JUNE 2021

Privacy Tech's Third Generation

A Review of the Emerging Privacy Tech Sector

Privacy Tech Alliance

FUTURE OF PRIVACY FORUM

AUTHORED BY

Privacy Tech Alliance and Future of Privacy Forum

with

Tim Sparapani and Justin Sherman

The Future of Privacy Forum launched the **Privacy Tech Alliance (PTA)** as a global initiative with a mission to define, enhance, and promote the market for privacy technologies. The PTA brings together innovators in privacy tech with customers and key stakeholders. Privacy Tech companies can apply to join the PTA by emailing **PTA@fpf.org.**

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting **fpf.org.**

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The privacy technology sector, until recently composed of relatively small startups focused on providing consumer data privacy regulatory solutions for businesses, is at an inflection point. The sector is rapidly maturing and expanding both in terms of the number of vendors and the products and services those vendors offer. Business customers increasingly are seeking privacy tech partners that provide easily integrated solutions to all of a business' data needs, and vendors are moving rapidly to meet this demand. This report is a review of that market, focused on current developments and progress. It also identifies misalignments within the market; trends in the future of privacy technology; and recommendations to address current challenges.[1]

The report offers a privacy "stack" typology for analyzing and understanding the privacy tech market today. It suggests that privacy tech has evolved through three main phases into the Privacy Tech 3.0 landscape seen now. The field started with an initial phase of privacy and security tech industry technology ideation and vendor formation (Privacy Tech 1.0), and then developed into a privacy and data security privacy tech landscape of technologies built natively within large companies, as well as increasingly sophisticated privacy tech vendors offering their services chiefly to support privacy regulatory compliance (Privacy Tech 2.0). Now the field has started to develop into a new state involving niche privacy tech vendors offering an essential or bespoke tool or technology for sale, and horizontally-integrated vendors or joint ventures between providers that offer tools for regulatory compliance and tools to maximize control over and the availability and value of personal data held by a business (Privacy Tech 3.0).[2] This report explains this typology and describes a taxonomy of terms and relationships to provide a consistent understanding of customer needs and privacy tech offerings commonly associated with this privacy stack.

Second, this report provides an analysis of market dynamics around privacy tech—from buyer and seller perspectives—in addition to a description of trends and predictions. The report's authors found striking consensus about the direction of the privacy tech industry, potential impediments to its growth, likely drivers of future acceleration, and recommendations for industry-led efforts to eliminate those impediments. Sophisticated providers of privacy tech and sophisticated purchasers of privacy tech identified as a major obstacle the lack of common privacy vernacular to define terminology and the inconsistent typification of the so-called privacy stack, i.e., the technologies that were core to the privacy technology industry.

Finally, this report identifies five market trends and seven implications those trends hold for the future of the privacy tech market. It then lays out a work plan of recommendations to facilitate the growth and maturation of the privacy tech industry.

This report does not address the market for cybersecurity services or identity services. Although many of these vendors provide services often described as privacy related, they serve a different market purpose. It also does not cover the growing number of business-to-consumer services which seek to help consumers request their data, monetize their data, or perform other consumer-driven functions with respect to data.[3]

OVERVIEW OF CONCLUSIONS

To research this report, the authors conducted more than 30 hours of interviews with dozens of the world's leading experts on the privacy tech market, including buyers of privacy tech services and sellers of privacy tech services. These interviews yielded important insights on the state of the privacy technology market from leading thinkers and industry participants. Several clear themes emerged on key issues, allowing us to offer the following conclusions and recommendations:

- The COVID-19 pandemic has globally accelerated marketplace adoption of privacy technology as individuals and organizations worldwide became more heavily dependent on digital technologies and services. It is unclear if this is a one-off event or a growth pattern that will sustain, but increased purchasing of privacy tech is clear.
- Common drivers of initial privacy technology purchases are regulatory compliance needs, contractual requirements with customers, and slowly emerging recognition of the reputational risks associated with data privacy breaches, broadly defined. These initial drivers often lead purchasers of privacy tech to explore other opportunities to deploy additional privacy tech offerings. Regulations by and large remain the biggest driver for privacy technology adoption, but the others are growing in importance to the extent that privacy is becoming a competitive differentiator in some sectors. Organizations are also deploying additional tools to mitigate potential harms caused by the use of data.[4]
- While jurisdictions in the US and around the globe have incorporated key concepts from other jurisdictions' consumer privacy regulatory schemes into their own, the privacy landscape is expected to become more complex and less homogenous as jurisdictions begin to diverge and increase regulatory complexity.
- Common privacy terms, including those included in statutes or regulations, are not uniformly defined or understood.
- The lack of common understanding about privacy terms is limiting the growth of the privacy tech industry. With respect to some privacy tech offerings, it is unclear whether vendor-developed privacy tech is sufficient to satisfy the regulatory compliance or business needs of would-be purchasers.
- In addition to lacking a common vernacular to describe privacy tech, there is no commonly accepted methodology for characterizing what technologies and services are part of the privacy technology industry or the so-called privacy stack. Many interviewed for this report, from both the sell-side and buy-side, agreed that it would be useful to classify privacy tech companies by the "business needs" their offerings satisfy.
- The lack of common vernacular and inconsistent typology for the privacy stack may also be causing some misalignment between the privacy tech available in the market and the needs of buyers.
- The leading edge of the market has passed through two initial stages of privacy tech and has entered a third. The first stage was typified by technologies engineered natively within some companies and offered by early vendors for sale to achieve a modicum of control over the personal data processed by a business (Privacy Tech 1.0). The second stage was the development of technologies engineered natively within large companies well-resourced enough to devote engineering capabilities to regulatory compliance solutions and horizontally-integrated companies or collaborations between companies offering personal data regulatory compliance services and tools for sale (Privacy Tech 2.0).
- Recently, privacy tech offerings are expanding well beyond products and services that assist in regulatory compliance into products and services that assist businesses in making the personal data they encounter both maximally available and maximally valuable for business services (Privacy Tech 3.0). For example, privacy tech

OVERVIEW OF CONCLUSIONS

tools are increasingly available to assist with business needs across the business enterprise, serving: (i) CIOs in making personal information accessible; (ii) CMOs in making personal information available for marketing and advertising; (iii) Chief Data Scientists in unlocking new insights from personal information; and (iv) CISOs in securing data; etc.

- Because we have entered the Privacy Tech 3.0 market phase, the key buyers of privacy tech within many large companies have shifted from the Chief Privacy Officer (Privacy Tech 1.0), to the General Counsels, Chief Information Security Officers, and Chief Technology Officers (Privacy Tech 2.0), to the Chief Marketing Officers, Chief Strategy Officers, and Head Data Scientist (Privacy Tech 3.0). The individual who continues to have the budget for software purchases tends to be the Chief Technology Officer, despite these changes. The Chief Privacy Officer continues to be an influencer of these purchases, but should recognize this development as a call to embrace the skills and scope of responsibilities to maintain a leadership mandate.
- For many companies, especially small- or medium-sized businesses and those that tend to serve only one regulatory market, Privacy Tech 2.0 or even 1.0 solutions may be sufficient to meet their needs. However, buyers serving global markets increasingly need to build or buy privacy tech that supports controls, regulatory compliance, and data availability and value. In short, while the market for privacy tech is maturing there is evidence of market segmentation between buyers, and the most sophisticated companies will need all three evolutions of privacy tech solutions.
- Buyers of privacy tech often prefer to buy integrated privacy tech products that accomplish numerous business needs rather than one-off, standalone privacy tech solutions. The exception to this rule is when a privacy tech vendor offers a "breakthrough" or "highly innovative" technology or service, which can justify a contract with a vendor for just one niche product or service.
- Because of buyers' increasing preference to buy horizontally-integrated privacy tech services, better-resourced privacy tech companies with numerous, fully developed tools and services are leading current market share.
- There is evidence of companies attempting to provide horizontally-integrated services as many privacy tech vendors add new features. However, companies that offer Privacy Tech 3.0 services focused on maximizing data value within regulatory limits are also increasingly providing offerings in the Privacy Tech 1.0 and Privacy 2.0 services to compete with traditional privacy tech vendors.
- This buyer preference for horizontally-integrated privacy tech services may lead to industry consolidation in the near term. For example, recently, some privacy tech companies have merged or acquired rivals or providers of adjacent privacy tech products. Further, some private equity companies appear to be "rolling up" privacy tech startups into larger offerings. Some providers are employing a third strategy of formally entering into partnerships, joint ventures, cross-selling, or similar collaborations. It is perceived by some that niche providers may increasingly struggle unless they are able to offer an entire suite of services.
- While the privacy tech market and privacy vendor strategy for ensuring longevity and growth is undergoing transformation, there is striking consensus about the determinative factors of how buyers choose whether to buy or build privacy tech. Our surveys found commonality among respondents about who in the corporate organizational structure often has the budget to purchase privacy tech, who in that structure identifies the business needs to be

OVERVIEW OF CONCLUSIONS

met by privacy technologies, and who must be consulted for successful privacy tech contracts to be signed.

