# Owning, using, and protecting data:

## opportunities and risks for leading insurers

Insurance Governance Leadership Network

January 2019


Insurance Governance Leadership Network

January 2019

IGLN

VIEWPOINTS

# Owning, using, and protecting data: opportunities and risks for leading insurers

Competitive pressures are driving insurers to seek the greatest possible advantage from the large amounts of data at their disposal. At the same time, security and privacy concerns are limiting their ability to do so. Regulation and customer expectations are elevating standards for privacy and data governance, and insurers need to develop systems, personnel, and governance policies to meet these higher standards. *"Both from a regulatory standpoint and from the point of view of information security and customer expectations, you need to build privacy requirements into the DNA of how you work as an organization,"* one IGLN participant said.

*"You need to build privacy requirements into the DNA of how you work as an organization."*

—Participant

Yet even while they face greater constraints on how customer information can be deployed, insurers are using big data to improve underwriting, risk management, operating efficiency, customer relations, and product innovation. The challenge for the industry is to manage the tension between deriving strategic value from data, safeguarding consumer rights, and maintaining industry and company reputations.

IGLN participants met in New York on December 5 to explore issues around this tension. This *ViewPoints* synthesizes three key themes emerging from the meeting and related discussions:

- **Big data and data analytics have the potential to generate significant business opportunities for insurers**
- **Significant challenges impede insurers' efforts to get maximum value from their data assets**
- **Senior leaders are tackling the challenges of privacy and data governance**

## Big data and data analytics have the potential to generate significant business opportunities for insurers

The proliferation of data and the emergence of new analytic tools create material opportunities. A staggering volume of data is being generated every minute—emails, texts, images, internet searches, data from internet of things (IoT) devices, and consumers' purchasing and entertainment habits. Firms in every sector are developing ways to monetize it; for example, tracking and analyzing mobile phone users' location and movements—sometimes down to the minute—has become a big business. Dozens of companies track location data through apps on users' phones, then use it to sell highly targeted advertising—an estimated $21 billion in 2018.[1]

Insurers possess immense amounts of data about their customers and are beginning to make efforts to derive greater advantage from it. One IGLN participant said, *"This industry, especially life, is at the infancy stage in doing this. The question is, 'How can we revolutionize life underwriting for the first time in 50 years?' It may take 10 years to do that. It's a worthwhile journey, but the journey is just starting."*

*"What happens when we get blindsided and disrupted by a data-driven company competing in a space where we have done business?"*

—Participant

The stakes are high. One industry observer predicted, "Insurers who take advantage of the opportunity in data and analytics will outperform those who do not."[2] An IGLN participant agreed: *"I've always said the one who wins on data will win."*

The effective use of data is critical for long-term survival. One participant said, *"Where the rubber meets the road is, what happens when we get blindsided and disrupted by a data-driven company competing in a space where we have done business?"* Another simply said, *"We have to be good at data to compete."* Boards have to ensure that these strategic challenges and opportunities remain on the agenda. One director said, *"I need to bring up with the board, 'Do we have a full-fledged data strategy, a cohesive top-down data strategy?'"*

IGLN participants identified several areas where new uses of data present significant business opportunities:

- **Improving the customer experience.** *"The question in the near field is, 'How do we use data to personalize the customer experience?'"* said one member. Another mentioned their work in *"developing value-adding products from sensor data."* Insurers are improving the customer experience through customization, tailored solutions, and ease of use, all

of which require deeper and broader access to customer data. While some customers are reluctant to share personal information, they are more likely to do so when there is a clear gain for them: *"If it's a benefit to them, they are prepared to let you make money off of it too,"* said one director.

