Silent Privacy

By Gamelah Palagonia, FIP, CIPM, CIPT, CIPP/E, CIPP/US, CIPP/G, ARM, RPLU+

Data security or cyber security rests upon the broad principles of confidentiality, integrity and availability of information assets. Known as the CIA triad, the principles can be summarized this way:

Confidentiality	Information can only be accessed by those who have a legitimate business purpose.
Integrity	Information is protected from unauthorized access or unintended changes or use.
Availability	Information is available to those who need it, when they need it.

Data privacy or information privacy is connected to and dependent upon data security or cyber security, but the principles are very different.

Data privacy

A common saying among privacy professionals is that you can have security without privacy but can't have privacy without security.

Think of it this way: People live in a completely secure home that no one can enter or leave without express permission. However, the home is made of transparent materials so their activities are on full display. They find themselves in a reality show in which details of their daily lives are packaged and sold without compensation -- except for the security.

Growing privacy concerns need to be effectively addressed in data privacy risk management.

This may sound like a story from a sci-fi TV series but, in our very real data-driven society, our personal data is being collected every day, either online or while in public or in presumed "private" places such as our homes. While consumers may assume their data is protected, in fact data security is not a given.

A new study from Pew Research Center reveals growing concern among Americans about their digital privacy and the fear that businesses are not good stewards of the personal data that is collected, stored and used. People increasingly want to know what data is being collected, who is collecting it, how it will be used -- and especially if it can be used against them. These growing privacy concerns need to be effectively addressed in data privacy risk management.

Tales from the data privacy crypt: Secret consumer scores and hidden digital fingerprinting

A recent New York Times article, "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too," tells a troubling account of off-the-radar companies that develop "secret consumer scores" or ratings. These ratings in turn are sold to other companies that may use the data to determine, for example, how long you wait on hold for customer service – or even the overall level of service quality that you receive. A low score may send you to the back of the line; high scores may yield elite treatment. In the writer's quest to find out what data had been collected about her, she was shocked to receive a 400-page report from one company that contained all the messages she had ever sent to hosts on Airbnb, years of Yelp food deliveries, and a log of every time she opened her iPhone's Coinbase app. In fairness, some of the companies use the data to fight fraud, but that's hardly the purpose in knowing of the writer's fondness for chicken tikka masala. She's living in the transparent house – secure but without privacy.

The Washington Post recently highlighted an experiment with Disconnect, a privacy software company. Disconnect found that at least a third of the 500 websites Americans visit most often use hidden "fingerprinting" code to extract technical information about user computer and their web browsing patterns.

Fingerprinting is not necessarily a bad thing. Fingerprinting can be used to run identity checks, prevent consumers from sharing a password, identify fraudsters and block harmful bots. Websites also may use digital fingerprints to know if consumers have visited before and to create profiles of consumer behavior. (The latter explains the use of targeted ads that follow consumers around the internet.) Websites draw on a variety of data points to build digital fingerprints. Apps on phones or tablets have even more personal data attributes to build digital fingerprints.

The bad thing is digital fingerprinting is not transparent, and few consumers are aware that they leave fingerprints on even some of the most routine web activities. Most websites do not disclose that they are creating digital fingerprints in their public-facing privacy notices, much less make it clear how they and their third-party partners might use and share that data.

Many companies may not realize the extent to which they collect and utilize digital fingerprints because they don't collect the data directly. They often rely on third parties, such as ad tech partners, to operate parts of their websites, and to glean and leverage consumer data, often for sale and marketing. In fact, marketing appeared to be the largest use for fingerprinting among the sites identified in the Disconnect experiment.

Digital fingerprinting should be disclosed to consumers, period. To stay out of regulatory crosshairs, at minimum, companies should give consumers the right to opt out of digital fingerprinting in addition to the rights to:

- Access personal data collected, shared or sold.
- Rectify or delete personal data.
- Restrict collection or use of personal data.
- Object to automated decision making (such as the secret consumer scores described by *The New York Times*).

From a risk management perspective, organizations should not expect regulators to be lenient just because executives don't know what their third-party partners or website operators are doing. Third-party risk oversight should be a standard component of data privacy risk management and in any case is required by regulations such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR).

Actions to protect consumer privacy are not just playing defense to avoid litigation or a regulatory crackdown. Companies that respect consumer privacy and provide transparency can create new business potential and win customer loyalty. Consumers may welcome the opportunity to shape their own digital fingerprint or profile based on products or services they use or desire, where they want to shop, what ads they want to see and what personal data is made available to third parties. Google, for example, already permits users to influence their fingerprints on its popular search engine. This model needs to be simplified and applied universally.

If behavioral advertising and marketing is about anticipating consumer wants, then consumer sentiment should be loud and clear. Forward thinking ad-tech and digital marketing companies have the opportunity to stay in front of consumer sentiment that is increasingly skeptical of intrusive digital technology. Market leadership will belong to advertising and marketing companies that are best at innovating and creating new ways of doing business while adapting a privacy-minded organizational culture.

