Introduction to Privacy and Compliance for Consumers (v2)

By Clare Nelson

To comment on this article, please visit our GitHub repository and submit an issue.

Table of Contents

Disclaimer

This article should not be considered legal advice. Identity programs that support data protection and privacy as a fundamental human right are complex and highly technical. Many of the data protection and privacy laws in countries around the world are evolving and open to interpretation. Please consult your organization's legal counsel for specific advice appropriate to your jurisdiction

Abstract

This article is the first of several sections of the IDPro Body of Knowledge that address *Privacy and Compliance for Consumers*. This introductory section sets the foundation for subsequent sections on privacy within the IDPro Body of Knowledge, providing an overview of a variety of topics, including definitions of privacy, different approaches to privacy in the consumer sector versus the workforce environment, and more.

Related Sections in the IDPro Body of Knowledge

Please refer to other forthcoming sections of the *IDPro Body of Knowledge*[i] for supporting and complementary information, notably:

- Andrew Cormack's "An Introduction to the GDPR (v2)"[ii]
- Andrew Hindle's "Impact of GDPR on Identity and Access Management (v2)"[iii]
- "Terminology in the IDPro Body of Knowledge"[iv]

Introduction to Privacy and Compliance for Consumers

Identity professionals, including enterprise solution architects, data scientists working in marketing, privacy professionals, product managers, and strategists at data brokers, have an extraordinary opportunity to improve privacy plus compliance with data protection regulations and laws for consumer-facing applications. Several critical issues drive the need for improvement:

1. Unique identification of a *natural person,* such as a consumer, is easier than ever before. The smallest shred of digital exhaust, physical actions, or attributes can be collected, correlated via machine learning, and analyzed to identify a unique consumer or household with sufficient probability.
2. Consent is broken. The complexity of privacy notices, and the length of privacy policies that are rarely read, lead to a pattern of ineffectiveness, the illusion of choice, burden on the consumer, and the eventual agreement to broad terms which may not have limits or may be modified at any future date with only limited or obscure notice. As privacy and law expert Daniel Solove has stated, "Giving individuals more tasks for managing their privacy will not provide effective privacy

protection."[v] There is a growing realization that privacy laws should make stewardship of data the responsibility of the data controller and/or data processor, not the consumer.

3. Data privacy laws are years behind technology innovations, and the gap is expanding. Privacy laws cannot keep pace with technological advancements and are years behind in catching up to the 4,000 data brokers and analytics companies that collect personal data across all touchpoints, many of which are adding muscle with machine learning. Many marketing companies, plus some of the world's largest organizations, are seeking alternatives to third-party cookies in order to be able to continue to identify consumers, all within the porous guidelines of current privacy law.
4. Anonymity does not exist, and pseudonymization provides weak protection
    a. For example, researchers have proved that based on geolocation alone, anonymity does not exist.[vi]
    b. Similarly, researchers posit that it is becoming easier to re-identify a person:
        i. Once released to the public, data cannot be taken back. As time passes, data analytic techniques improve, and additional datasets become public that can reveal information about the original data. It follows that released data will get increasingly vulnerable to re-identification—unless methods with provable privacy properties are used for the data release.[vii]
    c. *Communications of the ACM* recently published an article on anonymity that confirms what many mathematicians have always known: there is still a pattern in the anonymous data and a way to de-anonymize it.[viii]
        i. "Anonymized data can never be totally anonymous: anonymization is not sufficient for private companies to avoid conflicts with laws such as Europe's General Data Protection Regulation, and the California Consumer Privacy Act."[ix]

The scope of privacy for what the GDPR calls *natural persons* keeps expanding because the ability to uniquely identify a human being with the tiniest bit of digital exhaust or trace of online or offline behavior keeps expanding. Where a person ate lunch, the way they moved their mouse to find the cursor, what they said to a service representative over the phone in light of the warning, "this call may be recorded for quality purposes," what they bought online, their device and all its related attributes, or where they bought gas may be sufficient to uniquely identify a natural person. Long gone are the days when name, address, social security number, and date of birth were the only identifiers. Now, we need to protect massive collections of personal and related data in order to provide privacy for consumers.

Terminology and Acronyms

- Consent - permission for something to happen or agreement to do something

- GDPR – General Data Protection Regulation[x]
- CCPA – California Consumer Privacy Act[xi]
- Natural Person – an individual human being
- NY SHIELD Act – New York "Stop Hacks and Improve Electronic Data Security" Act[xii]
- Privacy - an abstract concept with no single, common definition

Scope

The lofty goal of this section on *Privacy and Compliance for Consumers* is to present a global perspective. However, the initial release of this section is more focused on the GDPR, CCPA, and NY SHIELD Act with a light coverage of China and the rest of the world. As noted below in the Resources section, the International Association of Privacy Professionals (IAPP) is an excellent source of information for immediate, current, comprehensive global coverage.

Requirements for data protection and associated privacy regulations are increasing around the world. On March 21, 2020, the NY SHIELD Act went into effect, and China is working on updated privacy law. Most are familiar with the GDPR and CCPA.[xiii] The figure below highlights global regulation and enforcement as heavy, robust, moderate, or limited.