- **Targeting products to existing customers.** Insurers are also using information collected to sell additional products and services to existing customers. One director described a specific potential opportunity related to data on customers' buying habits: *"We have a number of different sales channels, and it would be great to have data from all sales channels in one bucket."* For example, the director continued, *"If someone buys a cancer policy, what other things might be useful to that person? What is something we've seen historically in our product group that would help them? Big data would give us information to do that."*

- **More precise risk identification.** New technologies can permit better management of risks through superior data analysis. One IGLN participant said that while improving the customer experience is the most immediate application for data analytics, *"the 10-year quest for us is how to use data to manage and predict future risk outcomes."* One director described a recent development: *"We realized that the incidence and severity of car accidents had increased due to an upsurge in distracted driving."* The director said that this risk needed to be segmented *"in a new and different way, as opposed to just younger drivers versus older drivers. A lot of that distracted driving is around phones and people using GPS for directions and looking down, so we are putting cameras in cars to pick up on that."*

*"The 10-year quest for us is how to use data to manage and predict future risk outcomes."*

—Participant

- **Broadening coverage.** Better data has the potential to widen the scope of coverage by generating more nuanced understanding of risk pools. One participant said, *"We may be able to have better data around health issues—how diabetics live and manage diabetes, for example—and that additional information may allow us to provide coverage to certain diabetics, where now we are not providing coverage to any. There are societal goods that can come from this if people are willing to share their data."*

- **New types of coverage.** More data can make possible the development of new product lines for specific types of consumers. For example, by drawing on telematics devices in cars, insurers can offer usage-based policies. One participant noted, *"One thing that's coming is per-kilometer charging. That's great for me, but not so good for the insurance*

*companies. I don't drive a lot, I live in the city, I'm absolutely that customer. These technologies are going to change everything."*

## Significant challenges impede insurers' efforts to get maximum value from their data assets

While the opportunities afforded by the proliferation of data are clear, insurers face a number of impediments in realizing the value of their data, including heightened scrutiny from policymakers, regulators, and consumers. Some customers are reluctant to trust insurers with their information, and evolving privacy regulations and norms impose constraints on data use. In addition to these external constraints, insurers often lack the organizational and technical capacity to extract maximum value from the data at their disposal.

### Data privacy regulations

Insurance regulators regard consumer protection as a critical part of their responsibilities, and privacy as an essential component of consumer protection. One regulator said that privacy *"remains firmly on our agenda because data is at the heart of organizations, and its protection is vital to our agenda and our supervisory role. While the new GDPR [General Data Protection Regulation] regime heightens sensitivity due to the fines and things, privacy is and always has been central to our regulatory agenda."* Recently, concerns over privacy, as well as data security, have led to new laws and regulations proposed or in force in a number of jurisdictions.

#### GDPR

In May 2018, the GDPR came into effect across the European Union. This regulation, which an IGLN participant called *"one of the furthest-reaching pieces of EU legislation ever,"* codifies and enshrines new consumer rights and organizational responsibilities and is focusing boardroom attention on compliance and readiness. While the GDPR applies only to firms that collect personal data on EU residents, it may represent the leading edge of privacy regulation globally. A recent analysis noted that with the GDPR, "the European Union has become the focal point of the global dialogue on individual data privacy."[3] In addition, a number of jurisdictions, including Canada, Israel, Japan, and the state of California, have aligned their privacy laws with the GDPR. Observers expect that others will follow suit.

One IGLN participant suggested that just as a number of Asia-Pacific firms adopted capital requirements that were first imposed in the EU, they will soon follow the EU's lead on privacy regulation. Advocates and critics of the GDPR

agree that the privacy and data protection principles from which it is derived enjoy broad social acceptance.

