PRIVACY: BEYOND COMPLIANCE

ISACA

CONTENTS

ABSTRACT

This white paper examines today's privacy context and the way boards of directors oversee compliance with privacy regulations. It explores the human impact of privacy, highlighting that data are not merely an asset to be exploited, but rather a reflection of real human lives, and that personal data should be treated with dignity and respect. The paper provides direction to boards of directors and privacy practitioners on privacy issues they should consider, and it suggests best practices. It shows the imperative of moving from individual data self-determination to organizational information accountability, and it helps readers rethink their perspectives on privacy. Finally, it details the implications of these human-impact findings for a future of privacy beyond compliance.

Introduction

Think about all the data users give to Google®, Facebook®, Apple®, Twitter®, Amazon® and Microsoft®. Given that so much data are already being collected about consumers' daily lives—from data users voluntarily provide via apps and organizations to data obtained through surveillance, all too often without even knowing it—should users be looking for different ways of thinking about privacy?

Over a period of 3,000 years, cultures have tended to prioritize convenience and wealth over privacy.[1] Indeed, it has even been suggested that privacy is an anomaly,[2] suggesting that the dissemination of private information may be more pervasive than generally acknowledged. However, privacy has been pushed into the spotlight over the last 40 years, thanks to the mainstream adoption of the Internet and the establishment of organizations like Privacy International.[3] Privacy—the quality or state of being apart from company or observation or freedom from unauthorized intrusion[4]—is sometimes articulated as a desire to be left alone, or even as a basic human right. The word, "secret" has even been used to describe privacy. ISACA defines privacy as:

Rights of an individual to trust that others will appropriately and respectfully collect, use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived. What is appropriate depends on the associated circumstances, laws and the individual's reasonable expectations. An individual also has the right to reasonably control and be aware of the collection, use and disclosure of his/her associated personal and sensitive information.[5]

This paper takes readers on a journey through today's privacy landscape, including the way boards oversee compliance with privacy regulations. It explores the human impact of privacy, highlighting the principle that data are not merely assets to be exploited, but rather a reflection of real human lives, and that they should be treated with dignity and respect. It details the implications of these human-impact findings for a future of privacy beyond compliance.

Back to the 1990s: Privacy by Design

From the depths of the 1990s emerged a paradigm that began to change how the world thought about privacy. The timing of this paradigm shift was fitting, given that it coincided with awareness of the growing volume of public-surveillance activities enabled by the increased presence of closed-circuit TV (CCTV), which in turn gave rise to organizations concerned about this aspect of human-rights violations, like Privacy International.

Almost 30 years later, a similar concept—privacy as a human right—was embedded in the General Data Protection Regulation (GDPR), as is the term "privacy by design," the groundbreaking global paradigm introduced by Ann Cavoukian, Ph.D., the three-time former Information and Privacy Commissioner of Ontario, Canada.[6] The paradigm was groundbreaking because it moved away from the premise that the only responsibility of organizations was to comply with privacy regulations. Instead, it held that enterprises should operate from the premises of privacy by design and privacy by default.

Privacy by design requires that the actions an enterprise performs with respect to personal data be conducted in the context of data protection and privacy rights from the outset of an initiative, or simply put, that privacy is

[1] Ferenstein, G.; "The Birth and Death of Privacy: 3,000 Years of History Told Through 46 Images," The Ferenstein Wire, 24 November 2015, https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e

[2] *Ibid.*

[3] Privacy International, https://privacyinternational.org/

[4] Merriam-Webster, "privacy," www.merriam-webster.com/dictionary/privacy

[5] ISACA, *ISACA Privacy Principles and Program Management Guide*, USA, 2017

[6] Ryerson University, "Privacy by Design Centre of Excellence," https://www.ryerson.ca/pbdce/about/ann-cavoukian/

integrated into the entire engineering process. **Privacy by default** requires that enterprise leadership set a standard for protecting data that goes beyond mere compliance requirements. Enterprises that strive for personal data security by design, and enable privacy by default, create a solid basis for their customers/clients and stakeholders to trust that their personal data are in good hands and protected, a rewarding outcome for the organization.

Current-State Overview: It Is All About Compliance

In a corporate governance context, the focus of privacy is typically compliance as a minimum requirement for organizations to be on the right side of the law. The problem is that even this bar might be too high for some enterprises, which instead choose to pay the financial penalties imposed—penalties that may be a mere fraction of the cost of achieving privacy compliance (ignoring the financial impact of the realization of reputation risk).

On compliance, note that only about half of the countries of the world have some type of data protection laws.[7] These include the Personal Information Protection and Electronic Documents Act in Canada, the California Consumer Privacy Act in the US state of California, the Protection of Personal Information Act in South Africa, the Data Protection Act 2018 in the United Kingdom, the General Data Protection Regulation in Europe, the Lei Geral de Proteção de Dados in Brazil, the Personal Data Protection Bill in India and the Privacy Act in Australia. However, it is important to note that just because a country has a privacy law, it does not mean that the protection it offers individuals is adequate or comprehensive, or even comparable across countries.

One reason for the lack of worldwide comparability is that some privacy laws are outdated, with some origins predating social media platforms like Facebook and Twitter. Another reason is a difference in paradigm; in Europe, for example, the basis for privacy law is privacy as a basic human right, but not every country or culture has the same viewpoint. **Figure 1** shows the wide range of privacy regulations around the world with respect to their scope.