- Some purchasers expressed concerns about the "lock-in" effect of buying any privacy tech solution. In other words, some admitted they might not make a purchase for fear that doing so might lead their companies to be beholden to that vendor for numerous, future budget cycles even if better, competitor technologies emerge or the enterprise needs change.
- Market differentiation is important for small- or medium-sized buyers of privacy tech when compared to large scale enterprises. Small- and medium-sized buyers may be operating with smaller budgets and organizational structures. They may also rely on information technology infrastructure that differentiates their privacy tech needs from those of larger enterprise buyers.
- While large enterprises are significant purchasers of privacy tech services, many of the largest tech companies have the scale, unique needs, and engineering capacity to build privacy tech natively and as such purchase fewer services from privacy tech vendors.

OVERVIEW OF RECOMMENDATIONS

- Privacy tech stakeholders should develop and promote voluntary, shared, consensus-driven vernacular in the privacy technology market for the benefit of both buyers and sellers. Consensus definitions should then be used to facilitate developing a common typology for descriptions of the tools and services developed natively or made available for sale in the privacy tech marketplace.
- A trusted body should provide common definitions and standards for privacy enhancing technologies (PETS) such as differential privacy, homomorphic encryption, federated learning, and similar technologies, and should indicate the maturity and utility of these technologies for different business cases, as well as to how the uses of these PETS map to legal requirements.[5]
- Further research should be conducted to identify market segmentation and stratification in buyers based on the size of the corporate entity, the sophistication of the buyer, the industry sector, and other factors.
- Further research should explore what unique needs, if any, small- or medium-sized enterprises may have relative to those of large enterprise buyers of privacy tech.
- Future research might also explore whether the needs for privacy tech solutions differ between industry types in a meaningful way.
- Future research might also consider whether businesses that solely or primarily interact with the personal data of individuals from just one country or region have different privacy tech interests and needs than do businesses interacting with personal data on a multinational level.
- Vendors should recognize the need to provide adequate support to customers to increase uptake and speed time from contract signing to successful integration. Buyers will often underestimate the time needed to integrate privacy technologies and services into their existing business operations and may therefore need further assistance in realizing that integration.

INTRODUCTION

Countries around the globe are advancing regulations that put in place comprehensive requirements for the processing of personal information. The European Union's General Data Protection Regulation (GDPR) went into effect in 2018[6] and established extensive requirements on private and public sector entities providing services to data subjects in the EU, such as requiring a legal basis for processing data, registers of data processing, data protection impact assessments and balancing tests, consent management, privacy by design and making data available for access, deletion, and correction. The GDPR has proved to be a spur for global regulation, with numerous countries adopting legislation influenced by the GDPR or updating current laws to maintain or achieve an adequacy determination by the European Commission that supports international data transfers. Major markets such as India, China, Brazil, Japan, South Korea, and Canada have been particularly active. At the very end of 2019, India published a draft law that would update that nation's privacy laws. During the drafting of this report, Brazil finalized its consumer privacy regulation,[7] and both China and Canada published draft consumer privacy laws.[8] South Korea and Japan have updated legislation as part of adequacy negotiations with the EU.

In the US, California in 2018 passed the California Consumer Privacy Act (CCPA).[9] Just months after finalizing regulations implementing the CCPA, California voters expanded the law via a ballot initiative to further establish privacy requirements for businesses, seeking to incorporate protections inspired by the GDPR.[10] In 2021, Virginia passed legislation with similarities to the California Privacy Rights Act (CPRA), enhanced by consent requirements for sensitive data but greater flexibility for advertising.[11] Massachusetts, Nebraska, New York, Florida, and Washington, Connecticut and Colorado are just a few of the states that have extensive activity around data protection legislation.[12] As of the spring of 2021, Congress has yet to act, but consumer data privacy law proposals have been set forward in the Senate Commerce Committee, the leading committee of jurisdiction in that body, and the leaders of the House Energy & Commerce Committee have promised to develop a proposal. Further momentum is evidenced by the introduction of additional, comprehensive regulatory proposals by other influential members in each body. The Federal Trade Commission has traditionally avoided rulemaking due to the rulemaking constraints the agency faces, but has recently indicated that it is ready to advance a rulemaking effort in support of privacy requirements, in the absence of Congressional action.[13]

To support this rapid regulatory explosion, the "privacy technology" market is growing rapidly around the world. New or improved technologies are advancing in the market to support de-identification, privacy impact assessments, consent agreement design, data pipeline management, and similar techniques that are becoming essential to a business' regulatory compliance strategy. Meanwhile, emerging techniques like differential privacy, used to assess mathematical guarantees of disclosure control for a particular privacy model, are becoming commercialized as well. Venture capital firms are investing in the privacy sector,[14] encapsulating a global trend that follows a market demand for privacy technologies driven by the GDPR and the CCPA.[15] All told, privacy technology is a nascent market but a growing one, and will continue to expand as privacy becomes a more important part of regulatory compliance, business competitiveness, and consumer trust around the world. It is for this very reason that in 2019, the Future of Privacy Forum and the Israel Tech Policy Institute established the Privacy Tech Alliance, bringing together privacy innovators, academics, governments, and companies with interest in privacy technology's growth.[16] The International Association of Privacy Professionals has rapidly grown to 70,000 members, and new conferences have emerged to serve technology and engineering sectors of privacy, such as PEPR (Privacy Engineering Practice and Respect) and The Rise of Privacy Tech, joining long established technology or research focused conferences.[17]

Despite all this, however, there are few comprehensive examinations of this "privacy technology" marketplace. Limor Shmerling Magazanik, managing director of the Israel Tech Policy Institute, frames this as a problem of developing bridges to close existing gaps.[18] In other words, there is a need to assess and evaluate gaps, misalignments,

INTRODUCTION

and misunderstandings that may exist between buyers looking for privacy technologies to meet their needs—whether small- or medium-sized businesses or large enterprises with significant amounts of user data and information technology infrastructure—and the sellers offering those privacy technologies to said firms. Mapping out these gaps, misalignments, and misconceptions can help buyers, sellers, and policy analysts working in or observing the space to better understand where the market is today; where the market is headed; and how these technologies impact a business' compliance with privacy regulation increasingly put into place around the world.

Written over the course of five months, this report presents a mapping of the privacy technology marketplace, the involved buyers and sellers, and the gaps, misalignments, and misconceptions at play. It focuses on privacy technologies and does not focus on cybersecurity technologies. The report introduces this mapping of the market by drawing on a literature review, interviews with numerous experts in the privacy technology space, a survey of companies operating in the market (attached in the appendix), and the authors' own subject matter expertise on these issues, and it does so in several parts.

- First, it introduces the global growth of the privacy technology market. Second, it discusses specific regulations driving privacy technology adoption by businesses.
- Third, it discusses the lack of shared vernacular to discuss privacy technologies and the privacy technology industry. Fourth, it introduces a privacy "stack" typology, broken into three layers, that serve as both a lens of analysis and a contributing solution to the problem of shared vocabulary. Fifth and sixth, respectively, it applies this typology to the buy and sell side of the market, combined with interviews with subject matter experts, to capture gaps, misalignments, and mis-incentives in the privacy tech industry today.
- Seventh, it lays out five market trends and seven implications for the future of the market identified in the course of this report's research. And finally, it concludes with numerous observations about the privacy tech industry today and a set of recommendations to address current and emerging challenges.