## US privacy regulations

In the United States, insurers face privacy regulations at both the federal and state levels. The Federal Trade Commission has responsibility for enforcing fair-trade practices in the area of privacy and data use, and there are different federal laws and regulations governing the use of specific types of data. In financial services, the Financial Services Modernization Act (the 1999 Gramm-Leach-Bliley Act) regulates the collection and use of financial information and limits its disclosure, in some cases requiring institutions to disclose their privacy practices and allow consumers to opt out of sharing information.[4] In addition, 48 of the 50 states have passed data-breach notification laws, and the Securities and Exchange Commission has recently issued new cybersecurity guidelines that include guidance on disclosures in the event of a data breach.[5]

In 2017, the New York State Department of Financial Services issued data security regulations that include provisions similar to those found in the GDPR.[6] The regulations include a requirement that entities maintain a cybersecurity policy approved by the board or a senior officer, based on the entity's risk assessment. Covered entities must appoint a chief information security officer or the equivalent to perform periodic penetration and vulnerability testing and to establish limits to access and data retention; they must also have a written incidence response plan and notify the Department of Financial Services within 72 hours of a cyber breach.[7] In late 2017, the National Association of Insurance Commissioners adopted a model data security law that largely followed the New York regulations, and in early 2018, South Carolina became the first state to adopt the model law.[8]

In June 2018, California passed the California Consumer Privacy Act (CCPA), which, while not as expansive as the GDPR, contains similar provisions. The law, which will go into effect in January 2020, gives consumers the right to be informed about what information has been collected, rights to data access and portability, and the right to have their personal information deleted.[9] The law also expands the definition of personal information to include biometric data, location, and browsing history.[10]

At the 2017 Financial Services Leadership Summit, one network participant observed that the United States *"does not have a coherent view on data and privacy."*[11] However, recent months have seen significant momentum behind federal privacy regulation in the United States. In September 2018, the US

Chamber of Commerce released privacy principles that called for Congress to "adopt a federal privacy framework that preempts state law on matters concerning data privacy in order to provide certainty and consistency to consumers and businesses alike."[12]

In December, the Business Roundtable released a framework for a national consumer-privacy law and urged lawmakers to pass privacy legislation in 2019. Announcing the framework, Business Roundtable CEO Joshua Bolton said, "The lack of a uniform national privacy law that applies to all sectors undermines consumer trust in all industries. The time is now to enact federal consumer privacy legislation."[13]

*"Companies are trying to solve for privacy issues, with a recent focus on GDPR and how to operationalize the 384 requirements from that regulation."*

—Participant

In addition, large technology firms in the United States, even those that opposed privacy laws in the past, have been lobbying for federal privacy legislation.[14] By the end of 2018, a number of high-profile technology CEOs—including Tim Cook of Apple, Satya Nadella of Microsoft, and Marc Benioff of Salesforce.com—had publicly called for federal privacy regulation modeled on the GDPR.[15]

In November, US Senator Ron Wyden introduced draft privacy legislation that would create a centralized "do not track" list, allowing consumers to prevent companies from sharing their data with third parties or using it in targeted advertising. It would permit companies to offer paid versions of their services that do not rely on user data to generate revenue. Covered companies would have to submit annual data protection reports. Executives would face criminal penalties of up to $5 million in fines and 20 years in prison for intentionally misleading regulators.[16] Whether this specific proposal actually becomes law or not, some policy observers expect federal privacy legislation to pass in 2019.

Privacy regulations constrain organizations' ability to use data by limiting what they can collect, how they can use it, how long they can retain it, and the like. In addition, complying with new regulations requires significant investments of money and time that limit firms' abilities to address strategic questions. One participant noted, *"Companies are trying to solve for privacy issues, with a recent focus on GDPR and how to operationalize the 384 requirements from that regulation."* The participant further pointed out that companies have *"invested $3 million on average globally in response to GDPR, in creating programs [to comply with the regulation]."*

## Maintaining consumer trust

Recent data breaches and scandals about the misuse of data have further eroded consumers' trust in how companies protect their data. A poll

conducted in April 2018 found that only 20% of US consumers fully trust large companies to protect their information, while 73% believe that companies put profit ahead of their responsibility to protect consumers' information. The consequences of this lack of trust are significant.[17] The same poll found that 78% of consumers believe that the ability to protect consumer information is "extremely important," while 75% said that they would not buy a product from a company that they did not trust to protect their information, no matter how much they wanted the product.[18]