FIGURE 1: Scope of Privacy Regulations—A Global Sample

Region or Country	Scope of Regulations
European Union	GDPR applies to all 27 EU member states.
United States	Privacy requirements vary based on economic sector and state.
Canada	Privacy requirements vary based on province and territory.
Senegal	Privacy law focuses on data collection as it applies to being shared with third parties.

Beyond differences across geographic regions, there are often differences in the application of privacy laws to the public versus the private sector.

Despite the proliferation of privacy regulations, many consumers are still not comfortable with how their personal data are used. For example:

- 98 percent of respondents to a US survey felt they should have more control over the sharing of their personal data, and 79 percent of respondents in India did not feel comfortable with the sale of their data to third parties.[8]
- According to the Pew Research Center, 79 percent of Americans were not confident that companies would publicly admit to

[7] Komnenic, M.; "Privacy Laws Around the World," Termly, 14 March 2019, https://termly.io/resources/infographics/privacy-laws-around-the-world/

[8] Madhukar, C.V.; "How Privacy Tech Is Redefining the Data Economy," *The European Sting*, 17 September 2019, https://europeansting.com/2019/09/17/how-privacy-tech-is-redefining-the-data-economy/

misusing customer data,[9] and 74 percent of people from around the world expressed concern about the treatment of their data.[10]

This suggests that privacy laws are not strong enough in the eyes of the citizens they are meant to protect. Alternatively, this could suggest that enforcement is not strong enough, penalties are not strong enough or the public is misinformed.

Enterprise boards have a fiduciary duty to ensure compliance with the privacy laws applicable to the jurisdiction the enterprise operates in, whether those laws are effective or not.

Input from the CRO and from audit reports can be integrated within the board audit/audit and risk committee before reporting back to the main board of directors. In boards of directors that have separated audit and risk committees, some level of coordination may be required to develop a single view of the state of privacy compliance within the enterprise.

Corporate Governance

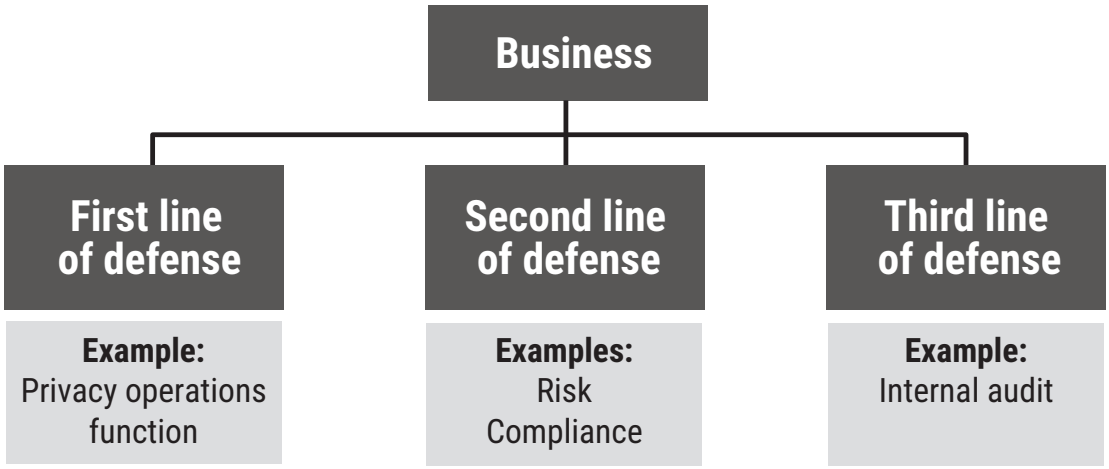
Privacy (and information security) follow the three lines of defense model (**figure 2**):

1. Operational functions
2. Oversight functions
3. Audit

The board of directors is specifically involved in aspects of lines two and three, determining the level of privacy compliance with the support of reports from the chief risk officer (CRO), for example, and from (independent) audit reports.

However, some elements of privacy might not come up in quarterly board meetings—e.g., privacy in the context of third-party vendors and privacy in the cloud—especially in the case of small or medium-sized businesses that leverage free cloud services. In these contexts, boards could mandate enterprisewide pseudonymization, anonymization and/or data minimization initiatives to ensure greater control and monitoring of the privacy landscape.

FIGURE 2: Three Lines of Defense



[9] Auxier, B.; L. Rainie; M. Anderson; A. Perrin; M. Kumar; E. Turner; "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, 15 November 2019, www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[10] *Op cit* Komnenic

Privacy Ethics

There is an ethical dimension to individual or departmental conduct with respect to the processing and use of data in the enterprise, but the topic may not make it to the boardroom in jurisdictions where the law is silent on the matter. In such cases, while the decisions made with respect to data may not be illegal, a key question remains: To what extent do those decisions serve the best interests of humankind?

In matters where the law is silent, boards of directors must evaluate whether privacy-related decisions are ethical. Once the question moves to ethics, things may get more complex for the board, starting with the need to select a framework for the evaluation of ethics in managerial decision making. For example, a small study[11] in Malaysia highlighted three perspectives of ethics in corporate governance:

- Corporate governance as a code of ethics
- Ethics as an implicit part of the corporate governance mechanism
- Ethics as an affiliate of corporate governance

While there may be more models, more important is that board ethics committees consistently apply and enforce a model that works for them. Without effective enforcement, ethics committees are barely paper tigers.

