# PRIVACY 2020

## 10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade

DATA PRIVACY DAY 2020

FUTURE OF PRIVACY FORUM

Jules Polonetsky | CEO, Future of Privacy Forum
Elizabeth Renieris | Founder, hackylawyER

## INTRODUCTION

Data is the lifeblood of modern organizations. Data collection and uses impact society and human interactions in unprecedented ways and will only become more important in the 2020s. The processing of personal data is increasingly recognized as a human right and quickly being extensively regulated to ensure lawful, fair, and transparent practices.

The existing data ecosystem is complex and the influence of data-intensive technologies is rapidly extending. Policymakers, privacy professionals, executives, and civil society must understand the basics of these technologies in order to assess how existing and proposed policies, systems, and laws will address the risks and benefits of emerging technologies, and to support appropriate guidance for the implementation of new digital products and services.

The Future of Privacy Forum has identified ten technologies or trends that will likely create increasingly complex data protection challenges over the next decade. We also highlight ten developments that can enhance privacy and, consequently, other rights – reasons to be optimistic that organizations will be better able to manage data responsibly. Some of these technologies are already in general use, some will soon be widely deployed, and others are nascent.

Technological advances are creating data protection challenges. But ultimately, managing key issues will continue to require trained people at the center of organizations to bring the human dimension to review products and services, to assess bias, to demand fairness, and to manage the systems and tools that can handle data protection at scale.

## TEN PRIVACY RISKS TO WATCH IN THE 2020s

*Innovations in Tech Linked to Human Bodies, Health, and Social Interaction*

1. **Biometric Scanning** – The increasing use of biometric-based recognition represents a general shift away from graphical user interfaces (GUIs) that depend on a keyboard or screen to biometric-enabled UIs such as Voice User Interfaces (VUIs) and other Natural User Interfaces (NUIs). Biometric scanning is based on machine learning systems, techniques, and algorithms that collect unique biometric features to identify individuals and infer attributes about them. Examples include voiceprints (used in voice recognition technology and voice-activated devices), facial scans (used in facial characterization and facial recognition technology), behavior and gestures (recognition based on bodily movements), physiological (such as flushed skin, or heart rate), and potentially genetic information.[1] Biometric interfaces will require organizations to assess how to apply traditional data protection and privacy principles in the absence of a screen or manual device input. Development of this technology will further blur the divide between law enforcement and consumer privacy concerns. Organizations building, selling, and deploying biometric scanning technologies should also consider fairness and justice concerns, such as training data shortfalls related to lack of diversity that can create or perpetuate systemic bias. In addition, security applications relying on biometric scanning systems may need to consider their accuracy as the market for "biometric camouflage" makeup, clothing, and wearables grows.

2. **Real World Evidence** – Real World Evidence (RWE) makes use of data from mobile devices, electronic health records, claims and billing activity and other patient generated data to assess

[1] *See* 2019 Tech Trends Report (12th ed.), Future Today Institute, at 97-98 (hereinafter "FTI Trends Report").

the safety and effectiveness of drugs or medical devices.[2] To the extent that many of the data sets collected may not be protected by HIPAA, regulators and organizations will need to ensure legal protections and enforceable commitments to protect this data and assure individuals of beneficial uses.

3. **Social Credit and Reputation Scoring Systems** – These systems derive rankings about individuals from algorithms built on behavioral data gleaned from social media and web posts, including the quantity and quality of an individual's online presence, an individual's contacts, social ties and interactions, personality attributes as extracted from their online posts, and more.[3] While consumers may be aware that sharing economy services use scoring algorithms within their apps to rate both providers and users, social credit and reputation scoring systems collect data from sources that span services and platforms, sweeping in a much broader array of unexpected information about an individual. Moreover, these analyses and scores may impact a person's ability to access certain products and services, or affect pricing. The inferences and recommendations regarding the ranked or scored individual have privacy implications for both them and their contacts and will need careful scrutiny.[4] But these automated individual assessments will likely have consequences on other rights as well. Without the sort of transparency and oversight provided by traditional credit scoring laws and regulations such as the Fair Credit Reporting Act (FCRA), fairness, algorithmic transparency, and accountability are core challenges for organizations designing and deploying these new, alternative scoring systems.