*"Trust enables consent. Especially if we think about edgier uses of data, we need to think about trust."*

—Participant

Insurance leaders recognize that they need to win and maintain their customers' trust. One participant said, *"Trust enables consent. Especially if we think about edgier uses of data, we need to think about trust."* Another participant insisted, *"Trust is becoming part of the customer strategy, not just a brand attribute. It* is *the strategy. You need to start by managing the customer experience of privacy."*

To maintain trust, insurers are communicating more clearly to customers what data a firm collects and how it uses that data. One director said, *"Customers want transparency about what data you are collecting and how you are using it."* Another participant advocated a *"shared gains model,"* citing the example of an insurer that *"wanted to use personal information to enhance the product for the consumer. They were successful for the most part because they told the story; they shared how they were going to use it and described the shared gain."*

Research and business experience show that privacy is a deeply personal concept that is significantly dependent on context. As one participant said, the definition of privacy has to *"start with the individual—it's about the individual's sense of what is theirs and what they are comfortable with. These are emotional and subjective and individual issues, so it is extremely challenging to regulate, responding to individual perception and emotions."*

Regulation, by contrast, often treats privacy as a cognitive issue, regarding consumers as rational actors deciding when and how to barter access to their information. GDPR, CCPA, and other legislation are based on assumptions about consumers' attitudes that may not be grounded in actual consumers' preferences. One participant said, *"We have no good data on this, about what people really want; they don't even know what they want."*

## Navigating evolving norms

There is an inherent tension between maximizing the insights and opportunities that can be generated from personal data and protecting individual privacy. As one participant said, policymakers and privacy

advocates *"think in terms of collecting the minimum necessary data, keeping it only as long as necessary, and using it only for the purposes for which it was collected. That is sacrilege for data scientists, who are looking for surprising correlations, so they want as much data as possible, want to keep it forever, and want to combine data sets to find interesting correlations and insights."*

These tensions mean that businesses must make trade-offs and recognize that data can be a liability as well as an asset, given the costs of protecting data and the legal, reputational, and financial risks associated with failing to protect it. *"From a business perspective,"* one participant said, *"this is about constraint, compliance, risk management, and operational processes. This slows things down. It is not supportive of innovative, data-driven businesses. The task of the business is to achieve growth despite constraint."*

*"It's not sexy—the shiny penny is artificial intelligence, but AI is being held back by the need to modernize data management processes and practices."*

—Participant

Leaders need *"to make hard-nosed business decisions about the risk versus the benefit"* of retaining data. One executive said, *"We have an expunging program where we look at data as a potential liability, and data scientists are part of making decisions about the data we retain."* Some organizations take a different tack: *"We're in the opposite category, on the path of never getting rid of data,"* said one director. *"Maybe there will be new services for which 50 years of historical clinical data is key to retain. Why delete it if there is a huge opportunity cost for deleting, if you can keep it legally?"* In some cases, insurers have no choice but to retain data, as one participant noted: *"In life insurance, we have hundred-year retention policies for customer information."*

## Building the right systems and processes

Insurers are creating systems, processes, and procedures to derive meaningful insights from their data. In practice, this is not easy. Many organizations, although they recognize that data is an extremely valuable asset, struggle to capitalize on it because they lack the necessary infrastructure and internal capabilities. One participant said, *"The critical challenge for us is operational effectiveness and the modernization of data management and governance practices and processes. Right now, they are not fit for purpose for modern data science and use of data, and not being managed in a way that prompts speed to market."* One executive said, *"It is a challenge just to get the data in legacy systems into a form that allows you to begin to use it."*

Inadequate systems and procedures for data can be more challenging than regulation or consumer mistrust. One participant noted that while organizations often start by asking whether regulation would allow them to

use data in a certain way, many also need to first ask, *"Does our data infrastructure allow us to do that?"* The participant continued, *"We might have data we don't even know we have, or we don't know its value and integrity. It is housed in different systems and not integrated into a single system."*