Global Growth of the Privacy Tech Industry

A "staggering 48,337.2 percent three-year growth rate" is what propelled *Inc. Magazine* to put privacy tech vendor OneTrust on the cover of their September 2020 issue and name them #1 on their Inc. 5000 list for 2020.[19] While *Inc.* focused on OneTrust in September, this prominent acknowledgement could just as easily have signaled the profound growth of the privacy tech industry as a whole. Initially created by computer engineers within companies who were wrestling with the personal data passing through their systems, working to assume a modicum of control over the privacy and security of that data, initial privacy tech solutions were turned into companies to offer these solutions to other businesses as a service. These initial companies offered products and services to help companies achieve fidelity with their privacy and security commitments in their public-facing privacy policies, or to meet contractual requirements imposed by larger companies with which they wanted to do business.

Many new privacy tech vendors then arose, propelled forward by the European Union's drafting of its then-forthcoming General Data Protection Regulation and by legislators in California modifying Alastair Mactaggart's ballot initiative into legislative language for what became the California Consumer Privacy Act. This included a number of providers offering privacy enhancing technologies (PETs) to help clients with de-identification, including homomorphic encryption, and more sophisticated uses of differential privacy, among others.[20] Alongside these new entrants into the market, existing vendors grew their offerings to help achieve privacy regulatory compliance. Gartner predicted in February 2020 that over 40% of privacy technology vendors will use artificial intelligence by 2023, which could help reduce administrative and manual workloads while enabling business use of data.[21]

"Organizations should explore and embrace advances in cryptography, evolving data minimization and analysis techniques, and small data/local processing trends to sufficiently mitigate risks."

— Jules Polonetsky and Elizabeth Renieris, *10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade*[22]

Recognizing this growth, 14 companies joined together in December 2019 to establish the Privacy Tech Alliance to represent the leading edge of this global growth.[23] Since that gathering, the industry's growth has continued to accelerate. Several experts surveyed for this report pointed to decisions by the European Court of Justice invalidating the EU-US and Swiss-US Privacy Shield agreements (the so-called Schrems II decision) and the demands of other C-Suite executives within businesses to use personal data profitably for a myriad of needs, such as training machine learning and artificial intelligence systems, fine tuning marketing efforts, analyzing data to find unforeseen connections or make predictions, or speed sales. When new tools and services from niche, cutting-edge privacy tech vendors are added to these other, existing lines of business and the number of privacy regulations around the world grows seemingly by the month, it is unsurprising to see the "staggering" growth of the kind described by *Inc.* in the fall of 2020.

Unforeseen and unforeseeable by those gathered to establish the Privacy Tech Alliance was the sudden arrival of a worldwide pandemic forcing billions to adjust their entire lives and carry on their normal life, schooling, business, and recreation activities online to the extent possible, all while producing previously unimaginable amounts of personal data. As the privacy tech industry has discovered, while this has been damaging to so many businesses, this pandemic has been catalytic for industry growth by forcing adoption of privacy tech tools by companies of all sizes in various markets. The reasons are perhaps intuitive: "Now, all the employees are online, all the customers are online, all the business processes are online; everything has to be virtual and digital," one vendor told the authors. While the catalyst for the acceleration of adoption of privacy tech was unforeseen by vendors of privacy tech, those vendors are universally convinced that the growth of the industry is not merely temporary or likely to slow. Experts surveyed pointed to the desire by many businesses to simultaneously demonstrate the accuracy of their privacy policies, comply with regulations, and use their personal data for new business purposes, such as training artificial intelligence or fine tuning marketing.

Specific Regulations Driving Growth of Industry

During the last decade, numerous privacy tech vendors formed companies in response to regulatory mandates that created tech needs by updating or overhauling consumer privacy regulations or legislation. For example, consent management tools such as Privo, Yoti, PrivacyCheq, Onano, and SuperAwesome had arisen to address long-standing parental consent requirements for businesses wanting to collect the data from minors younger than 13 years of age, in compliance with the US Children's Online Privacy Protection Act (COPPA). These tools became even more widely needed with the May 2018 implementation of the European Union's General Data Protection Regulation Article 8. "You see the biggest blip in privacy activity and demand right before a regulation comes into effect," one expert interviewed for this report said, "and after that you see kind of a huge drop-off." Both the GDPR and the recent enactment of the California Consumer Privacy Act and their creation of data subject rights have spawned a myriad of data mapping tools and companies.

As detailed within this report, venture capitalists and private equity funders are recognizing these various drivers of growth and investing more often and in greater dollar amounts in privacy tech startups, providing seed funding to the most recently conceived companies through enormous follow-on investment rounds with later-stage established privacy tech vendors.

Lack of Consensus Privacy Tech Definitions Limiting Growth of Privacy Tech Industry

Despite the development of the privacy tech market and its trajectory for accelerating future growth, interviewees for this report identified two impediments to the industry's growth that are slowing both the speed of closing sales contracts and the adoption of privacy tech by customers. The impediments repeatedly identified by those interviewed are: (i) a lack of common, consensus privacy tech definitions; and (ii) an unclear privacy stack typology to describe business needs and how the various privacy tech tools and services available in the marketplace might map to meeting those business needs. Both impediments were challenging to vendors and would-be purchasers of privacy tech, but together they create compounding difficulties that are limiting privacy tech adoption.

First, because the privacy technology market is relatively nascent, there is no clear set of shared terminology used by buyers and sellers in the market. On the buyer side, for instance, three medium-sized businesses in search of privacy technology might all use the term "data mapping" to describe their functional needs to vendors, while meaning completely different things in each case. On the seller side, to give another example, multiple companies might brand their products with similar terminology when in fact their privacy technology offerings meet very different client needs. Though there are many other examples: companies might talk past one another when using the same terminology; some companies, particularly those newer to privacy technology, may lack the terminology needed to specifically describe their needs or offerings; and other companies yet might internally speak different languages when describing how privacy technologies could meet their business needs. "Most lawyers don't get tech, and most technicians don't get law, and so it's not that they necessarily want to battle, but they do," one vendor told the authors. "They don't listen to each other, and even when they talk to each other, they use different words for the same thing." Further, another vendor said, this shared vocabulary problem is driven by company self-marketing as well: individual firms that "plant a flag, create a category" and then "try

and actually identify the people you want in that category and then obviously try and push out the people you don't" for competitive purposes. This lack of shared terminology simultaneously reflects and contributes to gaps, misalignments, and misunderstandings between buyers and sellers about regulatory compliance needs, privacy technologies on the market, and how the two fit together in the context of companies' existing data, technologies, and business processes.

The lack of consensus definitions creates numerous business problems. On a basic level, this creates a problem as old as contracting itself in which a buyer and seller may not reach a meeting of the minds about what is being offered and what is being obtained in any privacy tech contract. This leads to lengthy delays and multiple extra turns before contracts could be consummated to purchase privacy tech services. One expert interviewed suggested that this unnecessarily slowed the time to closure of any contract by adding numerous logistical and legal hoops before even getting to the integration of the privacy tech services into the business' information technology environment. Buyers may not be able to certify that they are meeting requirements imposed through contract by their own customers. Buyers may not have conviction that any privacy tech obtained from a third-party satisfies regulatory, statutory, or judicial requirements.