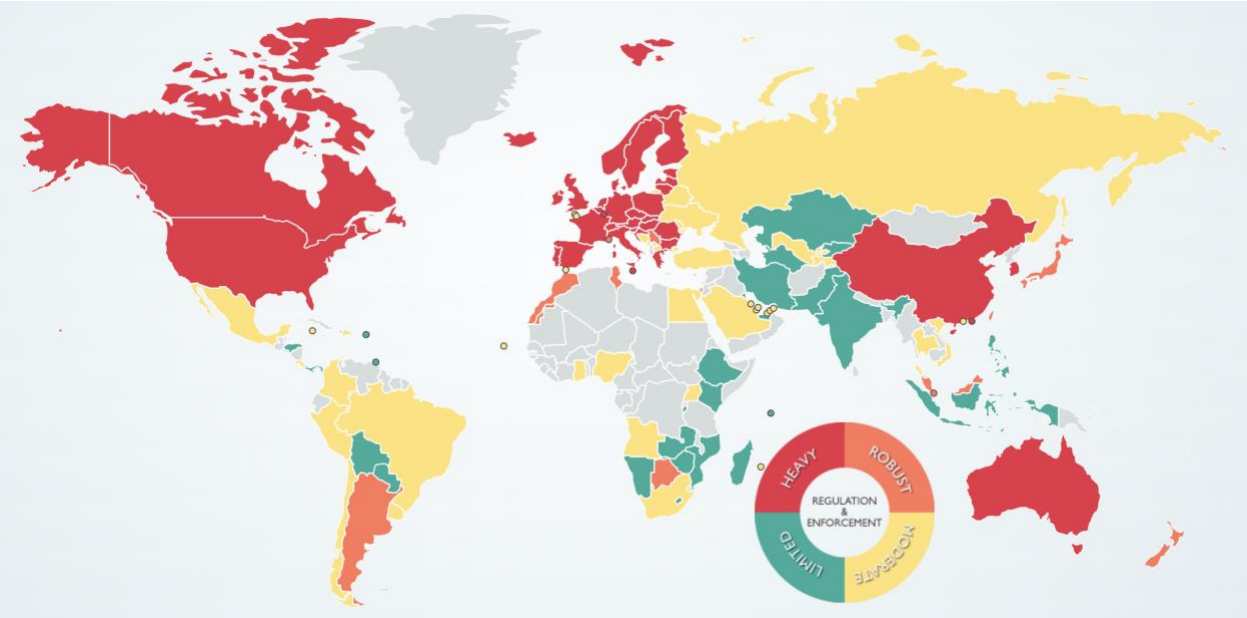

Figure 1 - Global Privacy Regulation Varies from Heavy to Limited[xiv]

In addition to a global scope, this section covers digital identities – including online services and apps – as well as physical interactions (e.g., customers entering a store or service establishment).

In this section, we consider personal data obtained, stored, or tracked through a variety of mechanisms, including cookies, electronic communications (Internet, email, messaging, apps), Wi-Fi, telephone, and Internet-of-Things (IoT). All of this data can be used to identify

a unique individual and may be considered private, requiring protection as a *fundamental human right*. The first recital of the GDPR states that data protection is a *fundamental right* according to the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union (TEFU).[xv,xvi] The United Nations adopted the Universal Declaration of Human Rights in 1948, a global mandate for privacy, as articulated in Article 17:[xvii]

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

	EU GDPR	EU ePrivacy Directive	US CCPA, NY **SHIELD**, other	California, Oregon IoT Security Law; Singapore, others	Rest of the World
What is covered?	Personal data, cookie consent	Cookies, Internet, email, messaging, phone; tracking mechanisms, right of confidentiality	Personal data, household data under CCPA	Any connected device; has an IP address or Bluetooth address	China - none; APEC - Personal Information*

Table 1. Beyond GDPR: Personal Data Includes Cookies, Phone, and IoT

*According to the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, Personal Information is any information about an identified or identifiable individual. [xviii]

The GDPR is closely related to the ePrivacy Directive. The ePrivacy Directive is soon to be replaced with the ePrivacy Regulation. The GDPR and ePrivacy Regulation are both parts of the data protection reform in the EU; where there is overlap, the ePrivacy Regulation overrides the GDPR, notably for cookies and electronic communication.[xix]

IoT law is covered below. Note that emerging laws seek first to get rid of embedded or hardcoded passwords. When an IoT device ships with the password already installed from the manufacturer, this makes it easy to breach privacy as well as to create botnet malware.

Setting the Stage

Scholars and privacy experts, including Hartzog, Zuboff, Schneier, and Maler, set the stage for examining these topics and beyond.

Hartzog

Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University, and among other roles is an Affiliate Scholar at Stanford Law School for Internet and Society. In April 2019, Hartzog co-authored *The Pathologies of Digital Consent* with Neil Richards, where they discuss defects that consent models can suffer, including: [xx]

- Unwitting consent
- Coerced consent
- Incapacitated consent

These consent defects are a far cry from the *gold standard of knowing and voluntary consent*. Hartzog and Richards conclude:

The over-use of consent in the digital context, combined with limited legal policing of the sufficiency of consent, has allowed great fortunes to be created on the basis of personal data, but it has also exposed consumers to data breaches, identity theft, and a surveillance economy unprecedented in human history, one which stretches the very notion of "consent" to say that it was ever actually agreed to.

More fundamentally, the manufacturing of consent by exploiting consent's pathologies has diminished the trust in our digital environment that is the key ingredient toward a better future. We can do better, but in order to do so, we need to recognize the pathologies of consent and limit consent to the contexts in which it is most justified. Going forward, we must rely on strategies other than fictive, manufactured, or coerced consent to minimize the risks and harms of our information economy if we seek to take advantage of its benefits in a sustainable, ethical, and progressive way.

These consent issues are discussed further in subsequent sections, including a proposed solution or *theory of consumer trust* as an alternative to an over-reliance on increasingly pathological models of consent.

Zuboff

In her recent, award-winning book, *The Age of Surveillance Capitalism: The Fight for a Human Future and the New Frontier of Power*, Harvard's Shoshana Zuboff clearly articulates her well-researched assertion that we live in a state of *surveillance capitalism.* Zuboff's message is clear:

"Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data.