Organizations need to master these data management or data engineering tasks before they can capitalize on emerging technologies. One participant said, *"Data is the raw material and it is not being managed in a way that prompts speed to market. It's not sexy—the shiny penny is artificial intelligence, but AI is being held back by the need to modernize data management processes and practices."* Another participant agreed: *"A poorly engineered data storage and management system makes it almost impossible for data scientists to do their job. Even with an excellent and adaptive engineering system in place, there's still a huge amount of cleaning and wrangling and other non-sexy work to do before you get to experiment and find interesting insights."*

*"We need somebody who is not only playing oversight and traffic cop with implementation of data management processes, but also leading on how we start to work through strategic applications across the enterprise … "*

—Participant

## Senior leaders are tackling the challenges of privacy and data governance

A growing number of boards are paying closer attention to privacy and data governance, and companies are developing more robust organizational structures and reporting procedures around privacy. In addition, insurers are increasingly integrating privacy considerations into business decisions and product design.

### Developing more mature organizational structures

Organizations have often lacked clear executive ownership for privacy, but organizational structures and roles are now evolving to better manage issues related to privacy and data governance. Insurers are increasingly assigning privacy and data governance to a single executive owner with significant clout, and some are developing more cross-functional collaboration to manage issues of privacy and data governance. One participant reported that at one insurer, oversight of privacy and data *"is between legal and compliance and the chief data officer,"* while at other organizations responsibility lies with the chief marketing officer.

One participant described creating a dedicated legal team devoted to issues of privacy and data protection, noting that *"having a dedicated team helps you address these issues but also convinces regulators that you are taking it seriously."* Another participant said, *"We need somebody who is not only playing oversight and traffic cop with implementation of data management*

*processes, but also leading on how we start to work through strategic applications across the enterprise, in partnership with law, ethics, risk, and so forth. We need somebody to put their hands on the wheel."*

Participants described the challenge of transforming a compliance-oriented approach into one where privacy informs decision-making throughout the organization. Even with a dedicated executive owner, an emphasis on privacy and data protection must be infused across the organization by developing what one participant called *"privacy culture"* or *"information culture."* Another participant said, *"When we ask the question, 'Can we use this data or not?' the decision belongs to the chief privacy officer, but at end of the day, first-line leadership has to take ownership of the issues as well."*

## Making privacy a board-level issue

The maturity of the board's role in privacy and data varies considerably from company to company. At one director's company, while privacy and data management issues are increasingly coming to the board, *"it's very ad hoc—we have no good documented processes as to how to deal with the issues—but awareness is there in a major way."* One executive said, *"As we think about privacy as a constraint, it is not well explored at board level. Oversight exists today at the company through the enterprise risk management dashboard, and there is the recognition that GDPR is something we need to keep an eye on, but we don't understand it well enough to do something concrete in business practices."*

*"Privacy has gone from being a bullet on the enterprise risk dashboard to a headline program."*

—Participant

Nonetheless, privacy is moving up the risk agenda and commanding more board attention. Privacy leaders and executives are increasingly reporting to the board. Although privacy risks are sometimes regarded as an element of cybersecurity, one participant said, *"Privacy has gone from being a bullet on the enterprise risk dashboard to a headline program."* Another agreed: *"We are treating privacy as more of a stand-alone issue that gets reported to the board—how we go to market and make communication adjustments to customers. We are not there yet, but it's not optional. We are in the first generation of thinking through it."* Another executive noted a progression in the board's interest in privacy over the last two years: *"They wanted to know about GDPR because of the materiality of potential fines. Then the board wanted to be updated on what we are doing about it, the status of the compliance program. Now the board is hungry for information about privacy."*

## Building privacy into business decisions

Organizations are increasingly building privacy into their strategic decisions and product design, a process that can be enabled by organizational changes and building a culture of information security.