While it was clear there were not yet consensus definitions, consensus was clear among those interviewed that collective action should be taken between privacy tech vendors, perhaps working with organizations that can convene stakeholders from all sides of industry, academia, and key non-governmental organizations, to develop consensus definitions. "Future of Privacy Forum," one vendor told the authors unprompted, "could be absolutely the place to develop such a vocabulary." Some of those interviewed would go further and utilize standard-setting bodies to further confirm legitimacy on definitions developed in common, and other interviewees were eager to see any definitions ratified by privacy regulators, legislative bodies, or courts to provide the privacy tech industry with greater certainty; turning to the National Institute of Standards and Technology (NIST) in the United States was just one example provided by a vendor.[24]

The Privacy Technology "Stack"

The problem of a lack of consensus privacy tech definitions is compounded by a secondary problem, which is that not only may buyers and sellers of privacy tech be using the same words, terms, and phrases to mean different things, but they may be contemplating the use of privacy tech for very different purposes than what was intended due to evolving needs of the business customers purchasing privacy tech solutions. In short, and as discussed in further detail throughout this report, some businesses are seeking privacy tech that allows them to do more than simply control personal data, or control personal data and comply with data privacy and security regulation. Now, many businesses may be intending to obtain from privacy tech vendors tools and services that simultaneously allow their businesses to control personal data, comply with a myriad of regulatory mandates concerning that data, and extract value[25] from that data. This maturation of privacy tech customer needs has, according to many interviewed for this report, caused extra confusion between buyers and sellers that requires not only the creation of consensus definitions but also a new understanding of the "privacy stack."

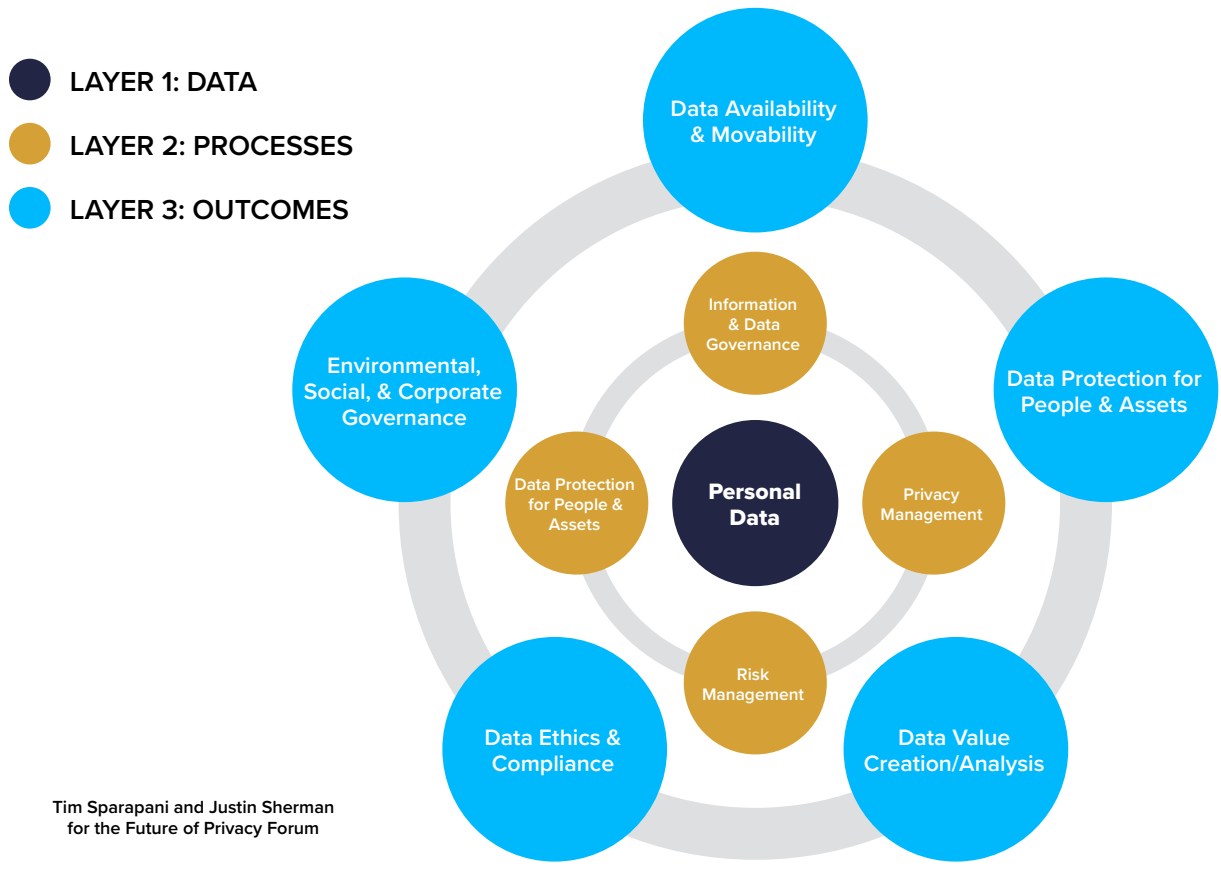
This report section therefore introduces a typology for privacy technologies aimed at tackling this challenge. The purpose is to address a lack of a clear framework and clear set of shared vocabulary with which buyers and sellers can analyze and discuss the privacy technology market. The purpose is also to link together business *processes* that companies perform with business *outcomes* that companies desire to achieve with privacy technologies. After all, as one vendor put it to the authors, "You don't collect and store data to just keep it—you're doing it to use it."

By no means is this the only framework that has been introduced to understand the privacy technology market: the International Association of Privacy Professionals, for example, published a typology of privacy technologies in 2019, broken down into privacy technologies for "privacy program management" and those for "enterprise privacy management." Within each of those categories, the IAPP report then broke down privacy technologies by actions firms might need to take (e.g., "data mapping", "website scanning").[26]

Rather than focus entirely on specific technologies or functions, however, the typology introduced in this report focuses on business process and business outcomes. It does this for several reasons. First, numerous buyers and sellers with whom we spoke conveyed experiencing or encountering confusion in the market with how privacy technologies plugged into existing business operations.[27] There can be too much focus on single technologies or discrete business needs in ways that obscure the broader goal of using privacy tech to fuse processes with desired outcomes. Second, small- and medium-sized businesses may have different technology needs than large enterprises, and they may have very different information technology infrastructures (e.g., smaller firms outsourcing their data to a third-party cloud provider versus larger firms running their own servers in-house). This can further fragment the terminology used by buyers and sellers to discuss privacy technology, including because it does not adequately include a focus on the unique buyer's existing processes. And third, in the future, existing privacy technologies might evolve, market demand for now-emerging privacy technologies might grow, and innovators could develop privacy technologies that do not yet exist. While any set of terminology will have to be reassessed if not updated as the privacy tech market matures, focusing a typology on business outcomes rather than on specific technical solutions might help create a terminology with more longevity.

The privacy "stack" for understanding the privacy technology market is composed of three "layers" (see diagram on previous page). The first and innermost layer is personal data itself. When a business is using privacy technologies, the center is data—and the key questions focus on the basics: what data fields are available, categorization, storage and access details. The earliest privacy technologies were either built natively within companies or purchased by the earliest vendors

The Privacy Technology "Stack"



Tim Sparapani and Justin Sherman
for the Future of Privacy Forum

in the market—and were typified by systems that attempted to help businesses simply gain control over the personal data they encountered as part of their business. For example, in addition to siloing personal data from information about individuals not requiring protection, these technologies may have segmented out "sensitive data" for additional control features, or simply provided consumers with adequate notice to help a business achieve requisite consent to collect that personal data. The second and middle layer is composed of four business processes: information and data governance; privacy management; risk management; and privacy operations. Privacy technologies can pair with or enable business processes at this layer, stacking on top of the personal data a business accesses (the first layer). These processes all interact and interrelate, and they may also be in constant evolution; for instance, risk management is not an action performed just once. Finally, the third and outermost layer is composed of five business outcomes: data availability and movability; data protection for people and assets; data value creation/analysis; data protection components of ethics and compliance[28]; and environmental, social, and corporate governance. Privacy technologies, stacked on top of and integrating with business processes (the second layer), can enable the business outcomes at this layer. Privacy technologies can also enable these five outcomes to interrelate and interconnect, and, ideally, to coexist simultaneously: so that data value analysis/creation and ethics and compliance are not mutually exclusive, for example. The layers of the "stack" are described in more detail below.

Data is the foundation of any privacy discussion. Depending on the legal jurisdictions in which a business operates, terms such as "sensitive data," "personal health information," or "personally identifiable information," among others, may have particular importance for a business in the first-layer, early stage of assessing their privacy technology system: they will guide legal and regulatory compliance and possibly contractual compliance as well.[29] Businesses may collect, analyze, store, or move data on customers, employees, contractors, and innumerable other actors (clients, prospective customers, etc.) with which the business interacts. Individuals are the center of this data, and it is their privacy that is concerned when businesses collect, store, and process their information.

