Stop Using the Privacy Paradox as an Excuse to Avoid Privacy by Design

In his influential book Privacy and Freedom, Alan Westin, who helped establish the concept of data privacy, identified four different states of privacy that individuals must regulate at one time or another:

1. Solitude or the opportunity to separate oneself from others and be free from observation
2. Intimacy or the freedom to be alone with others without interference from others
3. Anonymity or the freedom to be in public but still be free from identification or surveillance
4. Reserve or the individual's need to limit communication about themselves (protected by the cooperation of those around them)[1]

These are the traditional ways in which social scientists think about privacy. All four types of privacy are vulnerable. Personal privacy eroding as a consequence of technological development is a premise widely accepted today—and it is not entirely inaccurate. The insidious thing about the privacy threat to the digital world is that one may not even be aware that their privacy has been violated.

Although there is a consensus that privacy is an increasingly pressing concern, what is less clear is who is responsible for protecting individuals. Is it a personal responsibility? Are lawmakers responsible? Or is the onus on organizations that collect and or sell personal data? Each of these entities view (and treat) privacy differently, making it nearly impossible to work toward a common goal. However, it is time to understand that it is the collective responsibility of all these entities to reap all the benefits of modern digital world. Organizations should take the lead to follow the privacy by design approach by proactively embedding privacy into the design and operation of technology systems, infrastructure and business practices. Lawmakers should enable laws that rely less on empowering consumers and more on protecting them. And individuals should understand it is their ethical duty to protect their privacy and continue to educate themselves on how their online actions impact their privacy.

How People View Privacy

Many people may not be aware of how much information they share and how it can be used. Even in the rare instance when they have full knowledge of the consequences of sharing their personal information, they may be unsure what their options are for doing so. The majority of US citizens believe their personal data are unsecure, that data collection poses more risk than benefits and that it is not possible to go through daily life without being tracked (**figure 1**).[2] Although surveys show that people are highly concerned about their privacy,[3] anecdotal and empirical evidence indicates that individuals are willing to trade their personal information for relatively insignificant rewards.[4] This dichotomy of information privacy attitudes and actual behavior has resulted in the term privacy paradox being introduced to the public lexicon.[5]

SARAVANAN GURUMURTHY

Is a financial services technology leader with extensive global management experience in shaping and delivering strategic technology solutions for large investment banks and fintech and private equity organizations. He links business strategies and technology decisions to create sustainable success. Gurumurthy can be reached at https://www.linkedin.com/in/gsaran.

© 2022 ISACA. All rights reserved. *www.isaca.org*

FIGURE 1

How People View Privacy

Majority of American feel as if they have little control over data collected about them by companies and the government

% of U.S. adults who say…

		Companies	The government
Lack of control	They have very little/no control over the data_ collect(s)	81 percent	84 percent
Risks outweigh benefits	Potential risks of_ collecting data about them outweigh the benefits	81 percent	66 percent
Concern over data use	They are very/somewhat concerned about how_ use(s) the data collected	79 percent	64 percent
Lack of understanding about data use	They have very little/ no understanding about what_do/does with the data collected	59 percent	78 percent

Note: Those who did not give an answer or who gave other responses are not shown.

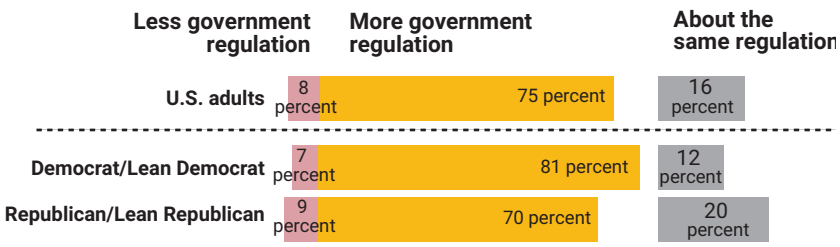
Source: Auxier, B.; L. Rainie; M. Anderson; et al.; "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, 15 November 2019, *https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/*. Reprinted with permission.

FIGURE 2

Government Regulations

Most Americans think there should be more government regulations of what companies can do with personal data

% of U.S. adults who say they think there should be_of what companies can do with their customers' personal information



Note: Those who did not give an answer were not shown.