One executive noted that until recently, *"almost all of privacy knowledge and compliance with the Department of Financial Services was being run by an attorney with no connections to the business."* More recently, the organization has been trying to push decision-making around privacy throughout the whole organization, rather than isolating it in the compliance function. Another participant said, *"The whole business needs to understand what CCPA is about. There are all sorts of business decisions that need to be made, so understanding of privacy has to exist throughout the management of the company. There are significant business choices that need to be made."*

*"The board wants to know, 'How does that stack up with privacy?'"*

—Director

Restrictions on the use of collected data need to be recognized early in product and business planning, and the implications of privacy concerns need to be made explicit. One participant noted, *"Boards may not be fully aware of the constraints on data, so calculated returns on investment for projects are likely to be off."* Another participant said, *"We have a process where if you launch a product, privacy is at the table. We are not evaluating their returns on investment without understanding what data we can and can't use, and we are not launching new products with data elements that are not consistent with our privacy policy."* More generally, senior leaders are asking for privacy impact assessments. One director said that with respect to new products, *"the board wants to know, 'How does that stack up with privacy?'"*

***

Insurers now understand more of the opportunities and challenges around the collection and use of data and the tensions between the strategic use of data and the need to protect users' information, respect their privacy, and gain their trust. In the words of one participant, senior leaders should *"start to focus their questions on information culture and what we are doing to ensure innovation around information. That can lead to a robust and informed conversation about whether you are maximizing or wasting your most important asset."*

## Policy update

In a briefing session, participants discussed the current legislative and policy landscape in Washington, DC. The 2018 mid-term elections gave back control of the House to the Democratic Party and thereby changed the political calculus in Washington. With likely a one-year window in which to pass meaningful legislation before the 2020 election cycle drowns out other priorities, IGLN participants discussed two areas of potential movement.

First, the recently agreed US-Mexico-Canada Agreement (USMCA)—signed in early December by President Trump and his counterparts in Canada and Mexico—needs to be enacted in legislation. Although the incoming chair of the relevant House committee supports the agreement, Democrats will likely seek to modify labor and environmental aspects of the deal and to extract concessions on other priorities, including infrastructure funding and changes to tax reform.

Secondly, there is a great deal of momentum to pass federal privacy legislation, in part because the business community, alarmed by the GDPR and CCPA, is pushing hard for a federal privacy framework to pre-empt potentially disjointed state regulations. In exchange for pre-emption, Democrats from states with stronger privacy regulations, such as California and New York, are expected to push to expand the authority and funding of the Federal Trade Commission to regulate privacy and to allow state attorneys general to enforce any new federal privacy framework. Participants raised concerns that legislators might not have a sufficient grasp of the technical aspects of privacy issues to craft meaningful and effective legislation.

## Appendix: Discussion participants

On December 5 in New York, Tapestry and EY hosted an IGLN meeting on owning, using, and protecting data. In the meeting and in preparation for it, we conducted numerous conversations with directors, executives, regulators, supervisors, and other thought leaders. Insights from these discussions inform this *ViewPoints* and quotes from these discussions appear throughout.

The following individuals participated in these IGLN discussions:

### IGLN Participants

- Bill Anderson, Chair, Sun Life
- Doug Caldwell, Chief Risk Officer, Transamerica
- Jan Carendi, Senior Advisor, Solera Holdings
- Lucy Fato, Executive Vice President and General Counsel, AIG
- Andres Franzetti, Chief Strategy Officer, Risk Cooperative
- Doug Johnson, Audit Committee Chair, Aflac
- Sara Lewis, Audit Committee Chair, Sun Life
- Karole Lloyd, Non-Executive Director, Aflac
- Eileen Mercier, Audit Committee Chair, Intact Financial
- Kjersten Moody, Vice President and Chief Data & Analytics Officer, State Farm
- Wayne Peacock, President, Property and Casualty Insurance Group, USAA
- Nancy Quan, Non-Executive Director, Liberty Mutual
- Bill Reed, Risk Committee Chair, USAA
- Bob Stein, Audit Committee Chair, Assurant, Inc.
- Steve Weber, Professor, School of Information, Department of Political Science, UC Berkeley, and Faculty Director, Berkeley Center for Long Term Cybersecurity