Furthermore, while one does not often see ethical behavior listed among the criteria required for an aspiring member of the board of directors—although integrity comes up often—there can be a conflict between the general expectations of directors and officers versus those of individual customers. In Canada, for example, the requirement is that directors and officers act in the best interests of the corporation.[12] However, the best interests of the corporation might be to monetize data as much as possible within the ambit of the law, and with no regard for the broader privacy interests of the individuals represented by the data. While these actions may not be illegal, the question is whether the actions are ethical and in the best interests of individual privacy.

There is a gap in privacy oversight if one considers only the compliance dimension of privacy and deprioritizes ethics and the best interests of data subjects.

The Human Element of Privacy

While there is no stopping the evolution of technology and the impact it has on privacy, the human component of the privacy conversation is not considered often enough. For example, while privacy became a fundamental human right in 1948 through article 12 of the Universal Declaration of Human Rights, different cultures perceive privacy in different ways. For example, within the region of Scandinavia, more Norwegians (84 percent) considered technology's impact on privacy to be positive than did their counterparts in Denmark (77 percent) or Sweden (69 percent).[13]

[11] Othman, Z.; F. Mohd-Shamsudin; "Role of Ethics in Corporate Governance," ResearchGate, September 2012, www.researchgate.net/publication/259827655_Role_of_Ethics_in_Corporate_Governance
[12] Government of Canada, "Directors and Officers," www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs06643.html
[13] Statista, "Technology's Impact on Privacy in the Scandinavian Countries in 2019," 21 November 2019, www.statista.com/statistics/1073777/technology-s-impact-on-privacy-in-scandinavia/

It is important to consider certain human elements of privacy—understanding that some findings may be regional and cannot be generalized, and that many aspects may not reach the agendas of generally compliance-oriented boards of directors.

Privacy Infringements Abound

Mobile phones and laptops are equipped with microphones and cameras, and most mobile phones have GPS capabilities that track users' movements. "Listening" and "seeing" devices from Google and Apple increasingly are welcomed into users' lives despite their documented privacy defects.

Facial recognition and fingerprint logins have become more commonplace. Smart devices like refrigerators and microwaves populate many kitchens. Most people load all manner of apps onto their phones, with little more than the briefest of pauses before pressing "I Accept" at the various privacy prompts. Parents post photos of their kids all over social media, without regard for their consent, which they are too young to give anyway.

Then there are those free (or very low cost) cloud storage solutions. Remember, if it is free, then the user is the product, in the form of personal data. Further, cookies—i.e., little bites of data stored on computers to track where on the Internet individuals have been—can be accessed by other websites for marketing or sometimes darker purposes. Though users may consent to the terms and services of solutions, service providers must ensure that they collect only the minimal amount of data, and use them ethically.

Individuals may choose to give away their data in return for certain benefits. In this context, consider the following: A privacy study involving 16,000 respondents worldwide in October 2018 examined how many of the respondents were concerned about online privacy versus how many were willing to accept online privacy risk in exchange for convenience (**figure 3**). The Netherlands had the lowest difference between the two scores while Brazil had the largest difference.[14] These findings reinforce perceptions of cultural difference with respect to privacy.

FIGURE 3: Sample Online Privacy vs. Convenience

Country	Online Privacy Concern	Willing to Accept Privacy Risk for Convenience
Netherlands	66%	63%
New Zealand	80%	75%
Brazil	89%	49%
Hong Kong	87%	51%

Thus, it appears that most people are comfortable giving up some privacy for convenience in spite of the risk. For example:

- AT&T® rolled out a US$30 service for users who did not want the privacy invasion of ad tracking, but an overwhelming number of users instead chose the ad model.[15]
- People at an art performance quite happily shared their US Social Security numbers, image or fingerprints in return for nothing more than a cinnamon cookie.[16]

In reality, absolute privacy requires absolute isolation. Those who want the benefits of a community and the services it offers will have to pay some kind of privacy-associated cost. As participants in this trade-off,

[14] Statista, "Share of Internet Users Who Are Concerned About Risks to Their Online Privacy vs. Their Willingness to Accept Certain Risks to Their Online Privacy to Make Their Life More Convenient as of October 2018, by Country," March 2020, www.statista.com/statistics/1023952/global-opinion-concern-internet-privacy-risk-convenience/

[15] *Op cit* Ferenstein

[16] *Ibid.*

enterprises must be careful to gather only the personally identifiable information (PII) that is absolutely necessary.

The Human Impact of a Data Breach

For perspective on the scale of data breaches in the United States—the country at the highest risk of data breaches[17]—the largest single data breach involved Yahoo® with the exposure of 3 billion accounts,[18] a number that's roughly equivalent to the total number of economically active people on Earth. Next in terms of scale was the Indian government's national-identity database breach, which exposed the personal data of more than 1.5 billion Indian citizens.[19]

For those aware that they have been impacted by a data breach (many will never know that their data have been exposed), the consequences could be limited to mere inconvenience—e.g., changing a password or canceling a credit card. However, consequences may also be more severe, as was the case in India, where access to food, health and human services was disrupted for a large portion of the population. Many banks routinely retrieve full and partial credit card numbers from the dark web as part of their credit card fraud analysis. Enterprises must consider the negative financial impact to the individual as a result of breaches, because it might take a financial institution months to provide restitution in some cases, as when card credentials are stolen.