4. **Internet of Bodies and Brain-Machine Interfaces** – Just as the Internet of Things (IoT) refers to a network of devices connected to or powered by the Internet, the Internet of Bodies (IoB) refers to a network of medical and biometric devices that attach to or are inside of our bodies and connected to the Internet.[5] While people have largely accepted wearables like smart watches, IoB devices may also include devices such as smart contact lenses, Bluetooth-enabled "smart pills," and WiFi-enabled pacemakers.[6] These more intimate devices raise a number of legal, ethical, and security challenges, including who should have access to the data they generate, how to mitigate the risks of malicious hacking, how to apply existing legal frameworks, and who is liable for vulnerabilities, malfunctions, or breaches. Even when looking to regulatory guidance, authority over some IoB devices between the Food and Drug

---

[2] *Statement from FDA Commissioner Scott Gottlieb, M.D., on FDA's new strategic framework to advance use of real-world evidence to support development of drugs and biologics*, FDA Statement (Dec. 6, 2018), https://www.fda.gov/news-events/press-announcements/statement-fda-commissioner-scott-gottlieb-md-fdas-new-strategic-framework-advance-use-real-world.

[3] Nizan Geslevich Packin & Yafit Lev-Aretz, *On Social Credit and the Right to Be Unnetworked*, Colum. Bus. L. Rev., 2016.

[4] *See* id.

[5] Andrea M. Matwyshyn, *The 'Internet of Bodies' Is Here. Are Courts and Regulators Ready?* via The Wall Street Journal (Nov. 12, 2018), https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566.

[6] *See id.*

Administration, the Consumer Product Safety Commission, Federal Trade Commission, or Health and Human Services (HHS) may be dependent on specific use contexts.[7]

A brain-machine interface (BMI), also known as brain-computer interface (BCI), mind-machine interface (MMI), direct neural interface (DNI), or human-machine interface (HMI), is a computer interface that can connect humans and machines by allowing people to communicate and control devices with their thoughts alone.[8] These interfaces have promising medical applications for victims of stroke and paralysis, as well as commercial applications, such as their use in autonomous vehicles as brain-to-vehicle interfaces. They raise significant privacy and security concerns, such as the risk of "brain-jacking" whereby malicious actors illicitly access wireless devices to change the implant settings, to access sensitive information about the patient, or to use the implant as a pivot point into hospital systems via less secure connections.[9] Commercial actors may also seek to pursue "neuromarketing" by using data from fMRIs, EEGs, eye tracking technology, and facial analysis to offer products, set prices, and improve ads.[10] In the future, companies may learn how to more effectively create market segments based on individuals with similar characteristics and proclivities. Environmental cues such as particular smell, or lighting controls might be provided to influence propensities, even while sleeping.[11] These kinds of activities pose ethical as well as privacy and security challenges and will require standards and guidance to protect the privacy of neural information and data derived from it.

*Innovations in Infrastructure*

5. **Automation and (Collaborative) Robotics** – While advances in software-enabled automation, digital home assistants, and simple robotics are generally available, increasingly sophisticated robots and AI-based systems are imminent. Robots that share data and code and perform computations remotely by accessing cloud-based data or systems promise greater efficiency and additional opportunities for services and collective learning across systems and platforms. An example of such "cloud robots" are semi-autonomous vehicles that access remote data for maps, real-time traffic conditions, etc.[12] Further in the future, collaborative robots or "cobots" could help other robots work more collaboratively and increase the effectiveness of robot-robot or robot-human partnerships. In such cases, it will become more challenging for existing legal frameworks to address data that is cogenerated by humans and machines, sometimes in different groups or locations. Security will be a significant concern, and organizations using cloud bots, for example, should ensure that the data is encrypted both at rest and in transit, and may also want to consider using advanced techniques such as homomorphic encryption

[7] *See id.*

[8] FTI Trends Report, *supra* note 1, at 173.

[9] Kimberley Mok, *How Brain Hacking Computer Interfaces Could Expose us to Hacking and Manipulation*, The New Stack (Dec. 25., 2017), https://thenewstack.io/brain-computer-interfaces-expose-us-hacking-manipulation/.

[10] Jonathan Pugh, *Brainjacking in deep brain stimulation and autonomy,* Ethics and Information Technology (September 2018, Volume 20, Issue 3, p. 219) https://link.springer.com/article/10.1007/s10676-018-9466-4/.