Layer #1 of the Privacy Tech "Stack"

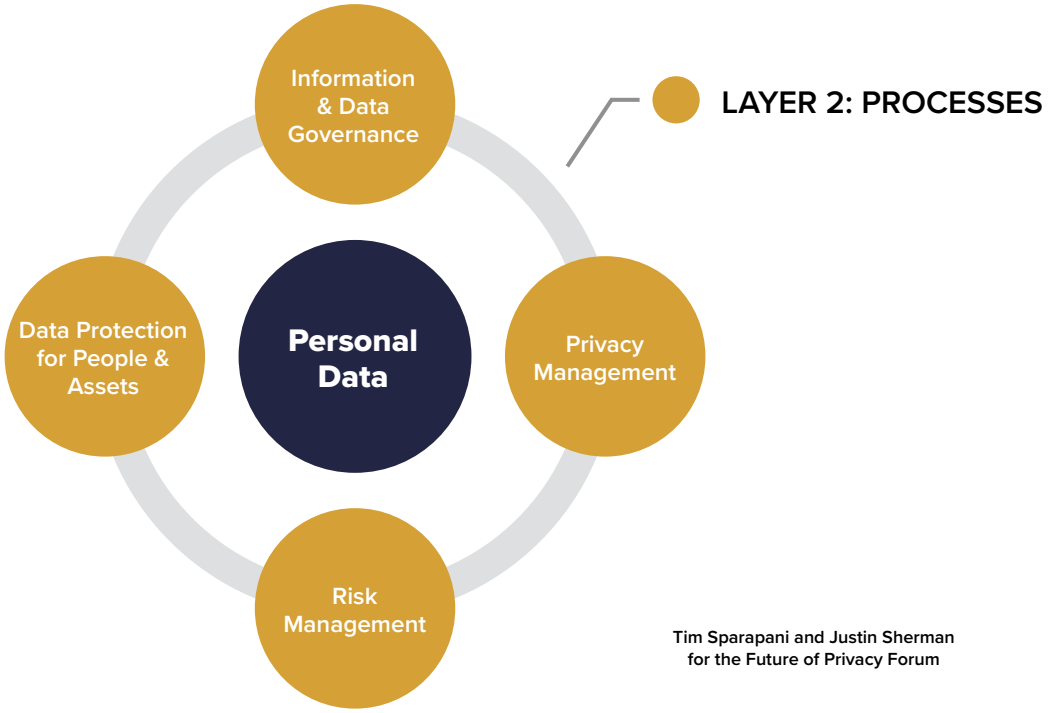
Privacy Tech 1.0: Focus on Data Control

Tim Sparapani and Justin Sherman
for the Future of Privacy Forum

The second layer of the privacy tech "stack" is composed of business processes that can be supplemented or enabled by privacy tech offerings. For example, a business might build or purchase a technology to generate data privacy compliance assessments, as part of the business' existing privacy and risk management processes, or a business might build or purchase data access control technologies to limit employee access to customer data, as part of the business' information and data governance processes. This layer is stacked on top of the business' data, which may be subject to privacy requirements based on contractual requirements, regulatory requirements, legal requirements, business reputational goals, and other factors.

Layer #2 of the Privacy Tech "Stack"

Privacy Tech 2.0: Focus on Regulatory Compliance



Tim Sparapani and Justin Sherman
for the Future of Privacy Forum

There are four business processes in layer 2 of the privacy stack.

LAYER 2 PROCESS	PROCESS DESCRIPTION
Information and data governance	Developing internal rules, protocols, and procedures for the collection, handling, transfer, storage, and analysis of data
Privacy management	Developing processes, procedures, knowledge bases, and other toolkits for internally assessing privacy of data
Risk management	Developing internal rules, protocols, procedures, and strategies for navigating and mitigating risks of data collection, storage, and use; conversely, also using data to navigate and mitigate business risks
Privacy operations	Building or acquiring the technologies and services to actualize data privacy definitions

The third layer of the privacy tech "stack" is composed of business outcomes that can be supplemented or enabled by privacy tech offerings. For example, a business might build or purchase a technology to identify customer data in a visual interface for customer relations and marketing personnel, or a business might build or purchase differentially private algorithmic tools to mask individual identifiers in a dataset while also enabling analysis on the data to create economic value for the business' marketing and data science teams. Increasingly, measuring performance for these business outcomes is being measured as part of environmental, social, and corporate governance analysis.[30] This third business outcome layer is stacked on top of the business' processes, which may themselves be supplemented or enabled by privacy technology offerings. Much like business processes relevant to data privacy, privacy technologies acquired for specific business outcomes are driven by contractual requirements, regulatory requirements, and numerous other factors. There is also a growing business imperative in some cases for ethical data review and/or data-sharing with other firms.

Layer #3 of the Privacy Tech "Stack"

There are at least five business outcomes that have been identified in layer 3 of the privacy stack.

LAYER 3 OUTCOME	OUTCOME DESCRIPTION
Data availability and movability	Chief Information Officers and other technology personnel ensuring data is readily available for use and is quickly and reliably transferred around the world
Data protection for people and assets	Chief Information Security Officers and other information security personnel ensuring data's confidentiality, integrity, and availability *[not the focus of this report]*
Data value creation/analysis	Chief Data Officers, Chief Marketing Officers and their marketing teams, and other data science personnel ensuring data generates and can be used to generate (e.g., through analysis) value for the business
Data protection as ethics and compliance	General Counsels, Chief Privacy Officers, Chief Ethics Officers, legal teams, and other compliance personnel ensuring data is legally collected, stored, transferred, and otherwise processed based on applicable regulations
Environmental, social, and corporate governance	Investors, board members, and corporations in general increasingly making environmental, social, and governance factors a business priority, including the protection of data

The fact that privacy technologies must integrate with existing business processes may seem obvious, but it's worth noting explicitly. The three layers visualize this: to develop a plan for privacy, a company must have data or be acquiring data. Building out from there, companies must figure out how data maps to existing business processes, like risk management or information governance. From there, companies can "stack" privacy technologies on top of those business processes in order to achieve specific outcomes with respect to data, which increasingly are measured at the Board level or by investors seeking to assess environmental, social, and corporate governance vis-à-vis data ethics and compliance. Privacy technologies can sit in these two outer layers. For a company to have a mature privacy technology system, it cannot have privacy technologies to achieve discrete outcomes without underlying business processes in place, and it cannot have processes oriented around data without privacy technologies that achieve specific needed outcomes for the business' data. Mature privacy technology systems are also continuously evolving: the framework should not be understood as representing a static market or a static set of business activities. As the market introduces new technologies, there may be more potential business outcomes added to the third layer, for instance. As a business acquires new data, new customers, and new technologies, to give another example, it may reevaluate the privacy technology offerings used to enable or supplement various business processes or data outcomes.

The key is understanding that privacy tech offerings in the market can fill different needs in the process layer and in the outcomes layer. In this way, the privacy tech "stack" offers a framework for analyzing the privacy tech market, analyzing specific privacy technologies, and moving towards a set of shared vernacular about privacy tech. The next three sections therefore apply this privacy tech "stack" to analyzing the buy side of the privacy tech market, the sell side of the privacy tech market, and the future of the market, respectively. It combines the stack representation with research conducted for the report, including from a literature review and conversations with dozens of subject matter experts in the privacy tech field.

The Buy Side of the Privacy Tech Market

The privacy tech stack can be used to understand the buy side of the privacy technology market by highlighting the business processes and desired outcomes of different buyer stakeholders. Based on the authors' conversations with buyers and sellers in the privacy tech market, privacy technology vendors might approach any number of individuals at a client or potential client organization to sell their offerings: the Chief Privacy Officer (CPO), Chief Data Officer (CDO), Chief Technology Officer (CTO), Chief Information Officer (CIO), and Chief Information Security Officer (CISO), in addition to the likes of marketing teams, legal teams, and customer relations teams. Buying power tends to be concentrated with CTOs, who may have the largest budget for privacy technologies relative to other stakeholders in the aforementioned list. Any one business, however, may have a range of individuals within the organization with an interest in privacy technology, varied given their data needs. They may also have different budgets and technology interests depending on the company. The privacy tech stack offered in this report, focused on the layering of data, business processes, and business outcomes, is therefore applied in this section to better understand this buyer side of the market.