Source: Auxier, B.; L. Rainie; M. Anderson; et al.; "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, 15 November 2019, *https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/*. Reprinted with permission.

In addition, the difference of opinion between privacy fundamentalists (i.e., those who are well versed in and concerned about privacy), the privacy unconcerned (i.e., those who feel they have nothing to hide) and privacy pragmatists (i.e., those who are somewhere in between the other categories) further complicates the privacy paradox. When it comes to privacy and accountability, people tend to demand the former for themselves and the latter for everyone else. In a 2019 survey, 75 percent of respondents said there should be more regulations on what enterprises can do with private data (**figure 2**).[6]

How Lawmakers View Privacy

Lawmakers operate under the assumption that privacy is a right. They have helped draft policies to ensure that personal privacy is well protected. The 2018 EU General Data Protection Regulation (GDPR) is widely considered a global benchmark for privacy regulations.[7]

Countries in Asia, the North and South America and the Pacific have implemented the following policies aimed at protecting personal privacy:

- Malaysia's Personal Data Protection Act, which went into effect in 2013, regulates the processing of personal data in regard to commercial transactions.[8]
- Brazil's General Protection Data Law, which became enforceable in 2018, is a federal law to unify 40 existing laws to regulate the processing of the personal data of individuals.[9]
- The US State of California Consumer Privacy Act (CCPA) of 2018 provides California residents with the right to know what personal data are being collected, to know whether the data are sold or disclosed to others, to say no to the sale of personal data, to access their personal data, to request businesses to delete it and to not be discriminated against for exercising their privacy rights.[10]

India's forthcoming policy may go even further than its predecessors, claiming "a right to privacy is part of the fundamental rights to life and liberty enshrined in the constitution."[11] Many laws allow organizations to collect, use and disclose data as long as they provide transparency about such practices and consumer consent is given for data use.

How Enterprises View Privacy

Many enterprises view private data as a currency. Customer data are considered one of the most important commodities, and organizations'

© 2022 ISACA. All rights reserved. *www.isaca.org*

increasing collection of data suggests that consumerism will evolve from being about the masses to a story of one. Enterprises justify the forced collection of private data by stating that they offer tailored experiences and recommendations to consumers. They also often add vague lines such as "We take your privacy and security seriously," to their branding to seem reliable but without adding any context. A report by the Norwegian Consumer Council highlights how enterprises employ a series of psychological dark patterns to push users toward selecting intrusive privacy options, resulting in the unintentional loss of user privacy while giving users an illusion of control.[12]

Organizations are forced to invest hefty sums to ensure that they are compliant with new regulations. By 2018, Fortune Global 500 enterprises had spent US$7.8 billion preparing for GDPR, including hiring data protection officers mandated for all enterprises handling large amounts of personal data.[13] Despite these measures, few organizations feel fully compliant, and many are still working on scalable solutions.

At the same time, enterprises are moving ahead with more technological innovations, some of which raise serious questions about data abuse and privacy. The collection of behavioral data can be problematic as it raises concerns about how organizations gather, navigate and use data particularly as more is collected, sparking significant debate about the ethics vs. positive application of new technology.

Privacy Is a Human Right

Human behavior is strongly influenced by specific and concrete ideas. Privacy, on the other hand, is an intangible, hard-to-quantify concept that is not often at the forefront of people's minds. But apathetic, often conflicting attitudes toward privacy can be remedied. Individuals must understand that privacy is the right for an individual to be free from uninvited attention and scrutiny. Article 12 of the Universal Declaration of Human Rights states that "No one must be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation."[14] Generations have long fought for the right to privacy. It is a human right similar to the right to equality, justice, freedom, nationality or religion. Edward Snowden, a former computer intelligence consultant with US National Security Agency (NSA), summed up the basic need for privacy quite well stating that "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."[15]

The Need for Privacy by Design

The notion that individuals have an ethical duty to protect their own privacy implies two things:

1. People have a duty to do the impossible
2. Personal responsibility for one's own privacy precludes government and enterprise responsibility for privacy protection