| | |
|---|---|
| EY | • Emily Coyle, Director, Office of Public Policy<br>• Dave Hollander, Global Insurance Leader<br>• Craig Rainer, Senior Manager<br>• Angela Saverice-Rohan, America's Leader for Privacy |
| Tapestry Networks | • Eric Baldwin, Senior Associate<br>• Jonathan Day, Vice Chair and Chief Executive<br>• Simon Wong, Partner |

## About *ViewPoints*

*ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

*ViewPoints* is produced by Tapestry Networks and aims to capture the essence of the IGLN discussion and associated research. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of senior management, advisers, and stakeholders who become engaged in this leading-edge dialogue, the more value will be created for all.

## About the Insurance Governance Leadership Network (IGLN)

The IGLN addresses key issues facing complex global insurers. Its primary focus is the non-executive director, but it also engages members of senior management, policymakers, supervisors, and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring, and trustworthy insurance institutions. The IGLN is organized and led by Tapestry Networks, with the support of EY.

## About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multistakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

## About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the insurance industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients, and for its communities. EY supports the IGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

## Endnotes

[1]Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018.

[2] Nic Gordon and Ofir Eyal, "Think Tank: Big Data, Big Impact," *Asia Insurance Review,* July 2016.

[3] Nuala O'Connor, "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, January 30, 2018.

[4] Ieuan Jolly, "Data Protection in the United States: Overview," ThomsonReuters Practical Law, October 1, 2018.

[5] US Securities and Exchange Commission, "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures," news release, February 21, 2018.

[6] Keith Button, "New Financial Services Cyber Laws Lay Responsibility on Boards," *Agenda,* August 7, 2017.

[7] Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2017).

[8] Don Jergler, "The State of NAIC's Data Security Model Law," *Insurance Journal*, September 21, 2018.

[9] Daisuke Wakabayashi, "California Passes Sweeping Law to Protect Online Privacy," *New York Times,* June 28, 2018.

[10] Dipayan Ghosh, "What You Need to Know about California's New Data Privacy Law," *Harvard Business Review,* July 11, 2018.

[11] Financial Services Leadership Summit, *Data Governance: Securing the Future of Financial Services,* ViewPoints (Waltham, MA, and London: Tapestry Networks and EY, 2018), 6.

[12] US Chamber of Commerce, "U.S. Chamber Releases Privacy Principles," news release, September 6, 2018.

[13] "Business Roundtable Releases Framework for National Consumer Privacy Law," Business Roundtable, December 6, 2018.

[14] Cecilia Kang, "Tech Industry Pursues a Federal Privacy Law, on Its Own Terms," *New York Times,* August 26, 2018.

[15] Daniel Michaels, "IBM CEO Ginni Rometty Criticizes Big Internet Platforms for Mishandling Customers' Data," *Wall Street Journal,* November 26, 2018; Todd Shields and Caroline Hyde, "Microsoft CEO Backs Federal Privacy Law over State Efforts," *Bloomberg,* October 10, 2018.

[16] David McCabe, "Democrat's Draft Privacy Bill Includes Prison Time for Execs," *Axios,* November 1, 2018; Jordan Valinsky, "Senator Wants to Punish Tech CEOs with Jail Time When Companies Violate Privacy," *CNN Business,* November 1, 2018.

[17] Mark Huffman, "Survey Finds Increasing Level of Consumer Concern about Privacy Protection," *Consumer Affairs*, April 17, 2018.

[18] Huffman, "Survey Finds Increasing Level of Consumer Concern about Privacy Protection."