- Although some of these data are applied to service improvement, the rest are declared as a proprietary behavioural surplus, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into prediction products that anticipate what you will do now, soon, and later.
- Finally, these prediction products are traded in a new kind of marketplace that I call behavioural futures markets.
- Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behaviour."[xxi]

Schneier

Zuboff's 2019 book on surveillance capitalism makes Bruce Schneier's 2015 book, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,* pale in comparison. Consumers are left wondering, "Why didn't you tell me it was so bad?" because Schneier does not provide the chilling detail about how far surveillance and collection of behavioral surplus have advanced. Zuboff's words are even reflected in marketing messages of leading "data protection" vendors, "Privacy is the right of an individual to be free from uninvited surveillance."[xxii]

Maler

In her 2018 Identiverse talk, *Don't Pave Privacy Cow Paths: Retool Consent* for the New Mobility, ForgeRock CTO, then-VP Innovation and Emerging Technology, Eve Maler describes why "Consent doesn't scale for the requirements of email, laptops, and browsers, never mind mobile devices and applications.

- How much worse is the situation going to get as connected vehicles become an ever-bigger part of consumers' lives and an ever more significant integration point for every industry?" Maler establishes the "New Mobility as a critical scenario for examining consumer requirements for trust, regulatory requirements for privacy, how consent experiences and consent management must adapt, and how we can begin to meet these challenges."[xxiii]

Maler's words were prescient because, in the rush to implement consent for GDPR compliance, many companies have simply paved cow paths. Her talk describes how to refactor consent to accommodate today's architectural requirements for asynchronicity, automation, and abstraction.

What is Privacy?

Privacy is an abstract concept, and there is a myriad of definitions.

Privacy as a Fundamental Human Right

The protection of personal data often refers to autonomy and control over one's data. This level of autonomy and control varies depending on the context. In general, the definition of privacy differs from country to country or state by state. Even though the US is one of 48 United Nations countries that voted to adopt the Universal Declaration of Human Rights, the US does not share the EU's embrace of privacy as a *fundamental human right.* For example, instead of a comprehensive, federal law, it is building a patchwork of state-specific laws.

- In the EU, human dignity is recognized as an absolute fundamental right.
- In this notion of dignity, privacy, or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value.
- The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8), and the European Charter of Fundamental Rights (Article 7).[xxiv]

Westin. In the 1960s, Privacy pioneer Alan Westin defined privacy as "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[xxv]

US Supreme Court. In 1989, the US Supreme Court wrote, "Both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[xxvi]

China. In the People's Republic of China (PRC), a complex array of laws govern personal data and privacy, due to be eclipsed by comprehensive regulation in the future. The trend indicates "individuals are gaining significant data protection rights in the private sectors but cannot claim any remedies for the infringements of their privacy carried out by the state government."[xxvii] Today, various laws apply, depending on the sector: financial services, e-commerce, telecommunications, Internet services, content providers, or healthcare.

APEC. The Asia Pacific Economic Cooperation (APEC) Privacy Framework can be downloaded here. The APEC Privacy Framework protects privacy within and beyond economies and enables regional transfers of personal information that benefits consumers, businesses, and governments. This framework is used as a basis for the APEC Cross-Border Privacy Rules (CBPR) System. The framework countries and participants include the countries in the map below.

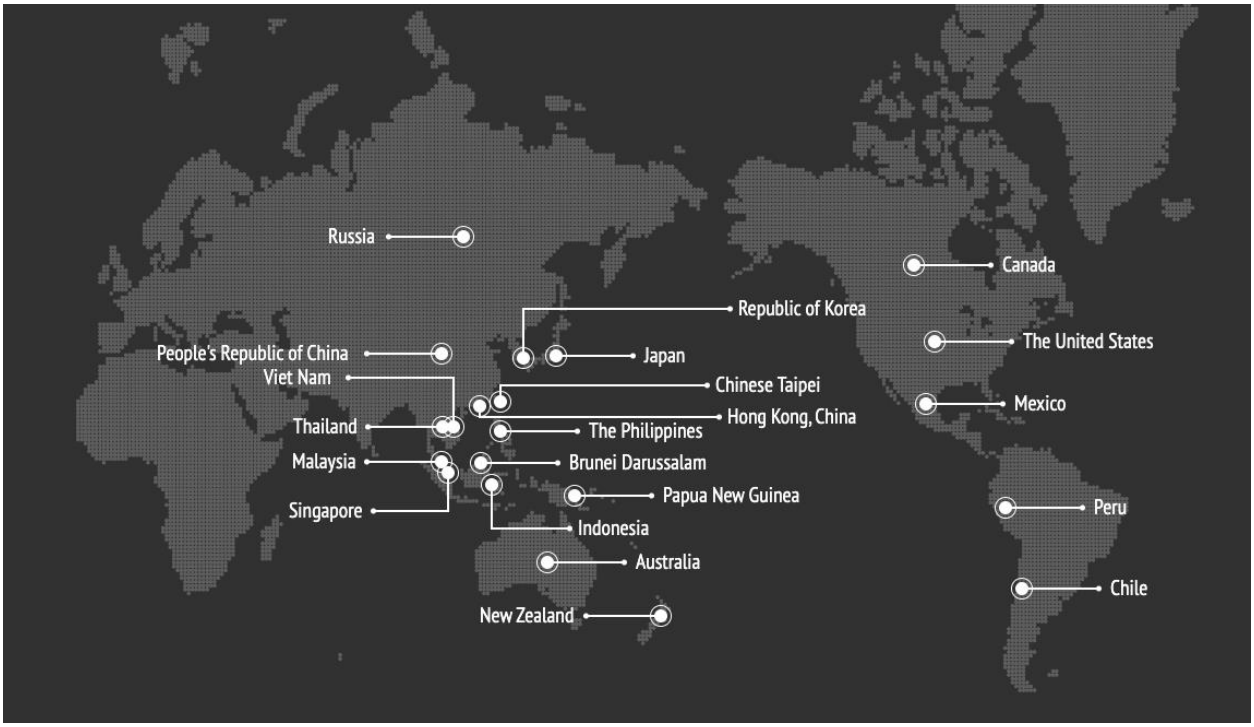

Figure 2 - Map of the APEC Cross-Border Privacy Rules (CBPR) System framework countries and participants[xxviii]