There are practical limits as to how effectively people can protect their own privacy. Many people lack knowledge of the technologies and data gathering practices that are now commonplace. Some people cannot avoid cultural and economic pressures to engage in transactions that result in information disclosures. Individuals have a limited ability to negotiate privacy-related terms and conditions with organizations and government entities. Protecting information privacy is difficult. It is easy to point fingers at people regarding their privacy maturity or lack of it (**figure 3**)[16] or to adopt the attitude of US Founding Father Benjamin Franklin when he said "They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[17] It is unlikely that consumer demand for privacy protection will force enterprises to instate it, however, it is worth noting that privacy behavior and maturity have significantly improved in recent years.[18]

Lawmakers appear to assume that empowered consumers can make rational, educated decisions about privacy in their own best interests. However, it is dangerous to assume that people are informed enough to willingly grant enterprises consent to use their data (and to act to protect their online privacy after the fact). There is a need for more effective privacy laws that rely less on empowering consumers and more on protecting them. A goal of policy should be to achieve more equitable power between individuals, consumers, citizens and those in possession of their data (i.e., governments and enterprises that currently have the upper hand). Effective privacy policies protect the naïve, the uncertain and the vulnerable. They should be sufficiently flexible to evolve with the emerging and unpredictable complexities of the information age.

LOOKING FOR MORE?

- Read *Privacy by Design. www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

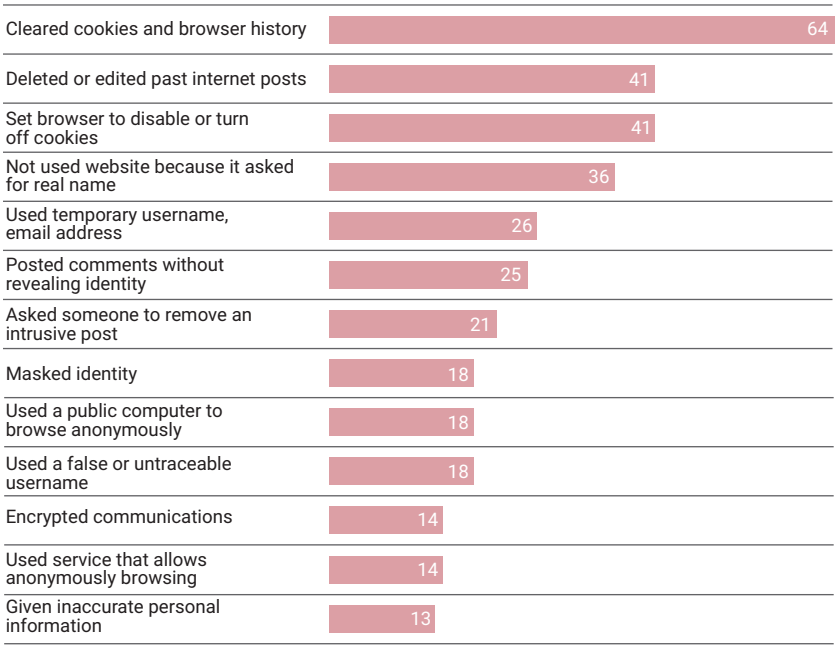
© 2022 ISACA. All rights reserved. *www.isaca.org*

FIGURE 3

Importance of Cyberculture

Consumer concerns over data collection and privacy are mounting, but few take adequate protective precautions.

Respondents taking action, % (n=792)



Source: Anant, V.; L. Donchak; J., Kaplan; H. Soller; "The Consumer-Data Opportunity and the Privacy Imperative," McKinsey and Company, 27 April 2020, *https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative*. Reprinted with permission.

New legislation should put the burden on enterprises to only use, disclose and retain consumer data for legitimate purposes—and obtaining individual consent should not override such an approach. Ideally, moving away from the current patchwork nature of regulation to a more standard common legislation across federal and international level to enable organizations to apply it consistently will make a huge impact. Finally, lawmakers should create legislation that enforces how governments can play a role in educating the public by ensuring that enterprises disclose any potential privacy threats and employing organizations to adhere to policies, all while setting a good example by abiding by best privacy practices themselves.