[11] Eban Harrell, *Neuromarketing: What You Need to Know*, Harvard Business Review (January 23, 2019), https://hbr.org/2019/01/neuromarketing-what-you-need-to-know/.

[12] FTI Trends Report, *supra* note 1, at 166.

to further reduce the risks posed by these models. In addition to the security risks associated with the increasing incorporation of robots and automated systems into homes and offices, there are heightened risks to privacy with the ability to collect and store more intimate information. In public, or semi-public/commercial environments informing individuals and providing controls will need creative designs beyond what is provided today. In many cases, awareness of the presence and role of AI-based systems will be critical to meeting individuals' expectations.

6. **Location Services and Proximity Tracking** – Precise location data is available via the location services on mobile devices which leverage GPS, WiFi and cell tower proximity.[13] Bluetooth beacons further assist services that determine proximity, as do the Bluetooth signals emitted by a wide range of devices such as wearables. Devices broadcast their MAC addresses, and venues can use Mobile Location Analytics (MLA) to detect how devices are moving within a space, and to identify repeat visitors. Soon, "5G" wireless technology will accommodate an exponentially expanding and complex data ecosystem by providing additional bandwidth to enable faster speeds, lower latency, and more connectivity. This technology will serve in supporting the technology for digital maps, geographic information systems (GIS), and more.[14] 5G signals have a shorter range, and so they require more numerous, smaller cellular towers, including indoors, potentially adding to the availability of location data. As these varied services come online, organizations connecting and communicating with consumers via these technologies will need a plan for complying with location data-related data protection and privacy requirements. Location data can potentially reveal sensitive information about individuals (religious beliefs related to their presence at certain worship venues, health related information revealed by presence at specific clinics etc.), mobility patterns, or aspects related to one's behavior, thus posing risks to privacy and safety.

7. **Smart Communities** – A smart community or smart city generally refers to a city or locality that integrates information communications technologies (ICT) and Internet of Things (IoT) sensors into its traditional infrastructure (e.g. roads, parks, buildings, etc.) with the aim of connecting and enhancing the lives of its citizens and providing responsive environments.[15] The importance and impact of smart cities will increase with the trend towards urbanization, as 70% of the world's population is estimated to live in cities by 2050.[16] Because of the vast amounts of data collection and consolidation possible in these wired cities, there are significant concerns about the risks to individual privacy, particularly with respect to sensitive information, including license plate tracking, facial recognition, government access to rideshare or mobility data, and deployment of a wide range of sensors that capture data in public spaces. Limited individual control and the impact of security breaches could expose people to significant risks. Private organizations participating in smart city projects or providing products and services to municipalities should consider the need for transparency, accountability, and public

[13] Matthew Kassel, *As 5G Technology Expands, So Do Concerns Over Privacy*, The Wall Street Journal (Feb. 26, 2019), https://www.wsj.com/articles/as-5g-technology-expands-so-do-concerns-over-privacy-11551236460?mod=rss_Technology.

[14] *What 5G Means for Your Business*, Networked World (Apr. 19, 2017), https://www.networkworld.com/article/3191264/what-5g-means-for-your-business.html.

[15] FTI Trends Report, *supra note* 1, at 334.

[16] *Powering Fast Forward Thinking,* The AXA 2019 Foresight Trend Book, AXA, at 8, https://group.axa.com/en/newsroom/publications/2019-foresight-trendbook.

consultation, as well as administrative and constitutional due process-related concerns.[17] Contracts should clearly determine rights and responsibilities in respect of data collection, processing, storage, demarcate points of contact, and outline how they will give effect to individual rights. Regulators seeking access to mobility data will need to consider data minimization, risks of law enforcement access to data, and re-identification due to breaches or FOIA requests. Communities should develop thorough, transparent data policies that maximize the utility of public data to residents and minimize privacy risks to individuals, while following community developed ethical standards.