Privacy Models

According to Samm Sacks, Senior Fellow Yale Law School, Paul Tsai China Center, there are two basic privacy models: 1) China, and 2) GDPR. She indicates that Viet Nam, Kenya, and India are more closely aligned with China's model.[xxix] Even though China's privacy laws are influenced by the GDPR, they are markedly different both in detail (for example, China supports implied consent, whereas the GDPR requires explicit consent) and in spirit (in general, the rights of the state supersede individual rights). The privacy dichotomy in China is evidenced by the increased protection of consumers from technology companies such as Renren and other Chinese Facebook counterparts, even as government surveillance intensifies.

Beyond privacy law, organizations approach privacy for consumers in a variety of ways. The role of the identity professional is first to understand the organization's posture with regards to privacy, security, and risk.

Privacy Taxonomy

One of the world's leading experts on privacy law is Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School. As depicted in Solove's privacy taxonomy below, privacy has two main parties:

- The Data Subject, or consumer
- The Data Holders, or data processor and controller

The four main processes in the privacy taxonomy comprise:

- Information Collection
- Information Processing
- Information Dissemination
- Invasions

The four processes may be viewed in order, starting with Information Collection and ending with Invasions. The Information Collection of data about a Data Subject is done by the Data Holder, or data processor and controller to put it in GDPR terms. The collection of data about a Data Subject or individual may be done by another individual, business, government, or external organization via surveillance or interrogation. The Information Processing includes the storage of data and any additional steps taken to apply something like a software algorithm to further derive value. Insecurity refers to a lack of security. Information Dissemination includes many harmful things that might result if the information is part of a list of undesirable actions, including a Breach of Confidentiality, Disclosure, Exposure, Blackmail, or Distortion. Invasions include intrusion and decisional interference, which Solove describes as "the government's incursion into the data subject's decisions regarding her private affairs."[xxx]

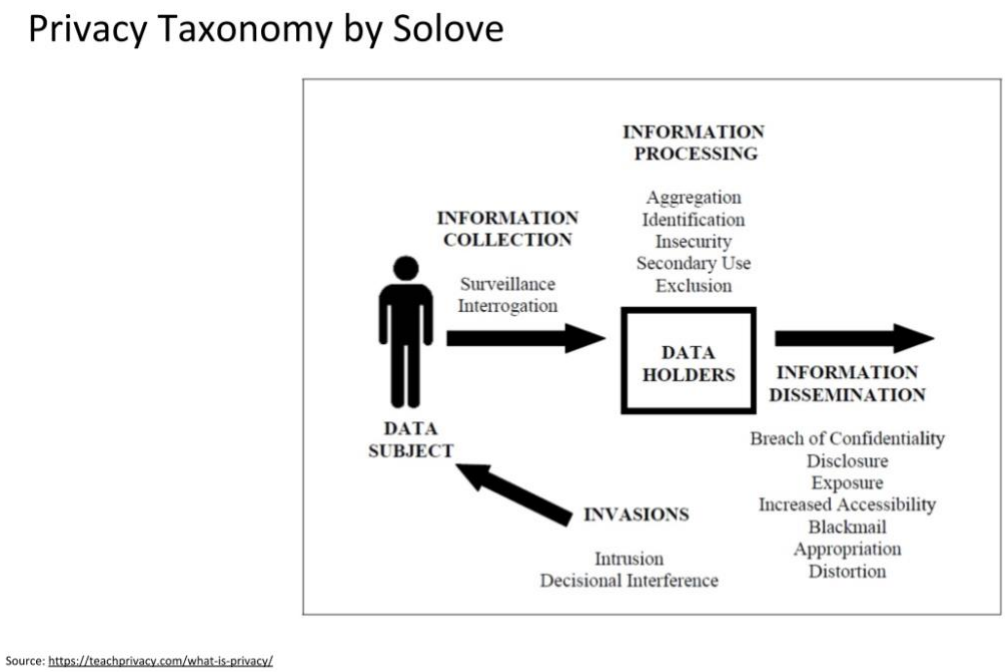

Figure 3 - Privacy Taxonomy by Solove

[Permission received from author to use this graphic]

Privacy by Design

Privacy by Design is the brainchild of Ann Cavoukian, one of the world's leading privacy experts; former Information and Privacy Commissioner of Ontario, Canada; former distinguished visiting professor at Ryerson University, where she was also Executive Director of the Ryerson's Privacy and Big Data Institute; and founder of Global Privacy and Security by Design Centre. Originally published in 2009, the Privacy by Design Principles, depicted in the figure below, are an integral part of the GDPR and subsequent GDPR-influenced privacy laws. Privacy by Design takes a holistic, systems engineering approach and makes it clear that compliance with regulations is not enough. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.[xxxi]

In the Privacy by Design figure below, note that *privacy by default* is one of the seven principles. The sharp contrast of cultural expectations may come as a surprise to some. As a gross generalization, the EU sensibility is to have privacy by default as the norm, whereas in the US, privacy by default is the rare exception.