Enterprises rely on insights from customer data to sharpen their strategy and enhance the customer experience. It is common sense to assume that with access to such data comes an obligation to protect them. Even if up-to-date privacy laws are in place, enforcement is often insufficient. Although fines under GDPR can be as high as four percent of an enterprise's annual turnover and sanctions can destroy an organization from a reputational, brand and financial perspective, regulators have limited resources to make every enterprise comply with the law. There must be a system put in place that provides assurance that organizations are doing all they can to protect consumer data.

Recommendations for enterprises include:

- Move from the current model of making only the benefits of online behaviors visible to making the costs of those decisions also visible.
- Create transparency and simple-to-use features to allow users to opt out of anything that makes them uncomfortable. This should include tracking cookies, user profiling and device fingerprinting.
- Make privacy the default. Organizations in countries with restrictive privacy policies may already have opt-out as the default, but most other organizations still have opt-in as the default.
- Similar to corporate responsibility programs that focus on social issues and philanthropy, privacy should be an element of enterprise culture so that what goes into a privacy policy depends on employee values and priorities.
- Follow the privacy by design (**figure 4**)[19] approach by proactively embedding privacy into the design and operation of technology systems, infrastructure and business practices. Organizations that do this differentiate themselves by taking deliberate, positive measures.
- Stop collecting and throwing every piece of data into a data lake, hoping it will have value in the future. Consider data minimization and move away from the tendency to want to keep data forever, even if they have no value, by implementing and clearly highlighting data retention policies.
- Make the board of directors responsible for recognizing a demonstrated ability to secure and protect digital data—both their own and their customers'—as a business imperative that yields a competitive advantage.

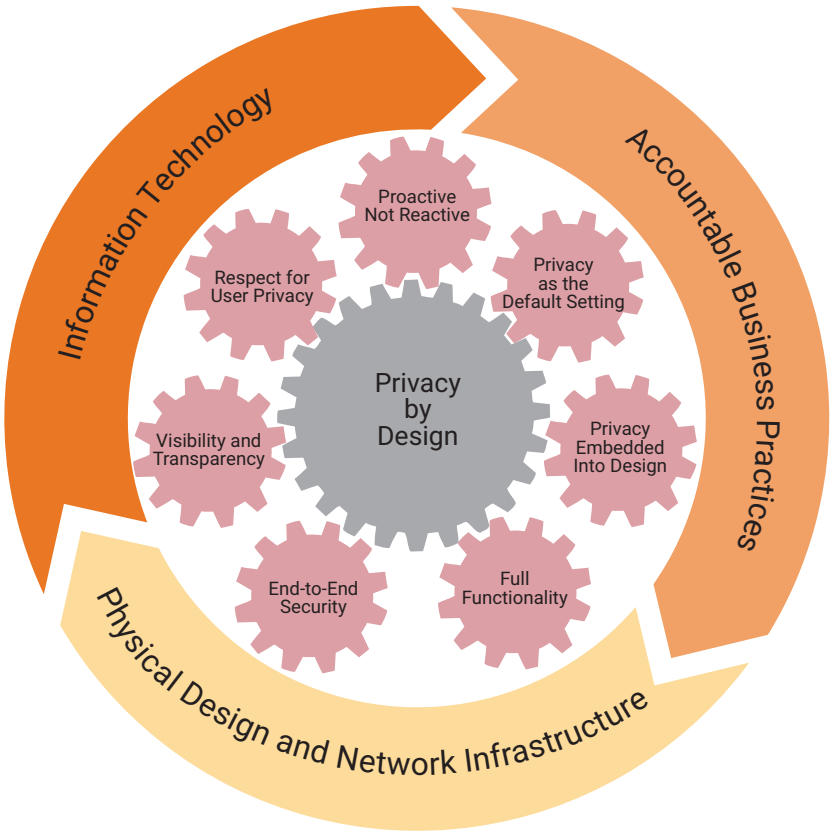
Conclusion

Harvard University (Cambridge, Massachusetts, USA) professor E.O. Wilson once said, "The real problem of humanity is the following: we have Paleolithic emotions, medieval institutions and godlike technology."[20] Indeed, expecting stone-age

© 2022 ISACA. All rights reserved. *www.isaca.org*

brains to self-manage personal data in an ever-changing digital environment is both unreliable and unrealistic. Consumers must demand more top-down privacy protection from such godlike technologies. While people continue to educate themselves, they have a responsibility to hold organizations that fail to protect private data accountable. The bar for enterprises must be raised so that they can no longer trample over consumers' rights to privacy. The benefits of the digital world come at a cost, but it is in the best interest of people, organizations and lawmakers to consciously and continuously endure that the benefits outweigh the costs by collectively working together.