Data privacy compliance

Data is the new currency. Leveraging the power of data to gain competitive advantages is a business reality, and doing it transparently and responsibly is both an ethical and a regulatory imperative.

The broad principles of data privacy compliance govern the collection, use, access, disclosure, disposal and retention of personal data. These principles are entwined throughout data privacy regulations in Europe and the United States.

Compliance with data privacy laws and regulations is more challenging than ever, and 2018 heralded a data privacy regulatory revolution. The EU's GDPR of that year was followed by California's ground-breaking CCPA and copycats that have been proposed across the United States. These new regulations have strengthened consumer rights and created new obligations and requirements for businesses.

In simple terms, regulations such as GDPR and CCPA require informed consent from consumers at the point of data collection. Informed consent involves transparency, which means disclosing to consumers how their personal data is to be used, shared or sold. Businesses covered by these regulations are also required to provide consumers with access to their data and the ability to rectify, delete and or restrict their data. They may also have the right to opt-out or object to automated decision making. This may sound easier than it actually is. The regulations entail operational changes relative to deploying new technologies and changing processes or hiring new staff to lead data privacy compliance.

In assessing whether data privacy practices are legally compliant, businesses need to seriously consider not only security breach notice laws and data protection laws. They also must weigh the impact and requirements of unfair business practices as well as new and developing consumer protection laws. This is a specialized, complex legal area that requires the advice of data privacy counsel.

With the potential for high fines and developing class-action exposure, the cost of non-compliance significantly outweighs the cost of compliance.

Privacy by design (PbD)

One effective method that organizations should consider implementing is Privacy by Design (PbD) to minimize their exposure to liabilities associated with non-compliance with data privacy regulations. PbD is a framework developed by Ann Cavoukian, Ph.D., Information & Privacy Commissioner, Ontario, Canada, based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure and business practices. PbD essentially means intrinsic or "silent" privacy.

PbD includes a set of seven information management principles that can apply to specific technologies, business operations, physical architectures and networked infrastructure – or even to entire information ecosystems and governance models. The seven (7) principles are:

1 *Proactive not reactive – Preventative not remedial*

The PbD approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.

2 *Privacy as the default*

PbD seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3 *Privacy embedded into design*

PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4 *Full functionality – positive-sum, not zero-sum*

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible and far more desirable to have both.

5 *End-to-end security – lifecycle protection*

PbD, having been embedded into the system prior to information collection, extends securely throughout the lifecycle of the data involved. This ensures that all data is securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, PbD ensures cradle-to-grave, secure lifecycle management of information.

6 *Visibility and transparency*

PbD seeks to assure all stakeholders that, whatever the business practice or technology involved, it is operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent to both users and providers alike.

7 *Respect for user privacy*

Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.

A PbD tool that organizations can utilize is a Privacy Impact Assessment (PIA). The purpose of the PIA is to minimize privacy risks while meeting the aims of a specific project, such as a new product/service or a digital marketing campaign. PIAs assist organizations by identifying and addressing risks at an early stage by analyzing how proposed uses of personal data and technology will work in practice.

PIAs are typically designed to accomplish three major goals:

- Ensure conformance with applicable legal, regulatory and policy requirements for data privacy.
- Identify and evaluate the risks of privacy breaches.
- Identify appropriate privacy controls to mitigate unacceptable risks.

Since PbD comes before-the-fact and not after, it is difficult to embed PbD into existing technologies and business practices without new technologies, specialized data privacy talent and organizational cultural changes. The changes may be costly at the onset but definitely worth it in the end.

Cyber insurance

Following the large-scale 2017 WannaCry and NotPetya cyber attacks, we witnessed how data security or cyber security incidents presented silent cyber risks involving insurance claims that may trigger traditional property or casualty insurance policies that were not intended to cover cyber exposures.

Traditional cyber insurance was intended to cover regulatory actions and subsequent fines and penalties stemming from security incidents or data breaches, not the actions relative to legal or regulatory non-compliance such as the unlawful use of personal data in the absence of any security incident or data breach.

The proliferation of consumer rights and business obligations under new and developing data privacy consumer protection laws in the U.S. and the EU has not only pushed data privacy into center stage, it has also created silent privacy exposures for businesses as well as their professional liability insurers.

Employment Practices Liability (EPL)

A decade ago, Illinois enacted the Biometric Information Privacy Act (BIPA), becoming the first state to require companies collecting biometric attributes such as facial, fingerprint and iris scans to obtain prior consent from employees or consumers. BIPA also established safeguards and procedures relating to the retention, collection, disclosure, use and destruction of biometric data.

Washington and Texas have passed similar laws. However, BIPA remains the only law that includes a private right of action that allows private individuals to file lawsuits for damages stemming from BIPA violations. BIPA includes statutory penalties of $1,000 for each violation and $5,000 if the violation is intentional or reckless.