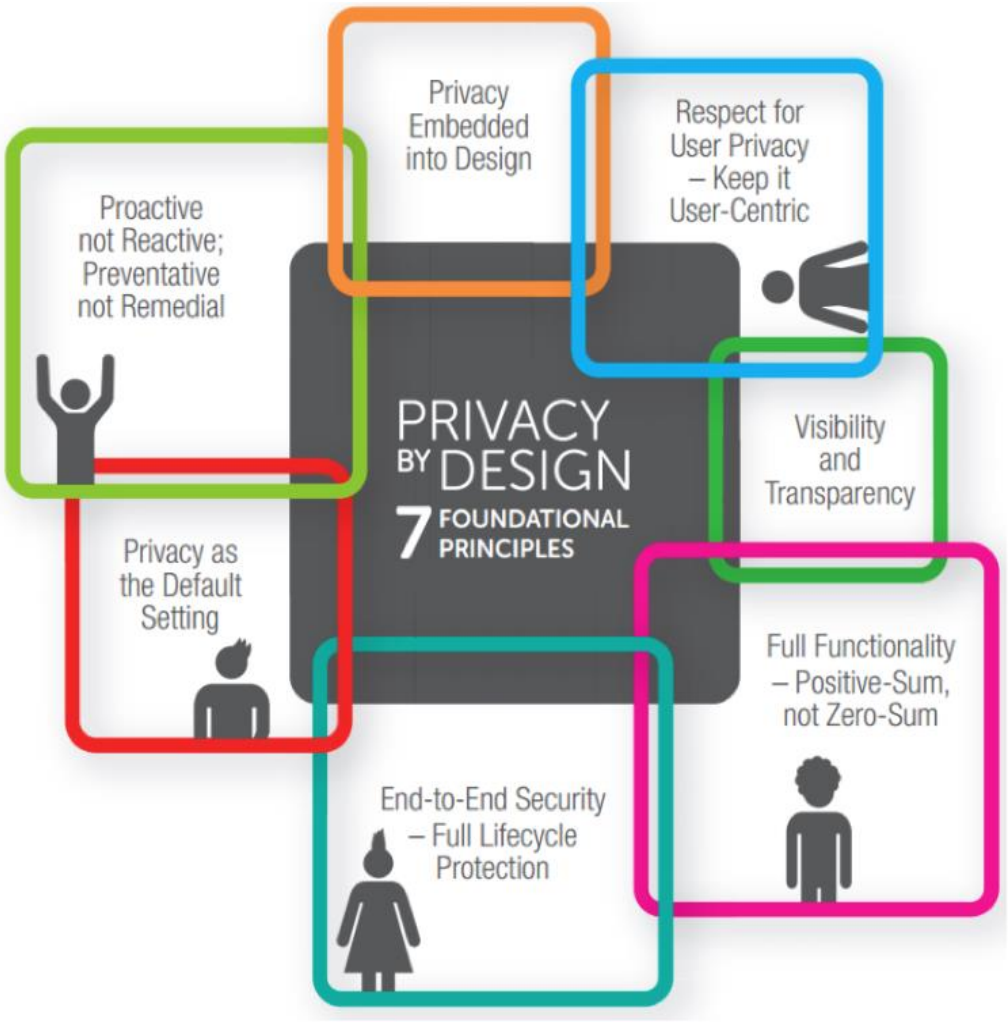

Figure 4 - Privacy by Design, Seven Foundational Principles[xxxii]

Cavoukian builds upon her initial Privacy by Design work in a subsequent document, *7 Laws of Identity, The Case for Privacy-Embedded Laws of Identity in the Digital Age*, where she maps privacy fair information to the Privacy-by-Design principles, resulting in "privacy-embedded Laws of Identity."[xxxiii] She warns:

> *A universal identity system will have profound impacts on privacy since the digital identities of people - and the devices associated with them - constitute personal information. Great care must be taken that an interoperable identity system does not become an infrastructure of universal surveillance.*

Compliance is Necessary but not Sufficient

To a limited extent, privacy law enforces data protection. This section applauds the advances of privacy law, plus it explores some of the failings, flaws, and shortcomings of privacy law, including consent issues, time lag, and reactive posture because the law cannot

keep pace with current innovations, and what Harvard's Shoshana Zuboff calls the asymmetric power stranglehold of Google, Facebook and others that are immune from the effective impact of privacy law because the law does not cover much of what they do with the collection of behavioral surplus.

- **Compliance ≠ Privacy or Security.** As an identity professional, remember that just because you are compliant does not mean you have achieved the appropriate level of privacy and security required by your organization (or expected by your customers), hopefully documented in its risk and privacy policies.
- **Privacy Law' Gap Growth' is Exponential.** Distinguished Fellow at Harvard Law, Vivek Wadha explains, "The gaps in privacy laws have grown exponentially. These regulatory gaps exist because laws have not kept up with advances in technology. The gaps are getting wider as technology advances ever more rapidly."[xxxiv]

Privacy and compliance capabilities are foundational for any Consumer Identity & Access Management (CIAM) program because they protect the personal data of consumers as well as safeguard organizations by defining guidelines for compliance in alignment with the organization's privacy, security, and risk management policies. If organizations do not comply, there are many negative consequences, including:

- Fines (for GDPR, up to €20 million or 4% of annual turnover, whichever is highest)
- Reputational or brand damage
- Loss of customers, loyalty erosion
- Lawsuits
- CEO may be held personally responsible

As an identity professional, you may be part of a team responsible for some or all aspects of privacy and compliance for consumers. This section will enable you to contribute and have a basic understanding of jurisdiction, consent, and data protection across the entire organization. For GDPR or CCPA compliance, you may interact with human resources, product engineering, security, marketing, IT, legal, customer support, procurement, and beyond, as shown in the figure below.

