Act and False Claims Act defense. He has successfully defended several clients in civil trials, defeated motions for class certification, won cases on summary judgment, obtained favorable results for clients through alternative dispute resolution processes, and negotiated favorable settlements for clients where appropriate.

Dov Scherzer
Shareholder
212.803.9925 | dscherzer@polsinelli.com

Dov's experience in in cyber-security includes counseling clients (customers and vendors) in connection with negotiating complex privacy, data security and related audit provisions in global IT outsourcing and other services agreements where the services involve the processing of highly sensitive data. That counseling is informed by an understanding of global privacy and data security laws and regulations, all of which must be taken into special consideration when entering into agreements.

Matt Todd
Shareholder
713.374.1650 | mtodd@polsinelli.com

Matt represents technology companies at all stages of the business lifecycle including organization and formation agreements, funding agreements, employment agreements, intellectual property development agreements, licenses, non-disclosure agreements and joint ventures. Currently, Matt serves as outside general counsel to several clients in high-tech, defense, and regulated industries. In addition to his legal experience, Matt has more than 10 years of experience in network administration and operations.

Jarno Vanto
Shareholder
212.413.2841 | jvanto@polsinelli.com

Jarno's extensive international experience allows him to partner with clients to help them achieve their business goals and provides a range of legal services, including global privacy and cybersecurity compliance programs, cross-border and domestic intellectual property licensing and other technology transfer agreements, and counsel for foreign technology companies. Prior to joining the firm, Jarno was a Legal Expert for the European Privacy Seal, where he evaluated information technology products and services with the intent of awarding them the EuroPrise European Privacy Seal.

About the Authors

Spencer Wood
Shareholder
312.873.3677 | swood@polsinelli.com

Spencer Wood began his career litigating disputes involving trade secrets, patents, and commercial contracts. Now, he applies that experience as he brings value to clients seeking to exploit and protect intellectual property rights. Spencer focuses on intellectual property asset management, information technology, digital media, and privacy rights. He regularly counsels clients engaged in structured acquisitions of technology assets, as well as the licensing and transfer of trademarks, patents, and copyrights.

Kathryn Allen
Associate
816.572.4884 | kallen@polsinelli.com

Kathryn's practice focuses on the often intersecting areas of information security/privacy, technology licensing/use, and intellectual property protection and monetization. She works in a variety of industries, including the heavily regulated health care and financial services industries as well as the technology startup and entrepreneurial space including craft breweries, software developers and technology outsourcers.

Rockwell Bower
Associate
214.661.5510 | rbower@polsinelli.com

Rockwell Bower is a trial attorney who focuses his practice on commercial litigation, antitrust, class actions, and information privacy. He is also a Certified Information Privacy Professional (CIPP/US), and his practice includes identifying, evaluating and managing risks associated with clients' privacy and cyber security issues. He advises clients on compliance with state and federal privacy regulations, data security requirements, and data breach notification procedures, including GLBA, HIPAA, HITECH, FCRA, other U.S. state and federal privacy data security requirements, and global data protection laws.

Gina Caya
Associate
415.248.2119 | gcaya@polsinelli.com

Gina is a litigator who focuses on protecting and defending clients in all phases of litigation. Her clients appreciate her dedication to understanding their business needs and challenges. Using her experience in a variety of industries, she finds creative and tailored solutions to her client's issues. Gina's practice includes contract disputes, real estate disputes, trade secrets cases, merger and acquisition litigation, food and drug law, and regulatory compliance.

About the Authors

Lindsay Dailey
Associate
312.873.2984 | ldailey@polsinelli.com

Lindsay serves clients at the intersection of healthcare regulatory and privacy/data security compliance. Prior to joining the firm, Lindsay worked with the American Medical Association, American Dental Association, and Rehabilitation Institute of Chicago. This in-house experience in corporate compliance and regulatory issues serves her practice and her clients well.

Amanda Katzenstein
Associate
415.248.2169 | akatzenstein@polsinelli.com

Amanda uses her extensive media and technology experience to assist clients with resolving their legal challenges. Experienced in privacy issues, she has been certified by the International Association of Privacy Professionals as a CIPP/US. She also develops trademark strategies for technology and media companies to accomplish their business goals with a particular focus on online advertising and mobile apps.

Joe McClendon
Associate
816.218.1266 | jmcclendon@polsinelli.com

Joe McClendon draws upon a rich history of working in IT project management to structure and negotiate technology agreements for Polsinelli's clients. He is IAPP CIPP/US certified and has nearly a decade of information technology and project management experience in the higher education and telecommunications industries.

Nicole Poulos
Associate
312.873.3687 | npoulos@polsinelli.com

Nicole Poulos is a technology attorney with particular experience in cloud computing, data center and infrastructure, and privacy and data security matters. Nicole began her career as a litigator, helping clients navigate complex business disputes. She now leverages the business insights she gained to provide clients with strategic, practical, and actionable advice on a variety of technology matters. She serves clients in industries ranging from telecommunications and technology to healthcare, financial services, retail, and manufacturing.

About the Authors

Ajay Sharma
Associate
816.218.1215 | asharma@polsinelli.com

Ajay's practice focuses on information security, data privacy, infrastructure, and health care technology transactions, but his experience spans a vast array of technology and intellectual property matters. In advising clients, Ajay draws on valuable technology industry experience, having worked at technology companies large and small prior to law school, including a major global technology company in its datacenter operations division.

For More Information

please contact

Daniel L. Farris, Shareholder
Polsinelli
161 N. Clark Street, Suite 4200
Chicago, IL 60601
312.819.1900 | dfarris@polsinelli.com

Lisa J. Acevedo, Shareholder
Polsinelli
161 N. Clark Street, Suite 4200
Chicago, IL 60601
312.463.6322 | lacevedo@polsinelli.com

polsinelli.com

polsinelli.com/services/privacy-and-data-security


POLSINELLI