> **"We're increasingly seeing on the business side that they see [data] as an asset, and they know they have to worry about the privacy component, but they are primarily interested in solving a business problem."**
>
> — Executive at Privacy Tech Vendor

There are often many stakeholders in any one business with interest in buying privacy technology. Framing the privacy technology market with the privacy tech stack can help illuminate the processes with which these stakeholders are involved (e.g., risk management) and how their desired business outcomes (e.g., data value creation/analysis) drive their purchasing outlook. Chief Pri-

vacy Officers are the most likely to have fluency in privacy technology from the buyer side and are routinely consulted concerning the suitability of privacy technology offerings to satisfy personal data control and regulatory compliance requirements. CPOs may be plugged into several of the layer 2 business processes, like privacy operations and risk management, and out of all the layer 3 business outcomes, they need to make the business' data privacy compliant. Similarly, General Counsels and legal teams with privacy experience are often consulted to ensure that any privacy technology being considered will solve, not create, privacy regulatory or privacy contractual difficulties. Chief Technology Officers and Chief Information Officers are involved with the information and data governance process in layer 2, and they may have several business objectives in layer 3, including making data available and movable. The list goes on: Chief Data Officers need to enable data value creation/analysis, for such functions as monitoring internal systems and conducting machine learning on customer data to generate economic value; Chief Information Security Officers need to make data secure (e.g., ensure its confidentiality, integrity, and availability); customer service teams need data to be identifiable, so they can read customers' data when interacting with them and even possibly modify it if needed; and so on. As one vendor on the sell side told the authors, "We're increasingly seeing on the business side that they see [data] as an asset, and they know they have to worry about the privacy component, but they are primarily interested in solving a business problem."

A clear conclusion emerging from the interviews was that the potential set of customers (by role) within businesses considering privacy technology purchases is expanding. "It's an infinite universe of challenges and things you might have to deal with in terms of business cases," one vendor told the authors. Because we have entered the Privacy Tech 3.0 market phase, the key buyers of privacy tech within large companies have shifted from the Chief Privacy Officer (Privacy Tech 1.0), to the General Counsels, Chief Information Security Officers, and Chief Technology Officers (Privacy Tech 2.0), to the Chief Marketing Officers, Chief Strategy Officers, and Chief Data Scientist (Privacy Tech 3.0). The individual who continues to have the budget for software purchases tends to be the Chief Technology Officer, despite these changes.

Conclusion

Roles in the C-suite with stake in buying privacy tech are expanding beyond CTOs, CPOs, GCs, and CISOs, to include other stakeholders like CMOs, CSOs, and Chief Data Scientists.

For any particular stakeholder on the buyer side, understanding the processes in the privacy tech stack into which they are integrated, and the business outcomes in the privacy tech stack which they desire, can help the stakeholder navigate the privacy tech market through better understanding of what needs a privacy tech offering should fill. Conversely, for those selling privacy tech to a potential stakeholder at a company, using the privacy tech stack to understand that stakeholder's particular personal data (layer 1), business processes (layer 2), and needed/desired business outcomes (layer 3) can help frame what that individual might be looking to purchase. For instance, privacy tech is increasingly intersecting with the information and data governance process, including such questions as who has access to what data, how data is described in business terms, how those business terms are propagated to personal data, and so on. This process-outcome framing may help to better illuminate how a privacy tech may fit into the business' activities and technologies, and how it could meet needs, without becoming too focused on technical terminology. This range of stakeholder needs on the buy side, even within a single business, contributes to the problem of no shared vernacular to discuss privacy tech in the market: lawyers may have less exposure to technology and may preference legal definitions, technologists may have less exposure to law and may preference technical definitions, various business units may have different perspectives on technology, and so on.

From buyer to buyer, the same respective stakeholder's budget, specific needs, and business-internal technological capacity varies. Large enterprises, for example, may be more likely to maintain their own information technology infrastructure for data storage in-house, such as managing their own servers. CTOs or CIOs at those firms may therefore have disproportionately larger budgets for data and information governance functions. Smaller- and medium-sized businesses, by con-

trast, may be more likely to outsource their data storage functions to third-party cloud providers. Their CTOs and CIOs may therefore have relatively smaller budgets for data and information governance. However, no two companies are the same, and the cloud computing market's continuous growth only highlights that many businesses, large ones included, are shifting to third-party data storage and application management infrastructure. The privacy tech stack speaks to this: a seller looking to market a privacy tech offering to a large enterprise's CTO should first assess the business' *processes* before assuming a certain technology will achieve the CTO's desired business *outcomes*. The information and data governance process at a firm that outsources all of its data storage and processing to a cloud computing provider will likely require different privacy technologies to achieve data privacy compliance than a large firm that manages all data in-house.

Another important question for buyers—in addition to mapping business outcomes to privacy technologies—is whether privacy technologies should be purchased from a third-party vendor or developed in-house. Several buyers with whom we spoke identified the nascency of privacy engineering as one constraint on in-house privacy tech development. Simply put, there may not be enough privacy engineering talent to go around in general. Companies with smaller budgets may focus their in-house IT personnel on more traditional technology processes, like development and upkeep of other applications and infrastructure, and may therefore not have the time to focus those employees on building privacy technologies. That said, some companies may be willing to make the investment in in-house privacy technology development if they cannot find the requisite offerings on the market or if they only need a small plug-in developed to supplement existing tools.

Conclusion

Buyers increasingly prefer to buy horizontally-integrated privacy tech services.

But the buy-or-build question is not just answerable based on a business' technology needs, which is why the privacy tech stack's focus on business processes and outcomes can be useful here too. Some buyers may be motivated to develop privacy technologies in-house because they best understand their own business operations and are thus best-suited to tailor tools to that environment. If those buyers purchased third-party technology off-the-shelf, it could require what is considered too much labor to integrate that technology into the buyer's systems. Several experts interviewed spoke to their experiences where buying privacy technology was the easy and speedy part relative to the post-contract signing integrations, and to the distraction caused by pulling engineers off of their primary task to develop products and services for sale by the business. Buyers might also purchase third-party privacy technology but build it into their own technology abstractions themselves, given it's not too labor-intensive, in order to minimize the number of contact points with the vendor technology. And of course, individual stakeholders in a business could make different buy-or-build decisions based on specific processes or desired outcomes: a CTO with a big budget might develop data identifiability tools in-house because they have the funds, while a CPO at the same company might purchase tools to help with privacy operations off-the-shelf because they don't have the budget.

Of course, the buy side is only one part of the equation. The next section therefore examines the sell side of the privacy tech market, drawing on the research conducted for this report, and also applies the privacy tech stack to understanding sellers in the market.

The Sell Side of the Privacy Tech Market

Because the privacy tech industry is, in many ways, in nascent stages, new providers are entering the market each year, in some cases offering entirely new products or in other cases competing directly with existing offerings. Firms might specialize in one service, such as cookie consent management tools, while others might seek to provide a suite of services. The number and range of privacy tech offerings on the sell side of the market, much like demand on the buy side, is only going to grow in coming years as more data privacy regulations are implemented, the desires and needs of businesses to extract value from personal data increase, and competitive pressures for firms to protect customer privacy grow.