By far the most sinister impact of a data breach is identity theft. Boards of directors must realize the very real harm that a breach of its enterprise security could cause and act to protect data and minimize potential damage. A nefarious hacker who figures out where a data subject lives, identifies family relationships, and learns the victim's national identity number, email address, telephone number and date of birth, has all that is necessary to impersonate the individual in almost every way. The hacker can apply for loans, buy firearms and commit crimes posing as the data subject.

As if all those consequences were not bad enough, the average time to identify a breach is nearly seven months.[20] So a person could be compromised financially and tarnished reputationally long before the breached enterprise even knows about the incident.

Given the increased number of enterprises capturing personal data, the public must ask what privacy means today. It seems that sensitive data can be breached at any time, even from trusted enterprises. Indeed, "every company we entrust with our data is vulnerable."[21] Privacy by design helps address this situation, rather than relying solely on good post-breach communication and cyberinsurance. Neither of those cures is of much help to the subject of the data breach, whose sensitive data may now be for sale on the dark web, for use by all manner of nefarious groups and individuals.

Given the increased number of enterprises capturing personal data, the public must ask what privacy means today. It seems that sensitive data can be breached at any time, even from trusted enterprises.

Internet Privacy Policies (to Which Users Generally Agree)

Those who take time to read the privacy policies of the websites they visit might notice it can be a bit of a Hobson's choice—i.e., having to accept the policy or forego the service. If visitors want the content and cannot find it anywhere else, but do not necessarily agree with the privacy policy, what should they do? Forego the content or their privacy?

[17] Mangat, M.; "81 Eye-Opening Data Breach Statistics for 2020," phoenixNAP, 27 January 2020, https://phoenixnap.com/blog/data-breach-statistics

[18] Sobers, R.; "107 Must-Know Data Breach Statistics for 2020," Varonis, 29 March 2020, www.varonis.com/blog/data-breach-statistics/

[19] *Op cit* Mangat

[20] *Op cit* Sobers

[21] Schmidt, M.; "What Does the Future of Data Privacy Look Like?," *Forbes*, 13 November 2018, https://www.forbes.com/sites/forbestechcouncil/2018/11/13/what-does-the-future-of-data-privacy-look-like/#703a94e91da7

If users choose to forego privacy, they end up exactly where they were before privacy regulations required a privacy policy—except that instead of being in the dark about what happens to their data, users have an inkling of what happens to it (including potential access of unnamed third parties for commercial purposes).

Future Implications for Privacy

Enterprises have often regarded data as assets—and thus, managed the information accordingly. A decade or two ago, it made sense to speak of data as assets. After all, information was the new gold, and it made business sense to want to mine data to identify opportunities to enhance revenue.

Privacy concepts did not have the legal or social profile they have today, and many enterprises exploited data almost at will. Data-driven cross-selling and upselling became everyday marketing speak, and enterprise income statements grew accordingly. At some point, the conversation turned to behavioral modeling and analytics to predict future sales (among other things), and that is when everything changed[22, 23] —highlighted by the recognition that predictive analytics could make incorrect inferences about people, potentially inflicting harm to the individual.[24]

Data as an Element of Humanity

Recently, as privacy concerns have evolved, so have relevant behavior and actions among boards of directors. For example, their focus shifted from discussing a cold, hard, fungible asset to considering the ways individuals engage the world around them. Suddenly every data point became more than a sales opportunity. Data points came to mirror someone's world, representing the hopes and dreams of individuals, their realities and their pains. No longer alienated, data assumed a human dimension.

Data points came to mirror someone's world, representing the hopes and dreams of individuals, their realities and their pains. No longer alienated, data assumed a human dimension.

Understanding information as a reflection of real persons changes the way enterprises should manage or regard it. Instead of treating it merely as an asset, enterprises must should understand that it represents the details of someone's life or death. As such, data demand much more respect than mere assets to be exploited. Leaving loose reports lying around suddenly becomes much more problematic than keeping an untidy desk—aspects of a person's private life might be exposed for all to see. Similarly, sending personal data by unencrypted email is no longer a minor misdemeanor or policy infringement. Personal data are more than just assets to be exploited; personal information requires respect for the individuals it represents.

COVID-19 Contact-Tracing Apps

Contact tracing is being deployed as a core communicable disease-control tool. It is a means to track

[22] Office of the Privacy Commissioner of Canada, "The Age of Predictive Analytics: From Patterns to Predictions," 2012, www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pa_201208/

[24] Naughton, J.; "Why Big Data Has Made Your Privacy a Thing of the Past," *The Guardian*, 6 October 2013, http://www.theguardian.com/technology/2013/oct/06/big-data-predictive-analytics-privacy

infected persons, notify those exposed and educate them about what they should do.

Heightened interest in applying technology to contact tracing has raised concerns about how it will be deployed in the United States—predominantly by Apple and Google, via iOS® and Android® respectively. The technology may actively collect data on the minutiæ of infected individuals' daily lives. However, will infected parties opting into this collection receive information on whether their data will be used beyond initial medical requirements or how long it will be stored? How will tracking organizations know who is infected, and how will they gain user consent for tracking? How will uninfected users agree to tracking?