*Innovations in Computing*

8. **Quantum Computing** – Quantum computing applies the laws of quantum physics to systems that process information and solve advanced computational problems.[18] Whereas classical computing uses "bits" holding a single binary value of 0 or 1, quantum computing uses "qubits" that can hold both values at the same time (known as "superposition") and can be highly correlated (known as "entanglement").[19] Quantum physics enables computing that is orders of magnitude faster, allowing for more advanced computation and better predictive analysis, with the potential to deliver breakthroughs in scientific and medical research, quantum chemistry, molecular modeling, real-time financial modeling, and advanced supply chain automation, among others. Security experts are worried about the potential ability of quantum computers to defeat modern forms of encryption relied on by existing data protection and data security practices.[20] However, quantum computers may also support new methods of encryption that are more secure.[21] Although quantum computers are unlikely to become mainstream in the near future, enterprises should at least begin to consider how they will protect information and digital assets in their transition to a post-quantum world.

9. **Spatial Computing (Augmented Reality/Virtual Reality)** – Spatial computing is a computing environment that seamlessly maps physical spaces and the people, places, and things inside of them, making digital information feel as though it is both physically present and reactive to the environment.[22] It works through a combination of technologies including video and audio sensors, 3D-capture, rendering, algorithms, and mixed-reality wearable displays that track the user's movements and relay information to the system.[23] For example, smart glasses project light directly into the user's eye to make it appear as though digital objects exists in the user's

---

[17] *See* Notice of Application, CCLA v Waterfront Toronto (Quayside), http://ccla.org/cclanewsite/wp-content/uploads/2019/04/Notice-of-Application-CCLA-and-Lester-Brown.pdf.

[18] *What is Computing?* (Microsoft), https://www.microsoft.com/en-us/quantum/what-is-quantum-computing.

[19] Daniel Wellers, *7 Innovations that could Shape the Future of Computing*, World Economic Forum (Sept. 21, 2016), https://www.weforum.org/agenda/2016/09/7-innovations-that-could-shape-the-future-of-computing.

[20] David Roe, *Quantum Computing Brings Potential and Risks to the Enterprise*, via CMS Wire (Dec. 3, 2018), https://www.cmswire.com/information-management/quantum-computing-brings-potential-and-risk-to-the-enterprise/.

[21] Larry Greenemeier, *How Close are we Really to Building a Quantum Computer?* in Scientific American (May 30, 2018), https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/.

[22] *See* FTI Trends Report, *supra note* 1, at 363.

[23] Amy Webb, *I Tested Working in a Mixed-Reality Office. It's Closer Than You Think*, via Inc. (WINTER 2018/2019 ISSUE), https://www.inc.com/magazine/201902/amy-webb/augmented-mixed-reality-virtual-workplace-magic-leap.html

physical world and surroundings.[24] These systems can collect a constant stream of user data, including everything the user sees and hears, as well as information collected and cross-referenced from applications using the system, content the user is watching or participating in, and any third-party apps or services integrated into the user experience. Design decisions regarding which data is stored locally and controls over third party apps will be essential to manage privacy issues.

10. **Distributed Ledger Technology ("Blockchain")** – A DLT, the most common of which is blockchain, is a record of verified transactions grouped into time-ordered digital entries known as blocks, which are sequenced together and verified by a digital fingerprint known as a hash.[25] The "distributed" aspect reflects the fact that the digital record (or ledger) is replicated and stored across a non-centralized network of computers, called nodes. Originally developed to create a monetary exchange system without the middlemen of banks or financial institutions, blockchain technology may be adaptable for commercial implementations, promising to facilitate "trustless" information sharing (that is, between parties that do not know each other) and immutable transaction storage. Although there are not yet any fully developed commercial applications of blockchain outside of cryptocurrency systems, proposed use cases include financial services, supply chain management, and identity management, among others. In addition to significant logistical hurdles around speed, scale, and security, public blockchains are unlikely to be compatible with data protection frameworks, due to the inability to meet requirements for rectification, erasure, and restriction of processing of personal data. Organizations seeking to leverage blockchain technology may want to undertake a privacy impact assessment, consider reducing the amount of personal data tied to the ledger, incorporate the use of advanced cryptographic and anonymization techniques, or include off-chain governance frameworks to give effect to individual rights regarding personal data.[26]

## TEN PRIVACY ENHANCING TECHNOLOGIES TO WATCH IN THE 2020s

Many of the opportunities offered by emerging technologies relate to increased speed, efficiency, productivity, commercial output, and connectivity. To the extent that these benefits rely upon more extensive collection and processing of personal data, they pose data protection and security challenges. Here are ten technological innovations and techniques that may be useful tools to manage privacy risks. At present, few of these are developed enough to be immediately transformative and each has limitations, but all are already having an impact in the market.