Much like the privacy tech stack can illuminate buyer motivations for acquiring privacy tech, the privacy tech stack can be used to analyze a sellers' privacy tech offerings. Using business processes (layer 2) as a lens, sellers might offer a range of privacy technologies that enable or supplement information and data governance, privacy management, risk management, or privacy operations stacked on top of data. Sellers could target the business process of a particular buy-side stakeholder—e.g., a CPO's privacy management process—or they could target the overall business' process with a privacy tech offering, such as selling risk management technologies to the CTO, CIO, and other executives. Using business outcomes (layer 3) as a lens, sellers might offer a range of privacy technologies that meet any number of a buyer's desired business outcomes. For instance, a data access control technology, which limits who can read and write to particular data, could help support the "data ethics and compliance" and the "data protection for people and assets" outcome at once under the US' Health Insurance Portability and Accountability Act (HIPAA). In a similar vein, privacy technology to track customer consent agreements could simultaneously help support "data ethics and compliance" and "environmental, social, and corporate governance" outcomes. Of course, seller offerings can span layers of the privacy tech stack as well. Technology using noise addition to satisfy differential privacy requirements or masking individual identifiers (e.g., a customer's name), while still allowing machine learning to be run on the data (e.g., identifying customer buy preferences), can help enable the "data ethics and compliance" and the "data value creation/analysis" objectives at once. This technology could potentially plug into a CPO's privacy management and risk management processes at the same time as it plugs into and better enables a CTO's information and data governance process.

"There is no single solution that can solve all privacy stuff."

— Executive at Privacy Tech Vendor

Vendor privacy tech solutions also differ in their interoperability and ease of implementation. Some offerings are off-the-shelf in that buyers can license and use immediately. Other seller offerings may require extensive integration. Integrating a solution with existing tools and technologies can also require additional time and resources on the buyer side. For example, a business might want to minimize the number of interactions their databases have with a privacy technology and may choose to custom-engineer the back-end setup to reduce the number of touchpoints. Interoperability also varies. Some seller products can be used relatively seamlessly alongside other sellers' privacy tech offerings, whereas other privacy tech offerings do not plug-and-play as well with other companies' products. This, too, can create work on the buyer side, meaning it can also serve as a point of differentiation for sellers who can effectively market the interoperability of their products. All of this is in part a product of the demand for different specific privacy technologies; as one seller put it, "there is no single solution that can solve all privacy stuff."

Conclusion

Buyers of privacy tech often prefer to buy integrated privacy tech products that accomplish numerous business needs rather than one-off, standalone privacy tech solutions.

The sell side of the privacy tech market also contributes to the lack-of-shared-vernacular problem. Because the privacy tech industry has developed quickly and is still very much evolving, it's not just the buy side that contributes to different, differently used, or even outright confusing terminology that discusses privacy technologies and how they integrate into the business (e.g., multiple different uses of the phrase "data mapping"). Individuals with whom the authors spoke conveyed that on the sell side as well, it takes time to develop the soft and hard skills to not only manage but discuss privacy technologies. Whereas some sellers may market their products as satisfying "differential privacy," for example, they may not mean the exact same thing as other sellers using the same terminology.[31] Sellers offering "data discovery" solutions, to give another example, might encounter a problem of applying a privacy concept to a variety of business activities—where a task like "conducting a data inventory" may mean very different things in different cases based on the seller's specific technological offerings and what kind of artifacts (e.g., outputs of that process) they are promising to potential buyers. Imprecision in terminology can come from both the buy and the sell side of the market.[32]

Conclusion

Additionally, growing fragmentation in privacy regulation regimes worldwide and even within countries will only contribute to the shared vernacular problem.

Finally, sellers may approach different kinds of buyers depending on their offerings. There are companies offering privacy tech solutions that sell to all sizes and types of firms; some are industry-specific in their offerings; others only market to large enterprises or, in other cases, to small- or medium-sized enterprises; and others yet will offer one kind of privacy tech product to larger firms and have a different version that is offered to smaller ones. Just as there are many stakeholders at a single business on the buy side who might be interested in privacy tech, sellers in the privacy tech market also have different calculations they make to determine who they approach to buy their products. Focusing on the business processes which a privacy tech enables or supplements, and the business outcomes a privacy tech helps achieve, is one way to categorize the sellers in the market.

Just as interviewees were clear that unless and until consensus definitions for common privacy tech terms were developed, they were also in near uniformity about re-imagining the "privacy stack" to reflect the more recent, third phase of privacy tech development: meeting business needs in addition to data control and regulatory compliance. Quite simply, buyers and sellers of privacy tech are speaking a different language. They also do not share a vision of how privacy tech available in the marketplace maps with emerging business

needs to also use personal data, extract value from insights gleaned from that data, and perhaps train artificial intelligence systems with that data. A clear insight drawn from these interviewees is that a new privacy stack typology, such as that offered by this report, may provide substantial value in translating what customers say they need and want from privacy tech and what vendors say they are capable of providing.

With this picture of both the buy side and the sell side of the privacy tech market today, it is worth looking forward to assess where the market is headed and what some of these challenges—like a range of stakeholders in a business on the buy side, or the shared vernacular problem in the market writ large—mean for privacy technology's future. The next section therefore explores the future of the privacy tech market and potential implications, drawing on the privacy tech stack framework and the authors' conversations with subject matter experts.

Market Trends and Implications for Competition

Recognizing that the privacy tech market is continually evolving and that buyers and sellers lack a shared set of vernacular for discussing it, this section combines insights from the authors' research and interviews with representatives of buyers and sellers with the privacy tech stack to analyze the future of the market. It does this by discussing five identified market trends and seven implications for future competition in privacy tech. This then feeds into the final report discussions which offer recommendations.

Five Market Trends

Buyers desire "enterprise-wide solutions." Products that work across all parts of their organization are more attractive from a business perspective. Instead of multiple negotiations with numerous vendors for various privacy tech services, a buyer can, in theory, reduce business and legal negotiations substantially if there is an enterprise-wide solution that can accomplish business needs at all layers of the privacy stack. These privacy technologies could reduce buyers' acquisition costs, in that a business only needs to purchase one tool for a particular task that many of its stakeholders (e.g., CTOs, CIOs, etc.) could use, and they could also reduce the costs of plugging that technology into the business' systems and processes. When privacy technologies fit well into the privacy tech stack not just for one buyer stakeholder but for the entire buyer's business, that can be a differentiator for a seller. That said, however, enterprise-wide solutions are not without their own costs; products that can be used by more stakeholders in a business are going to require those stakeholders to take part in conversations about purchasing and to likely expend some time and resources on implementing the technology. As one buyer told the authors, "Technology that can be controlled by and operated by, exclusively, the privacy team—great. But if it is a thing that is going to require the cooperation of anybody beyond the privacy team, I think it's really hard for companies to adopt."

Buyers favor integrated technologies. Privacy technologies that interoperate well with other privacy technologies (even those offered by different vendors) are more favorable from a buyer perspective. "Nobody wants a bespoke solution" where "they have to deploy nineteen other bespoke solutions to meet their use cases," one vendor told the authors. Less work to integrate privacy technologies into existing business processes and with existing business technologies means more time and money saved for the buyer. As highlighted by the privacy tech stack, a single privacy technology could plug into multiple business processes that each have their own technologies and sub-processes, all of which are stacked on top of data. One seller offering might also be working in concert with numerous other seller offerings in order to achieve multiple business

outcomes simultaneously, such as ensuring data is privacy compliant on the one hand but identifiable for customer service and marketing purposes on the other. Conversely, multiple individuals with whom the authors spoke stressed the insufficient emphasis on the labor required to integrate some technologies into the business environment and make them work effectively. Privacy technologies that will require more work to integrate may be less appealing to prospective buyers. There can also be a vendor lock-in effect to proprietary solutions, where technologies that make a buyer more dependent on that particular offering make it more costly for that buyer to switch to other technologies in the future. "If you're stuck with a technological system that you pay for and it's hard to switch out of," that's a problem, said one buyer.

Some vendors are moving to either collaborate and integrate or provide fully integrated solutions themselves. In light of the previous trend, some privacy tech vendors are moving to collaborate with other vendors to promote interoperability, so that their offerings are easier to set up and run once purchased. Recognizing competition presented by larger competitors with enterprise-wide solutions, some privacy tech vendors are increasingly creating collaborative offerings or forming partnerships to cross-sell others' services while they sell their own and increase the likelihood the collaborating companies beat out individual business competitors offering enterprise-wide or varied-but-integrated privacy. This kind of "alliance work," as one individual put it, can itself be a potential competitive boost for a seller.[33] In the opposite case, some other privacy tech vendors are moving to provide fully integrated solutions themselves rather than work with other sellers. BigID, for example, shifted during the COVID-19 pandemic to add new data analytics capabilities to its platform.[34] There are many firms doing neither and continuing to provide offerings that may be, from a buyer perspective, insufficiently interoperable, but it is certainly the case that some sellers are already aware of this buyer demand for integrated products and are adjusting their privacy tech development strategies accordingly.