These are exactly the kinds of details that Europe's GDPR requires data controllers to specify—e.g., the type of data collected, the purpose of the data collection and how long the data will be stored—noting that contact tracing will require the opt-in of the infected person[25] and of uninfected people as well. In this respect, guidelines for data controllers and contact-tracing tools in the EU have been compiled.[26] Furthermore, there is the tricky possibility that enterprises like Apple and Google become involved in government health surveillance, given that (as publicly traded commercial entities) they already have an operating context for all the other data they collect about individuals.[27]

So while the public might be open to tech-based, contact-tracing solutions at present, some legal experts suggest that sentiment may change as more people become aware of actual (or even perceived) privacy implications of contact-tracing solutions, especially since there are two types of personal data at stake—PII and geolocation data.[28] It may be helpful for enterprises to apply privacy-by-design principles when working with governments on contact-tracing initiatives[29] to help ensure accountability in data protection[30] and to obviate the risk of lawsuits.[31] The data life cycle is also critical. What is secure now may not be secure in a few years—so all collected data must be properly maintained for security purposes.

In a joint statement, Canadian federal, provincial and territorial privacy commissioners announced a set of privacy principles for use as guidelines at any level of government when launching smartphone-based contact-tracing functionality.[32]

On a broader scale, there is concern that snooping technology developed for counterterrorism operations will be turned on citizens as part of government efforts to control the pandemic. Expressed differently, the concern is that the types of surveillance used to combat the pandemic "could permanently open the doors to more invasive forms of snooping later."[33] In South Korea,

[25] Yan, H.; "Contact Tracing 101: How It Works, Who Could Get Hired, and Why It's so Critical in Fighting Coronavirus," CNN Health, 27 April 2020, www.cnn.com/2020/04/27/health/contact-tracing-explainer-coronavirus/index.html

[26] European Data Protection Board, "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak," 21 April 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[27] Lewis, J.A.; "Big Company, Big Government, Big Brother? Privacy After Covid-19," Center for Strategic & International Studies, 17 April 2020, www.csis.org/analysis/big-company-big-government-big-brother-privacy-after-covid-19

[28] See for example, Hildebrand, M.J.; "Privacy Concerns Multiply as Digital Contact Tracing Spreads: U.S. Tech Industry Takes the Lead as Congress Fails to Act," Client Alert, Lowenstein Sandler LLP, 22 June 2020, https://www.lowenstein.com/news-insights/publications/client-alerts/privacy-concerns-multiply-as-digital-contact-tracing-spreads-us-tech-industry-takes-the-lead-as-congress-fails-to-act-privacy.

[29] Carlton, A.; "Even in a Pandemic, Consider Privacy by Design," Towards Data Science, 18 March 2020, https://towardsdatascience.com/even-in-a-pandemic-consider-privacy-by-design-735d68cfa803

[30] Brook, C.; "Adopting Accountability in Data Protection Post COVID-19," Digital Guardian, 15 April 2020, https://digitalguardian.com/blog/adopting-accountability-data-protection-post-covid-19

[31] Hudgins, V.; "Demand for COVID-19 Tracking Places Greater Emphasis on Privacy by Design," Law.com, 14 April 2020, www.law.com/legaltechnews/2020/04/14/demand-for-covid-19-tracking-places-greater-emphasis-on-privacy-by-design/?slreturn=20200408120908

[32] Office of the Privacy Commissioner of Canada, "Supporting Public Health, Building Public Trust: Privacy Principles for Contact Tracing and Similar Apps," 7 May 2020, https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/

[33] Singer, N.; C. Sang-Hun; "As Coronavirus Surveillance Escalates, Personal Privacy Plummets," *The New York Times*, 17 April 2020, www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

distinct privacy issues emerged when infected persons were "hounded" by Internet mobs who deanonymized the location history data of the infected parties, ultimately identifying the infected people by name.[34]

Holding Enterprises Accountable for Temporary Privacy Violations in a Crisis

As previously noted, contact-tracing technology can significantly enhance the ability of communicable-disease authorities to track the spread of diseases and viruses like COVID-19. Consequently, some governments may temporarily limit certain freedoms in an effort to help monitor and control the spread of the virus.[35]

Not only governments need to be held accountable. What about enterprises in general? What about the issues of data fusion and the possibility that personal inferences can be established on the basis of public information? In these contexts, how will boards of directors apply their fiduciary duties—will they choose to pay a noncompliance fine to maximize profits? Or will they choose to preserve the rights of individuals whose PII they may exploit, or at least fail to protect?

A Post-Privacy World?

Is privacy—at least as generally understood today—a lost cause in a digital and interconnected world?[36] Involuntarily provided data held by one source may not provide a completely identifiable record, but when fused with data from another source, the record may be re-identified and become significantly more valuable in the wrong hands.

One proposal for dealing with the current state of privacy concerns is to migrate from a paradigm of individual data self-determination to one of enterprise information accountability.[37] Here the focus shifts to the role of enterprise governance in ensuring privacy, and to the board's fiduciary duty to ensure that enterprises ethically obtain and process the data they use. Privacy practitioners should ensure that enterprises maintain policies to track the sources of data used for key processing activities and that they understand the life cycle of shared PII. Boards of directors should request enterprise reports on the effectiveness of the adoption life cycle approach.