*Advances in Cryptography*

1. **Zero Knowledge Proofs** – Zero knowledge proof (ZKPs) are cryptographic methods by which one party can prove to another party that they know something to be true without conveying

[24] FTI Trends Report, *supra note* 1, at 284-285.

[25] Dr. Garrick Hileman & Michel Rauchs, *Global Blockchain Benchmarking Study (2017)*, Cambridge Centre for Alternative Finance, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf.

[26] We are skeptical that blockchain will have transformative business or social impact, but we include it in this paper because we believe that the drive to test blockchain related strategies will create privacy risks that could be consequential.

any additional information (like how or why the mathematical statement is true). ZKPs can be used in identity verification contexts, for example, to prove that someone is over a certain age without revealing their exact date of birth. ZKPs help with data minimization and data protection and promote privacy by design and default.

2. **Homomorphic Encryption** – Homomorphic encryption is a process that enables privacy-preserving data analysis by allowing some types of analytical functions and computations to be performed on encrypted data without first needing to decrypt the data.[27] It may be especially useful in applications that retain encrypted data in cloud storage for central access.

3. **Secure Multi-Party Computation** – Secure multi-party computation (SMPC) is a distributed computing system or technique that provides the ability to compute values of interest from multiple encrypted data sources without any party having to reveal their private data to the others. A common example is secret sharing, whereby data from each party is divided and distributed as random, encrypted "shares" among the parties, and when ultimately combined can provide the desired statistical result.[28] Compromising one share is insufficient to expose the remaining data. SMPC holds particular promise for sharing or managing access to sensitive data such as health records, but in some cases may still be vulnerable to revealing inferences about individuals.

4. **Differential Privacy** – Differential privacy (DP) is a rigorous mathematical definition of privacy that quantifies the risk that an individual is included in a data set. It leverages anonymization techniques that involve the addition of statistical "noise" to data sets before calculations are computed and results released. DP can be global or local.[29] Global DP is server-side anonymization or de-identification (where trust resides in the service provider); local DP is applied on the client or user's device. There are now differentially private versions of algorithms in machine learning, game theory and economic mechanism design, statistical estimation, and streaming. Differential privacy works better on larger databases because as the number of individuals in a database grows, the effect of any single individual on a given aggregate statistic diminishes. SMPC and DP are federated learning approaches.

*Localization of Processing*

5. **Edge computing and Local Processing** – For devices where speed is of the essence or connectivity is not constant, applications, data, and services are increasingly run away from centralized nodes at the end points of a network. Such local processing helps with data minimization by reducing the amount of data that must be collected (accessible) by the service provider, or retained on a centralized service or in cloud storage.

---

[27] *See* David Wu, University of Virginia Computer Science Department, available at https://www.cs.virginia.edu/dwu4/fhe-project.html.

[28] *See* Christopher Sadler, *Protecting Privacy with Secure Multi-Party Computation*, New America (Jan. 11, 2018), https://www.newamerica.org/oti/blog/protecting-privacy-secure-multi-party-computation/.

[29] Evaluation of Privacy-Preserving Technologies for Machine Learning, Outlier Ventures Research (Nov. 2018), https://outlierventures.io/research/evaluation-of-privacy-preserving-technologies-for-machine-learning/.

6. **Device-Level Machine Learning** – New machine learning focused semiconductor components and algorithms — along with the speedy, low-cost local storage and local processing capabilities of edge computing — are allowing tasks that used to require the computing horsepower of the cloud to be done in a more refined and more focused way on edge devices.

7. **Identity Management** – Many identity management solutions under consideration or development leverage a variety of platforms, including distributed ledger technology (described previously), and local processing, that capitalize on device-level machine learning to provide the ability for individuals to verify and certify their identity. This enables people without internet access beyond smartphones or other simple devices to form secure connections, exchange identity-related credentials (such as transcripts or voting records) without going through a centralized intermediary. Verified personal data can be accessed from the user's device and shared via secure, encrypted channels to third parties, with data limited to the basic facts necessary for the relying party (e.g. that the individual is over 21, or does in fact qualify for a specific government service) on an as-needed basis. Depending on the implementation and standards, identity management can create privacy risks or can be deployed to support data minimization and privacy by design and default.