HOW DO WE START MANAGING A DATA PRIVACY PROGRAM?

- The implications of the GDPR/CCPA reach well beyond the core, ongoing compliance functions.
- Alignment with the GDPR/CCPA has downstream implications on various business operations.

Privacy/ Compliance	Data subject / Consumer requests, DPIAs, data sharing, etc.	**Human Resources**	Training, employment agreements, etc.	**Product Engineering**	GDPR/CCPA product functionality
Cyber Security	Security assessments, monitoring of cyber security program, etc.	**Marketing**	Consent management, cookies, etc.	**Information Technology**	Protection-by-design, encryption, minimization, etc.
Legal	Regulatory guidance, third-party relationships, etc.	**Customer Support**	Data subject / Consumer requests, customer inquiries, etc.	**Procurement**	Third party relationships

Figure 5 - How to Start Managing a Data Privacy Program, an Example[xxxv]

Why Consumer Services Need Different Privacy and Compliance Strategies

CIAM and Workforce IAM

Privacy and compliance strategies for workforce IAM have some overlap with CIAM, but CIAM differs in some key regards. For this reason, simply applying workforce privacy and compliance to CIAM projects may not be optimal. Below are some of the key differences between privacy and compliance strategies for workforce versus CIAM projects:

- SCALE: CIAM scale is often orders of magnitude greater to reflect a large consumer population versus a smaller, more predictable number of employees and workforce
- CUSTOMER EXPERIENCE (CX): CX requirements for consumers are more demanding. For its members, IAPP provides a GDPR-centric document, *The UX Guide for Getting Consent:*
    - *"Consent is at the very heart of data protection and privacy,"* and while it is important, it is not the be-all and end-all of a privacy program. For example, a layered or intelligent privacy notice strategy can help make privacy interactions less cumbersome.
    - The data subject must have a say in how personal data is collected, used, shared, and destroyed.
    - Even if a choice doesn't appear to be promoted, wording, widget, and sequence matter.[xxxvi]

- LAW: Depending on the jurisdiction, the privacy law may differ in some cases for IAM versus CIAM.
- AUTOMATION: Appropriate levels of automation differ to meet spikey or unpredictable consumer demand.
- ADVERTISING: Online behavioral advertising in particular, and any advertising in general, is typically aimed at consumers, not the workforce.
- MACHINE LEARNING AND PROFILING: What the GDPR refers to as "automated processing", including profiling (automated processing of personal data to evaluate certain things about an individual); plus, machine learning is often applied to consumer data for different purposes for the workforce versus consumers.

CIAM and Social Identity

CIAM often relies on integration with social media identity providers. There are several benefits to this direction, including reducing end-user friction during sign-up and self-service registration, generating fewer usernames and passwords for the end-user to memorize, and simplified business processes that allow for outsourcing user account recovery processes. This integration is not without drawbacks, however, as integration with social media identity providers may enable cross-site tracking of users without their permission.

Security is Critical

Identity professionals need to understand their organization's risk management policies for security and privacy and work in concert with their colleagues who create those policies, as well as those responsible for the implementation of the policies. The security policy is a necessary dependency for any successful privacy policy. There is a saying, "You can have security without privacy, but you can't have privacy without security."[xxxvii] Security or cybersecurity may be used interchangeably. Some also use the term information security. In the figure below from the NIST Privacy Framework, the relationship between cybersecurity risks and privacy risks makes it clear that managing cybersecurity risk may help mitigate privacy risk, but it is not sufficient because privacy risk can result from incidents outside the realm of cybersecurity incidents. For example, smart meters or smart thermostats may collect and record personal data and possibly represent a privacy risk even though they are operating as intended.

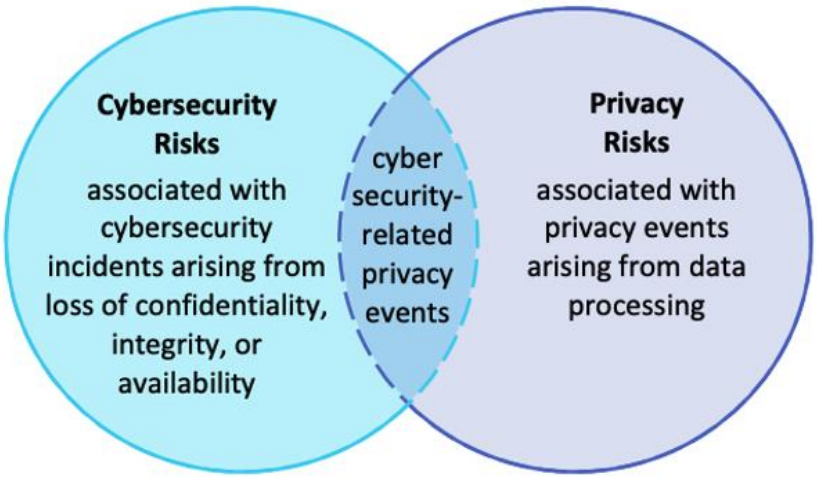

Figure 6 - Relationship Between Cybersecurity Risks and Privacy Risks[xxxviii]

Privacy Policy is a Business Decision

An in-depth understanding of an organization's policies will provide clarity for the identity professional's role in privacy and compliance for consumers. For example, in some cases the marketing department may need to collect extensive personal data, and the organization's privacy policy may allow this. In other cases, the organization's business may depend on trust and confidentiality of personal data; and there may be ample budget to ensure data protection for consumers in a visible, transparent, and robust manner.