Beyond Compliance

There is a privacy context that goes beyond mere regulatory compliance, extending to issues such as ethics, trust, respect for the human dimension of data and consideration of privacy by design. This privacy context is about more than obeying the law. It is also about giving customers an opportunity to build or rebuild trust in a world where trust is diminishing. The benefits extend not only to enterprises, but to humanity in general. An enterprise can differentiate itself by elevating data standards and becoming a new breed of ethical data manager.

Looking ahead, enterprise sustainability will be built on a culture of trusted partnerships with stakeholder groups that include the customer, whose trust will be gained through greater transparency.[38] It is worth noting that a five-year study tracking the performance of the most trustworthy companies in the United States—measured by financial stability and strength, conservative accounting, corporate integrity, transparency, and sustainability—found a return of

[34] *Ibid.*

[35] G4 Media, "România, Moldova, Letonia și Armenia au Activat Derogarea de la Aplicarea Prevederilor CEDO, Având în Vedere Activarea Stării de Urgență," 19 March 2020, www.g4media.ro/romania-moldova-letonia-si-armenia-au-activat-derogarea-de-la-aplicarea-prevederilor-cedo-avand-in-vedere-activarea-starii-de-urgenta.html

[36] Kraker, P.; "Post Privacy: What Comes After the End of Privacy?" Science and the Web, 25 April 2012, https://science20.wordpress.com/2012/04/25/post-privacy/

[37] *Ibid.*

[38] Nayar, V.; "Profits, Ethics, and Trust," *Harvard Business Review*, 20 January 2009, https://hbr.org/2009/01/no-profits-without-ethics

approximately 83 percent (price growth), compared to the S&P 500® Index that returned comparatively low 42-percent growth over the same period.[39] Incidentally, transparency is an element of privacy by design.

The financial benefits of trust are supported by similar findings from respected institutions such as the American Institute of Individual Investors, the Dutch University of Maastricht, Erasmus University and *Harvard Business Review*. While trusted companies outperform their peers in the long run, only 18 percent of consumers globally trust business leadership (15 percent in the US).[40]

"We are a society in search of trust. The less we find it, the more precious it becomes."[41] Sadly, only a third of American adults trust their government, and this level of trust has been shrinking[42] from a high of about 75 percent in the early 1960s.[43] Are there opportunities to rebuild trust, or are the low levels of citizen-government trust to be accepted as a new normal?

Trust is partially won by fulfilling an enterprise's social responsibility.[44] One of the most pressing questions in all of this: What is an enterprise's role within the communities where it operates? Boards need to evaluate whether an organization's purpose is just to make money, or if it should also benefit the societies and communities where it operates. Does it have a responsibility to help solve some of the world's most pressing problems, like pollution and low wages, which can be a direct result of maximizing profit?

The World Economic Forum® positions the problem of trust as a distinction between short-term profitability and the long-term interests of a broader community of stakeholders, including customers and the surrounding community in which enterprises operate.[45] Even more, it has been suggested that the more high-tech the world becomes, the more high-touch it should be (i.e., providing greater levels of personal attention), and that trust reconciles the power of technology with human beings.[46]

Boards need to evaluate whether an organization's purpose is just to make money, or if it should also benefit the societies and communities where it operates.

For example, a study in India found that ethical enterprises were more profitable than others, given the competitive advantage gained from ethical practices.[47] Furthermore, ethical practices build the kind of consumer support businesses need to be successful, with up to 56 percent of Americans choosing not to buy from brands thought to be unethical.[48] Some enterprises think that acting ethically only adds to the cost of doing business. However, in reality, it adds value not only for customers, but also for the enterprise, in terms of increased profitability and improved performance.[49]

Thus, there is every indication that developing trust and ethical practices does an enterprise good. If customers trust that an enterprise will do the right thing as a steward of the data representing slices of their lives, then in a future world

[39] Kimmel, B.; "Trust: The Direct Route to Profitability," Trust Across America, 2 July 2014, www.trustacrossamerica.com/blog/?p=1322
[40] *Ibid.*
[41] Blasingame, J.; "When Trust Is a Best Practice, Profit Margins Increase," *Forbes*, 10 October 2016, www.forbes.com/sites/jimblasingame/2016/10/10/when-trust-is-a-best-practice-profit-margins-increase/#16bb7a113bbe
[42] Rainie, L.; S. Keeter; A. Perrin; "Trust and Distrust in America," Pew Research Center, 22 July 2019, www.people-press.org/2019/07/22/trust-and-distrust-in-america/
[43] Pew Research Center, "Trust in Government: 1958-2015," 23 November 2015, www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/
[44] Schwab, K.; "The Profitability of Trust," World Economic Forum, 10 December 2014, www.weforum.org/agenda/2014/12/the-profitability-of-trust/
[45] *Ibid.*
[46] *Op cit* Blasingame
[47] Singh, S.; "Ethics and Profitability: Can They Coexist?" Springer, 2008, https://link.springer.com/chapter/10.1057/9780230611016_4#citeas
[48] Washington State University Carson College of Business, "3 Reasons an Ethical Business Leads to Profits," https://onlinemba.wsu.edu/blog/3-reasons-an-ethical-business-leads-to-profits/
[49] McMurrian, R.C.; E. Matulich; "Building Customer Value and Profitability With Business Ethics," *Journal of Business & Economics Research*, November 2006, https://clutejournals.com/index.php/JBER/article/download/2710/2756

of privacy, the enterprise will have lived up to its customers' expectations. It will have done so in a way that could be a lot more meaningful than mere regulatory compliance—which actually seems to do little to allay customer concerns.