*Advances in Artificial Intelligence (AI) & Machine Learning (ML)*

8. **"Small Data"** – Small data AI and machine learning systems use significantly less, or even no real data, via techniques such as data augmentation (manipulating existing data sets), transfer learning (importing learnings from a preexisting model), synthetic data sets (see below), and others.[30] With small data techniques, the future forms of AI might be able to operate without needing the tremendous amounts of training data currently required for many applications.[31] This capability can greatly reduce the complexity and privacy risks associated with AI and ML systems.

9. **Synthetic Data Sets** – Synthetic data sets are sets of artificial data created to replicate the patterns and analytic potential of real data about real individuals or events by replicating the important statistical properties of real data.[32] They can be created at a vast scale and reduce the need for large training or test data sets, particularly for AI and ML applications, and thus support reduced data sharing or secondary use concerns.

10. **Generative Adversarial Networks** – Generative Adversarial Networks (GANs) are a type of artificial intelligence, in which algorithms are created in pairs (one to "learn," and the other to "judge"). Used in unsupervised machine learning, two neural networks contest with each other in a framework to produce increasingly better simulations of real data (e.g., creating faces of people, or handwriting). One valuable use: generating synthetic data sets.[33]

---

[30] Harsha Angeri, *Small Data & Deep Learning (AI): A Data Reduction Framework*, Medium (Apr. 1, 2018), https://medium.com/datadriveninvestor/small-data-deep-learning-ai-a-data-reduction-framework-9772c7273992.

[31] H. James Wilson, Paul R. Daugherty, Chase Davenport, *The Future of AI Will be About Less Data, Not More*, Harvard Business Review (Jan. 14, 2019), https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more.

[32] Applied AI, *Synthetic Data: An Introduction & 10 Tools*, (June 2018 update), https://blog.appliedai.com/synthetic-data/.

[33] Dan Yin and Qing Yang, *GANs Based Density Distribution Privacy-Preservation on Mobility Data*, Security and Communication Networks, vol. 2018, Article ID 9203076, (Dec. 2, 2018), https://doi.org/10.1155/2018/9203076.

These tools and resources can potentially help mitigate data protection concerns posed by future technologies. The broader market for compliance tools for privacy and security professionals continues to accelerate and includes a wide range of legal, technical and policy tools and will be the subject of our next report, jointly with the Privacy Tech Alliance. Services that discover, map, and categorize data for organizations, wizards that help manage and complete privacy impact assessments, programs that handle data subject access requests and consent management, and de-identification services are already supporting privacy and security professionals at leading organizations as well as attracting investor interest. Data protection resources entering the market are increasingly central to building systems that allow professionals to manage the challenges that accompany the expanded data collection and the multiplying uses.

### SHORT TERM

**Browsers, Operating Systems and Platforms -** Much of the important digital activity today takes place on top of technology structures operated by a number of leading companies. Access to data is enabled or restricted by decisions those organizations make and the technical or contractual requirements they establish. The last few years have been marked by these platforms implementing a host of restrictions, due to a range of reasons including regulatory pressure, media and consumer backlash due to well publicized scandals such as Cambridge Analytica, and browser and operating system competition. It is notable that as of January 2020, every leading browser has strictly limited or committed to limit most third party cookie tracking, a staple of today's data ecosystem. We expect a continued pivot to privacy as these companies compete in sectors such as cloud, smart city, automotive, education, health, payments and other areas that are highly regulated or where data and trust expectations are not compatible with the broad data sharing of ad tech.

## CONCLUSION

The digital world is entering a qualitatively different era, marked by tremendous advances in the kinds and quantity of information and inferences collected and the contexts in which the data is generated and used. Major shifts in user experiences and user interfaces (UX/UI) are adding amazing possibilities, but also adding complexity and challenges. The nature of the data ecosystem is more interactive, more pervasive, and more encompassing, which means that the ex-ante design of products and services, as well as ongoing assessments and calibration, are absolutely essential to enable effective data protection and provide acceptable privacy controls and outcomes for individuals. Organizations should explore and embrace advances in cryptography, evolving data minimization and analysis techniques, and small data/local processing trends to sufficiently mitigate risks. With a focus and strategy for data stewardship, organizations can make careful decisions about the benefits and risks of new technologies, as well as the required safeguards.