Figure 7 - Relationship Between Privacy Risk and Organizational Risk[xxxix]

How an organization deals with consumer privacy and any associated risk is a business decision; the option to mitigate, transfer, avoid, or accept risk may be made in concert with privacy policy formulation or at a later time.

- **Mitigate**. Mitigating the risk (e.g., organizations may be able to apply technical and/or policy measures to the systems, products, or services that minimize the risk to an acceptable degree);

- **Transfer**. Transferring or sharing the risk (e.g., contracts are a means of sharing or transferring risk to other organizations, privacy notices, and consent mechanisms are a means of sharing risk with individuals);
- **Avoid**. Avoiding the risk (e.g., organizations may determine that the risks outweigh the benefits, and forego or terminate the data processing); or
- **Accept**. Accepting the risk (e.g., organizations may determine that problems for consumers are minimal or unlikely to occur; therefore, the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).[xl]

Is Privacy a Competitive Advantage?

As noted above, laws and regulations typically lag innovative product and service offerings. Compliance with current and upcoming privacy laws is only the start. Privacy may be a competitive advantage or not. It depends on your organization and its consumers. In 2010, data protection pioneer and expert Alan Westin was paraphrased, "The idea that privacy can be used as a business advantage is dead, privacy controls are too complex for consumers to understand and a certification culture would be more effective."[xli] Others take the counterargument. Organizations realize that many consumers would enjoy greater control over their data. Privacy for consumers is an opportunity to build trust. Among others, a GDPR and CCPA paper from Akamai provides "tips to build customer trust through regulatory compliance and identity governance."[xlii]

Beyond GDPR: ePrivacy and the New European Strategy for Data

The ePrivacy Directive, soon to be a Regulation, is discussed below. In February 2020, the EU published "A European Strategy for Data." The continuous advancement and proven EU leadership in data protection is a driving force for the rest of the world.

The European Strategy for Data is sector-specific, e.g., healthcare, and provides for:

- Data can flow within the EU and across sectors.
- European rules and values, in particular personal data protection, consumer protection legislation, and competition law, are fully respected.
- The rules for access to and use of data are fair, practical, and clear, and there are clear and trustworthy data governance mechanisms in place; there is an open but assertive approach to international data flows based on European values.[xliii]

Blockchain. The European Strategy for Data includes the evaluation of blockchain technology.

- New decentralised digital technologies such as blockchain offer a further possibility for both individuals and companies to manage data flows and usage, based on individual free choice and self-determination. Such technologies will make dynamic

data portability in real-time possible for individuals and companies, along with various compensation models.[xliv]

In addition, the French data protection authority, known as the National Commission on Informatics and Liberty (CNIL), has spearheaded work on "responsible use of the blockchain in the context of personal data" plus the potential privacy risks inherent in the technology.

The challenges raised by blockchains in terms of compliance with human rights and fundamental freedoms necessarily call for a response at the European level. The CNIL is one of the first authorities to officially address the matter and **will work cooperatively with its European counterparts to suggest a strong and harmonised approach.**[xlv]

Conclusion

Although it may be difficult to define privacy, the fundamental principles of Privacy by Design, depicted in Figure 5 above, create a well-defined foundation for understanding and implementing *Privacy and Compliance for Consumers*. This is why Privacy by Design is included in the GDPR and CCPA, and has significantly influenced subsequent privacy regulations and laws. By now, identity professionals have a clear picture of the interlinked dependencies between identity, privacy, and security. Security protects the data; how privacy is provided is based on business and risk policies. The silver lining for the daunting task of implementing privacy and compliance for consumers is that it may be viewed as a competitive advantage and well worth the extra effort.

Author Bio

Clare Nelson, CISSP, CIPP/E, AWS Certified Cloud Practitioner; is the CEO of ClearMark Consulting, specializing in business development and product strategy. Prior to that, she was VP Technology Alliances & Channel Sales for Identity Governance and Cloud Privileged Access Management leader Saviynt, responsible for AWS and Google Cloud partnerships. Clare's passion for cybersecurity includes her specializations in identity and privacy comprising: MFA, IGA, PAM, identity proofing, privacy-preserving authentication based on ZKP, identity theft, AML/KYC, and GDPR. Clare has held leadership positions at Novell, EMC2, Dell, and AllClear ID. She is a co-founder of C1ph3r_Qu33ns, an organization dedicated to cultivating and supporting the careers of women in cybersecurity. Clare is a second-generation yogi and technologist, and has a degree in mathematics from Tufts University.

Change Log

Date	Change
2020-06-17	V1 published
2021-09-30	Updated date of NY SHIELD act; added section on CIAM and Social Identity; added section title for CIAM and Workforce IAM; added Heather Flanagan as editor