What about the side effects? They are all positive, according to the research cited in this paper, and no doubt coupled with increased customer loyalty. The findings emphasize that efforts to build ethics and trust are not undertaken at a cost to the enterprise, but that they can help it grow, in alignment with the privacy-by-design principle of positive-sum impact.

Effective privacy governance will ensure compliance with continually evolving privacy regulations and will always pursue clarification of what privacy means. By being transparent and doing what is right—particularly with respect to data—the enterprise will begin to earn back the trust of the communities it serves. In this way, customers will see that these digital slices of their lives are in good hands, that their personal information is treated respectfully. As a result, the enterprise will gain mindshare from customers with respect to the products and services it offers, resulting in more profitable outcomes. Though privacy is important, it is just one of the many elements enterprises should consider when organizing their governance structures, hierarchy, roles and responsibilities, or developing their mission statements. It can be difficult to integrate privacy into enterprise behavior, tone and governance—but doing so successfully can help build customer trust and potentially profits.

Toward Tomorrow's Privacy Governance

The traditional perception of privacy—that it is something akin to secrecy—may be long gone. Whether it is due to the sheer volume and scale of data breaches, or to the fact that privacy regulations did not enforce consumer rights early enough (thereby allowing organizations to amass and exploit individuals' personal data), the fact is that an incredible amount of personal information is readily available, waiting to be used or abused. Because so many consumer data are available, enterprises must ensure that they handle the information responsibly.

Assuming that data will continue to be acquired by all manner of stakeholders both legally (if not ethically or with opt-in) and illegally, one could argue that all personal data will eventually become available, in one way or another. At that point, personal data may not be adequately controlled or protected by restricting access. Rather, it will become increasingly important for enterprises to be clear about how they acquire and use the data. The goal will be something akin to the purpose of the GDPR, requiring that citizens be informed of the purpose of processing. In other words, the control mechanism will be a set of laws governing how enterprises acquire, use and present data about customers—data that customers opt in to provide, for uses to which they proactively agree.

The role of management is to ensure that enterprises monitor whether a user has opted into the processing in accordance with the law, and also to ensure that enterprise data sources have been acquired through legal—and preferably also ethical—means.

Beyond Compliance: Focus Areas for Boards of Directors

Boards of directors have a fiduciary duty to act in the best interests of the enterprise. However, to act in the best interests of the enterprise "is not synonymous with acting in the best interests of shareholders. …In considering what is in the best interests of the corporation, directors may look to the interests of…shareholders, employees, creditors, consumers, governments and the environment to inform their decisions."[50] The matter is actually not one of profitability or privacy—as some demonstrate through their actions—but rather one of profitability plus privacy.

The matter is actually not one of profitability or privacy—as some demonstrate through their actions—but rather one of profitability plus privacy.

Furthermore, the duty-of-care requirement (part of a board's fiduciary responsibility in some jurisdictions) requires directors to be reasonably informed and to oversee management's decisions through the lens of their impact on the enterprise. Do management's decisions expose the enterprise to levels of legal or reputational risk that extend beyond its risk appetite? If not, the next test is whether the good decisions of a director are also assessed as good decisions by an alternative "reasonable person" (someone who is qualified to fulfill the role of director and who incidentally may also be a customer). If there is disagreement, then there may be the makings of a corporate governance dilemma.

A breach of fiduciary duty is basically an act that constitutes mismanagement,[51] because the duty of care was not exercised appropriately. Thus, a board that encouraged profit at all costs—without considering the best interests of the enterprise, including the best interests of its customers—might be considered in breach of its fiduciary duty, depending on the unique circumstances of the enterprise it serves.

Incidentally, "fiduciary" is etymologically rooted in older terms for "trust."[52] By exercising its fiduciary duty to the enterprise, the board in effect is reinforcing the trust that constituent stakeholders have in the enterprise—an attribute that is good for business.

In the context of fiduciary duty and the best interests of the enterprise, the implications of the previous section, "The Human Element of Privacy," are numerous for boards of directors, extending significantly beyond mere compliance to matters of ethics and trust. Boards must consider the following:

1. **Privacy culture**—It is not in the organization's best interests that regionally diverse customers are potentially disenfranchised by a one-size-fits-all approach to privacy. Multiregional or multinational enterprises need to determine to what extent differences in privacy perceptions between regions are considered in the organization's product and services design.
2. **Risk for reward**—It is not in an enterprise's best interests for its customers to be left with an uneasy feeling about the privacy risk required to receive a benefit. Boards need to decide to what extent the enterprise is acting in its customers' interests by at least educating them about the impact of changes to their privacy settings.
3. **Security by design and privacy by design**—It is in an enterprise's best interests to ensure that privacy is not an afterthought of its development initiatives. Boards must determine whether the enterprise's cybersecurity initiatives should change to ensure the enhanced privacy of its customers, and whether the organization's systems adequately adopt privacy by design and privacy by default. Boards must determine how to communicate requirements to management.