FIGURE 4
Privacy by Design



Endnotes

1 Westin, A.F.; *Privacy and Freedom*, Ig Publishing, USA, 2015
2 Auxier, B.; L. Rainie; M. Anderson; *et al.*; "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, 15 November 2019, *https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/*
3 Security Magazine, "75% of Americans Very Concerned About Online Privacy, But Most Don't Take Any Significant Action," 10 February 2021, *https://www.securitymagazine.com/articles/94560-of-americans-very-concerned-about-online-privacy-but-most-dont-take-any-significant-action*
4 Carrascal, JP; C. Riederer; V. Erramilli; M. Cherubini; R. de Oliveira; "Browsing Behavior for a Big Mac: Economic of Personal Information Online, Proceedings of the 22nd International Conference on World Wide Web, May 2013, *https://www.researchgate.net/publication/311491414_Your_browsing_behavior_for_a_big_mac_economics_of_personal_information_online*
5 Kokolakis, S.; "Privacy Attitudes and Privacy Behavior: A Review of Current Research on the Privacy Paradox Phenomenon," Computers and Security, 2015, *https://www.researchgate.net/publication/280244291_Privacy_attitudes_and_privacy_behaviour_A_review_of_current_research_on_the_privacy_paradox_phenomenon*
6 *Op cit* Auxier
7 Regulation (EU) 2016/679 General Data Protection Regulation (GDPR), European Union, 2018, *https://gdpr-info.eu/*
8 PricewaterhouseCoopers (PwC), "Personal Data Protection Act 2010 (PDPA)," *https://www.pwc.com/my/en/services/assurance/pdpa.html#:~:text=On%2015%20November%202013%2C%20the,with%20respect%20to%20commercial%20transactions.*
9 Deloitte, "Brazilian General Data Protection Act," *https://www2.deloitte.com/br/en/pages/risk/articles/lgpd.html*
10 US State of California Department of Justice, "California Consumer Privacy Act (CCPA)," https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law.
11 Panday, J.; "India's Supreme Court Upholds Right to Privacy as Fundamental Right—and It's About Time," Electronic Frontier Foundation, 28 August

© 2022 ISACA. All rights reserved. *www.isaca.org*

2017, *https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time*

12 Norwegian Consumer Council, *Deceived by Design,* 27 June 2018, *https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf*

13 Lindsey, N.; "Global 500 Faces GDPR Compliance Costs of $7.8 Billion," *CPO Magazine*, 1 December 2017, *https://www.cpomagazine.com/data-protection/global-500-faces-gdpr-compliance-costs-of-7-8-billion/*

14 United Nations, *Universal Declaration of Human Rights,* Paris, France, 10 December 1948, *https://www.un.org/en/about-us/universal-declaration-of-human-rights*

15 Rusbridger, A.; E. MacAskill; J. Gibson; "Edward Snowden: A Right to Privacy Is the Same as Freedom of Speech, Video Interview, *The Guardian,* 22 May 2015, *https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video*

16 Anant, V.; L. Donchak; J. Kaplan; H. Soller; "The Consumer-Data Opportunity and the Privacy Imperative," McKinsey and Company, 27 April 2020, *https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative*

17 National Archives, Pennsylvania Assembly: Reply to the Governor, 11 November 1755, *https://founders.archives.gov/documents/Franklin/01-06-02-0107*

18 *Op cit* Anant

19 Cavoukian, A.; *Privacy by Design: The Seven Foundational Principles, Information and Privacy Commissioner of Ontario*, Canada, 2011, *https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf*

20 Oxford University Press, *Oxford Essential Quotations, 5th Edition,* United Kingdom, 2017

© 2022 ISACA. All rights reserved. *www.isaca.org*