While recent BIPA cases have been largely litigated in Illinois, the Ninth Circuit Court of Appeals recently applied BIPA in Patel v. Facebook, a class action lawsuit filed in the Northern District of California. The Ninth Circuit is the first federal circuit court to conclude that a plaintiff alleging a BIPA violation has standing for purposes of Article III of the U.S. Constitution. The ruling makes it easier for plaintiffs to certify BIPA class actions, ***within and outside of Illinois.***

Most cyber insurance policies exclude employment-related practices with a caveat that the exclusion would not apply to an otherwise covered claim. Cyber policies typically provide coverage in the event of a data breach or security incident involving employee data. The operative term and coverage trigger is *"data breach or security incident."* Few cyber insurance policies cover the wrongful use of personal data in the absence of any data breach or security incident, which would essentially afford coverage for BIPA actions. However, cyber insurers did not intend to afford Employment Practices Liability (EPL) insurance under cyber policies and may seek to exclude BIPA going forward in 2020.

Both cyber insurers and EPL insurers have paid BIPA claims during 2019, but EPL is the appropriate coverage for BIPA actions filed by employees. Properly written cyber insurance policies that include the Wrongful Use of Data coverage trigger would provide coverage for BIPA claims made by consumers. Organizations should be prepared to answer BIPA-related underwriting questions as part of their EPL renewal process and should also consider increasing their EPL limits.

Cyber coverage clarity

Wrongful Collection v. Wrongful Use

The coverage term "wrongful collection" stems from a relatively old law called the Song-Beverly Credit Card Act of 1971. The act was designed to protect consumers from having their personal identification information stored and subject to unauthorized use by retailers. In 2011, a California Supreme Court ruled that the act prohibits the collecting and storing of customer zip codes when completing credit card transactions, opening the door to class-action law suits alleging privacy violations. Under modern laws such as GDPR and CCPA, rightfully collecting personal data is a given, it is the "wrongful use" of personal data that creates the legal liabilities.

Management & fiduciary liability

It took time and major cyber attacks for cyber security discussions to dominate boardroom conversations. Boards of directors are ultimately liable and responsible for the survival of their organizations, and data privacy should be big part of that responsibility in today's data-sharing economy.

The National Association of Corporate Directors (NACD) Director's Handbook on Cyber-Risk Oversight outlined five principles that all corporate boards should consider as they seek to enhance their oversight of cyber risks. The five NACD principles can be easily adapted for data privacy:

- Directors need to understand and approach data privacy as an enterprise-wide risk management issue, not just a compliance issue.
- Directors should understand the legal and regulatory implications of data privacy risks as they relate to their company's specific circumstances.
- Boards should have adequate access to data privacy expertise, and discussions about data privacy risk management should be given regular and adequate time on the board meeting agenda.
- Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
- Board-management discussion of data privacy risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Some executives make the mistake of assuming that their cyber risks are covered by existing policies. Some may even accept a high degree of risk in the belief that compliance with data privacy laws and regulations may be too onerous and burdensome. This would not be a wise approach. Cyber insurance does not cover intentional wrongful acts except under certain circumstances, such as those that may be committed by a rogue employee (i.e. stealing data, or intentionally making data available to unauthorized users).

Furthermore, organizations that adopt the non-compliance approach may unwittingly be tapping their Directors & Officers Liability limits of insurance relative to regulatory actions and class-action claims made by employees or consumers for violations of data privacy laws. Underwriters of Directors & Officers insurance are aware of the potential of increasing exposures. Policyholders should expect underwriting questions to that end.

Further, laws proposed in 2019 such has the New York Privacy Act impose new fiduciary liabilities. If enacted, the N.Y. privacy act would require companies to disclose their methods of de-identifying personal data, to place special safeguards around data sharing and to allow consumers to obtain the names of all entities with whom their data is shared. The act includes a private right of action, not just in the context of data breaches like CCPA but for any violation of the law.

Conclusion

The term "digital transformation" is widely used to describe how technology has radically changed the way consumers work, shop and entertain themselves. In the past, consumers have been willing to trade a degree of privacy for the speed and convenience of new technology. But this tolerance is fading as consumers better understand how personal information is gathered and used without their knowledge or consent.

Consumer concerns are reflected in heightened litigation and a growing web of regulations as evident in Europe and North America. In this new environment, companies must develop and maintain robust data privacy risk management efforts, including insurance coverage that addresses emerging privacy- and data-related exposures.

The creative yet disruptive power of digital transformation will continue to pick up speed. Risk management must move at the same pace to protect an enterprise, its shareholders and employees.

Willis Towers Watson hopes you found the general information provided in this publication informative and helpful. The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal advisors. In the event you would like more information regarding your insurance coverage, please do not hesitate to reach out to us. In the United States, Willis Towers Watson offers insurance products through licensed subsidiaries of Willis North America Inc., including Willis Towers Watson Northeast, Inc.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW371684/12/2019

willistowerswatson.com

Willis Towers Watson