[50] Fasken, "Doing Business in Canada 2019," 17 June 2019, www.fasken.com/en/knowledge/doing-business-canada/2019/06/directors-officers-liability/#:~:text=Under%20the%20EF%AC%81duciary%20duty%20of,%2Dinterest%20or%20self%2Ddealing.

[51] *Ibid.*

[52] *Ibid.*

4. **Hobson's choice**—It is not in an enterprise's best interests to give a customer the perception of choice where in fact there is no choice. In the exercise of its fiduciary duty, the board must determine if it is comfortable that the enterprise is acting ethically with respect to the collection and utilization of its customers' data, notwithstanding any appearance of choice. This extends to implementing a privacy policy that asks for customer consent for data and data processing in exchange for a service for which few viable alternatives exist.
5. **Analytics, artificial intelligence and machine learning**—It is not in the organization's best interests to act on outcomes of analysis that might be biased or otherwise invalid without explicitly testing for those defects. A simple bias could occur, for example, if more personal data were available for one population group than another. The problem with bias, however, is that it cannot be addressed unless one knows of its existence.[53] Furthermore, the potential to re-identify or deanonymize data during data processing should be identified and controlled to maintain privacy. Finally, an enterprise should be able to explain the data processing to data subjects, as required by GDPR Article 5 (lawful, fair and transparent processing).
6. **Personal data as a reflection of a real person's life**—Given that digital transformation is imperative, it is not in an enterprise's best interests to underplay customer centricity. Rather, it is in the enterprise's best interests to acknowledge the humanity of its customers in its digital transformation efforts.
7. **A post-privacy world**—It is not in an enterprise's best interests to ignore or otherwise underplay new technology that has the potential to help solve pressing privacy problems.
8. **Surveillance and tracking**—It is in an organization's best interests to ensure that its customers are aware of the scope and practice of surveillance and tracking. There are implications for governments too: It would be possible to build public trust where trust is dwindling, if governments were clearer on the scope and extent of their surveillance and tracking. Boards should recognize that governments might demand data held by an enterprise—or simply bypass the enterprise and establish means of collection through ancillary technology (perhaps even surveilling the enterprise's own communication infrastructure).

Each of these points highlights the role of directors in ensuring that diverse human privacy issues are governed and managed not only in the enterprise's best interests, but also in the best interests of its customers. These points also highlight the principle that privacy beyond mere compliance is a clear requirement of board directors in the exercise of their fiduciary duty.

[53] Grootendorst, M.; "How to Detect Bias in AI," Medium, 31 January 2020, https://towardsdatascience.com/how-to-detect-bias-in-ai-872d04ce4efd

Conclusion

It is surely an illusion that privacy—as formerly understood—is sustainable; in fact, it is arguably more relevant in today's hyperconnected digital world than ever before. The Internet, social media, and government and enterprise activities have created new uses and, unfortunately, abuses of data—and in the process, have changed the world. Yet, the public's understanding of what it means to be private in this new context has not kept pace. It is time to reevaluate the idea of privacy.

Consumers might readily grant enterprises explicit consent to use personal data, given assurance that it is used responsibly and ethically. However, enterprises' existing efforts at such assurance are not sufficiently effective—and this leads to significant implications for boards, particularly from the perspective of privacy governance beyond compliance.

Perhaps one way to ensure privacy in the future will be a hybrid of enterprise informational accountability and identity solutions. The challenge is, perhaps, not so much in confronting a post-privacy world, but rather in reshaping public perceptions of privacy. Legislation—underpinned by public support and emerging technology—must evolve to keep pace in a rapidly changing, hyperconnected world.

Acknowledgments

ISACA would like to acknowledge:

Lead Developer

Guy Pearce
CGEIT
Chief Digital Officer, Convergence.tech, Canada

Expert Reviewers

Matt Altman
CISA, CRISC, CISM, CGEIT
President, Altman Consulting and Technology, Inc., USA

David Astles, Ph.D.
CRISC, CISM, CISSP
Chief Information Security Officer, United Kingdom

Ashwin Chaudhary
CISA, CRISC, CISM, CGEIT, CDPSE, CCSK, CISSP
Chief Executive Officer, Accedere, Inc., USA

Joyce Chua
CISA, CISM, CDPSE, CFE, CIA, CIPM, CIPP(A), CIPP(E), (C)CISO, FIP, IRCA ISMS Associate Auditor, ITILv3, MCP, PMP
Asia Pacific Privacy Officer, Sony Electronics, Singapore

Mathew Holdt
CISA, CIA
Audit Manager, Protiviti, USA

Board of Directors

Tracey Dedrick, Chair
Former Chief Risk Officer, Hudson City Bancorp, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CDPSE, CISSP, FBCI
Partner, FORFA Consulting AG, Switzerland

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Gregory Touhill
CISM, CISSP
President, AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
Chief Executive Officer, introSight Ltd., Israel

Anna Yip
Chief Executive Officer, SmarTone Telecommunications Limited, Hong Kong

Brennan P. Baybeck
CISA, CRISC, CISM, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

Chris K. Dimitriadis, Ph.D.
CISA, CRISC, CISM
ISACA Board Chair, 2015-2017
Group Chief Executive Officer, INTRALOT, Greece

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

DISCLAIMER

ISACA has designed and created *Privacy: Beyond Compliance* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400

Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/privacy_beyond_compliance_2020

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/