[i] "IDPro Body of Knowledge," IDPro, https://www.idpro.org/body-of-knowledge/.
[ii] Cormack, Andrew, "Introduction to the GDPR (v2)," IDPro Body of Knowledge, 30 June 2021, https://bok.idpro.org/article/id/11/.
[iii] Hindle, Andrew, "Impact of GDPR on Identity and Access Management," IDPro Body of Knowledge, 31 March 2020, https://bok.idpro.org/article/id/24/.
[iv] "Terminology in the IDPro Body of Knowledge," IDPro Body of Knowledge, 30 September 2021, https://bok.idpro.org/article/id/41/.
[v] Solove, D., "The Myth of the Privacy Paradox," SSRN e-Library, 24 February 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265.
[vi] Narayanan, Arvind, and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets," The University of Texas at Austin, n.d., https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.
[vii] Narayanan, Arvind, Joanna Huey, and Edward W. Felton, "A Precautionary Approach to Big Data Privacy," 19 March 2015, https://www.cs.princeton.edu/~arvindn/publications/precautionary.pdf.
[viii] "'Anonymized' Data Can Never Be Totally Anonymous, says Study," The Guardian, 24 July 2019, https://cacm.acm.org/news/238352-anonymized-data-can-never-be-totally-anonymous-says-study/fulltext.
[ix] Ibid
[x] "Complete guide to GDPR compliance," Horizon 2020 Framework Programme of the European Union, https://gdpr.eu/.
[xi] "California Consumer Privacy Act (CCPA)," Office of the Attorney General, California Department of Justice, https://oag.ca.gov/privacy/ccpa.
[xii] "An act to amend the general business law and the state technology law, in relation to notification of a security breach," Senate Bill S5575B, The New York State Senate, 7 May 2019, https://www.nysenate.gov/legislation/bills/2019/s5575.
[xiii] "The California Consumer Privacy Act of 2018," Assembly Bill No. 375, Chapter 55, California State Legislature, 29 June 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
[xiv] "Data Protection Laws of the World," map, DLA Piper Intelligence, https://www.dlapiperdataprotection.com/
[xv] "Charter of Fundamental Rights of the European Union," Official Journal of the European Union, C 392/391, 26 October 2012, http://data.europa.eu/eli/treaty/char_2012/oj.

[xvi] "Treaty on the Functioning of the European Union," Official Journal of the European Union, C 326, 26 October 2012, ttp://data.europa.eu/eli/treaty/tfeu_2012/oj.
[xvii] United Nations, "The Universal Declaration of Human Rights," 1948, https://www.un.org/en/universal-declaration-human-rights/.
[xviii] "APEC Privacy Framework," International Association of Privacy Professionals (IAPP), n.d., https://iapp.org/resources/article/apec-privacy-framework/.
[xix] "The new EU ePrivacy Regulation: what you need to know," i-SCOOP, n.d., https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/.
[xx] "Richards, Neil, and Woodrow Hartzog, "The Pathologies of Digital Consent," SSRN e-Library, 11 November 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433.
[xxi] Naughton, John, "'The goal is to automate us': welcome to the age of surveillance capitalism," The Guardian, 20 January 2020, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.
[xxii] Petters, Jeff, "Data Privacy Guide: Definitions, Explanations and Legislations," Varonis, 29 March 2020, https://www.varonis.com/blog/data-privacy/.
[xxiii] Maler, Eve, "Don't Pave Privacy Cow Paths: Retool Consent for the New Mobility" (video), Identiverse 2018, 26 June 2018, https://www.youtube.com/watch?v=eP5U2sA6EFk&t=254s.
[xxiv] "Data Protection," European Data Protection Supervisor, n.d., https://edps.europa.eu/data-protection/data-protection_en
[xxv] Westin, Alan F. "Privacy and freedom." Washington and Lee Law Review 25, no. 1 (1968): 166.
[xxvi] Cate, Fred H., Beth E. Cate, "The Supreme Court and information privacy," International Data Privacy Law, Volume 2, Issue 4, November 2012, p 255-267, https://doi.org/10.1093/idpl/ips024.
[xxvii] Pernot-Leplay, Emmanuel, "Data Privacy Law in China: Comparison with the EU and U.S. Approaches," (blog post), 27 March 2020, https://epernot.com/data-privacy-law-china-comparison-europe-usa/.
[xxviii] Member Economies map, Asia-Pacific Economic Cooperation, https://www.apec.org/About-Us/About-APEC/Member-Economies.
[xxix] Sacks, Samm. "China's Emerging Data Privacy System and GDPR." *Washington, DC: Center for Strategic and International Studies* (2018).
[xxx] Solove, Daniel J, "A Taxonomy of Privacy," University of Pennsylvania Law Review, Vol. 154, No. 3, January 2006, https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf.
[xxxi] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles," www.privacybydesign.ca, n.d., https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
[xxxii] "Privacy By Design," graphic, Aristi Ninja, n.d., https://aristininja.com/privacy-by-design/.
[xxxiii] Cavoukian, Ann, "7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age," Information and Privacy Commission of Ontario, n.d., https://collections.ola.org/mon/15000/267376.pdf.
[xxxiv] Wadhwa, Vivek, "Laws and Ethics Can't Keep Pace with Technology," MIT Technology Review, 15 April 2014, https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.
[xxxv] ISACA webinar, Robotic Process Automation (RPA) and Audit, March 19, 2020, https://www.isaca.org/education/online-events/lms_w031920
[xxxvi] "The UX Guide for Getting Consent," IAPP, n.d., https://iapp.org/store/books/a191a000002FUZKAA4/.
[xxxvii] Schwartz, Karen D., "Data Privacy and Data Security: What's the Difference?" ITPro Today, 2 May 2019, https://www.itprotoday.com/security/data-privacy-and-data-security-what-s-difference.

[xxxviii] "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0," National Institute of Standards and Technology, U.S. Department of Commerce, 16 January 2020, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[xxxix] Ibid

[xl] "NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management," Preliminary Draft, National Institute of Standards and Technology, U.S. Department of Commerce, 6 September 2019, https://www.nist.gov/system/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf.

[xli] "The Privacy Advisor," IAPP, Vol. 10, No. 10, December 2010, https://iapp.org/media/pdf/publications/Advisor_12-10_print.pdf.

[xlii] "White Paper: GDPR, CCPA, and Beyond: How to Comply with Data Privacy Laws and Improve Customer Trust," Akamai, n.d., https://www.akamai.com/us/en/campaign/assets/whitepapers/gdpr-ccpa-and-beyond-wp.jsp.

[xliii] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions," European Commission, COM(2020) 66 final, 19 February 2020 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN.

[xliv] Ibid

[xlv] "Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data," CNIL, 6 November 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.