Data is *the* enterprise asset. The innermost layer of the privacy tech stack, and therefore the stack's center, is data. Business processes that relate to data privacy build on top of data, and business outcomes that can be achieved in concert with those processes are built on top of that—but data remains the underlying asset. Data "privacy" technology is therefore just a part of the broader business use of data; it is one part of enabling the extraction of economic value from data. While most buyers looking to acquire privacy technology are driven by regulatory requirements above all else, the slow and steady emergence of competitive pressures for companies to promote and protect data privacy speaks to growing recognition in many industries of data as a key enterprise asset that must be appropriately managed and protected.

Jurisdiction impacts the shared vernacular problem. Applying the privacy tech stack in different jurisdictions highlights additional complexity associated with the shared vernacular problem. Take layer 3 of the stack, business outcomes, as an example. "Data ethics and compliance" is going to mean different things in different regulatory jurisdictions depending on the laws and regulations at play, as well as the terminology used in business and research communities to discuss privacy tech. One example several individuals with whom the authors spoke highlighted is pseudonymization and de-identification, which have different meanings in the US and the EU, including to what extent they are distinct. Even when regulatory or statutory terms start out with a common definition, differing interpretations of those terms by regulators or judges can cause divergence over time of the meaning of a common term in different states or countries. Even "legal terms are not understood the same way," as one vendor remarked.

"Interaction between industry and academic researchers is a critical element to what will be achieved in advancing privacy technology, helping privacy researchers understand technological and business needs and developments on the ground."

— Jules Polonetsky and Jeremy Greenberg, *NSF Convergence Accelerator: The Future of Privacy Technology*

For compliance with the US' HIPAA, for instance, the US Department of Health and Human Services lays out two de-identification methods: "a formal determination by a qualified expert"; and "the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual."[35] The purpose is to minimize the risk that the de-identified data is linked back to any particular individual's identity when the data is made available to an anticipated recipient. The EU's GDPR, to provide another example, defines anonymous information as "no longer identifiable," where "account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

Of course, these definitions refer to an ideal state; in practice, de-identification may not work, and it can also be implemented incorrectly. Many attempts to mask the identities of individuals in openly published datasets have failed, because it was all too easy for researchers to link the allegedly anonymized data back to individuals through "auxiliary data," or information from a third source that provided missing links.[36] In other words, the attacker was able to unmask the real identities of the individuals in the dataset because that attacker had additional information. But regulatory jurisdictions are impacting the discussion of this issue and relevant technologies, and therefore the broader issue of a lack of common vocabulary in the privacy tech market.

Seven Implications for Competition

Buyers favor integrated solutions over one-off solutions. The privacy tech market is always evolving, but buyers repeatedly told the authors that they disfavored one-off solutions that only did one or a few things to satisfy their business' privacy needs, unless they were especially novel or provided true break-through privacy technologies that could uniquely solve one of the privacy stack needs for the business. Generally, though, they preferred integrated solutions. In line with the trend of vendors focusing on the interoperability of their privacy tech offerings—whether through collaboration with other sellers or through integration efforts on their own—buyers will likely continue showing a preference for integrated solutions over one-off solutions. If this trend continues, it likely will result in the largest privacy tech vendors with the broadest suite of products and services gaining additional customers faster than competitors without these advantages. New buyers in the privacy tech market may not yet have these preferences (or have them as strongly), but based on author conversations, it does not appear this preference is going away. This could push more sellers towards integrating their privacy tech products better with other sellers' privacy tech products and with traditional IT systems. This could also reduce the competitiveness, over time, of stand-alone privacy tech offerings in the market that do not integrate well with other technologies.

Collaborations, partnership, cross-selling, and joint ventures between privacy tech vendors are increasing to provide buyers integrated suites of services and to attract additional market share. In response to this buyer preference for pre-integrated suites of privacy technology services, privacy tech vendors of all sizes are forming mutually advantageous business partnerships. The partnerships are taking many forms from the informal all the way through full joint ventures. BigID, for example, announced a partnership with Auritas in August 2020 to "[enable] SAP customers to identify at risk data across the enterprise while incorporating a solution to dispose of unwanted and redundant data both inside and outside of their SAP systems."[37] WireWheel partnered with Crownpeak in November 2019 to offer a suite of privacy tools for the California Consumer Privacy Act before it went into force in January 2020.[38] BigID and WireWheel announced their "expanded partnership and set of integrations" in May of 2020.[39] TrustArc has partnered with such firms as Alibaba Cloud, Evident, and RadarFirst in the last couple of years to bolster offerings on privacy and data protection.[40] And OneTrust, to give one more example, announced a partnership with the Data & Marketing Association in August 2019 to better supply privacy tools and resources to marketers.[41] More recently, OneTrust integrated its services with startup privacy tech vendor Integris and then acquired the company, following in April 2021 with

the acquisition of ethics and compliance vendor Convercent.[42] Smaller companies that are not included in these collaborations face additional challenges due to this trend that could cause them to run out of cash or fail to attract additional rounds of investment.

Private equity and private equity-backed companies will continue their "roll-up" strategies of buying up niche providers to build a package of companies providing solutions to provide the integrated solutions buyers favor. This may lend itself to more integration among privacy technologies in the market. It also may benefit those firms to be wrapped up in such a fashion. For example, in July of 2020, Aura, which describes itself as a "technology company dedicated to simplifying digital security for consumers" announced they were "[c]ommitted to creating a unified platform of services" and that they were acquiring three privacy companies: Figleaf, a "company that allows consumers to control their own data online and offline"; Pango, which operates multiple Virtual Private Network (VPN) services; and PrivacyMate, an anti-data broker service that "continuously monitors and prevents the collection and sale of personal information online and offline."[43] While the success of any private equity roll-up of various privacy tech vendors is not certain, there was virtually unanimous consensus among the experts with whom the authors spoke that private equity firms will continue to view the privacy tech industry as a growth industry and that the strategy of buying up niche providers to create a comprehensive package of companies providing solutions is here to stay. The experts commenting on this strategy viewed this as an attempt to build competitors to the largest privacy tech vendors that provide a myriad of privacy technology products and services.

Venture capital will continue funding the privacy tech sector, though not every seller has the same level of success fundraising. Privacy technology startups continue to raise substantial fundraising rounds. In February, OneTrust announced they had raised a $210 million Series B round valuing the company at $2.7 billion,[44]followed by a Series C round concluding in April 2021 that took its value to 5.3 billion.[45] WireWheel announced a $10 million venture capital investment round in February as well, bringing their venture investment to a reported $23.6 million.[46] These investment rounds followed two $50 million investment rounds announced in January, with Securit.ai raising $50 million for a Series B investment round,[47] and BigID raising $50 million for a Series D investment round.[48] In December 2020, BigID announced a new funding round that placed the company's valuation at over $1 billion.[49] Although these are eye-popping investments in privacy tech, they are just a fraction of the total VC and other private investment in data privacy and data security technologies. Crunchbase, which tracks private investments, reported that there was nearly $10 billion invested in privacy and security tech in 2019 alone.[50] That said, not all sellers have the same success raising VC funds. Some firms have little trouble at all raising money; others are newer to the market and therefore encounter their own challenges in that way. Having working privacy technology to deploy and a track record of sales appears to be the magic formula for attracting venture capital support. Though given privacy technology is a nascent market with a lack of clear, shared vernacular, one of the biggest competitive factors for sellers seeking VC funding going forward may be those firms' ability to effectively situate themselves, not just literally but also rhetorically, among the other players in the market. Venture capital firms themselves, moreover, are not immune from the shared vernacular problem either.

Big companies may acquire strategically valuable, niche players. As the bigger sellers continue to grow, they may purchase smaller sellers to complement their offerings and contribute to a shift towards better integration with other technologies. To the extent larger companies can offer more solutions to prospective buyers—that is, selling privacy technologies that can enable or supplement more business processes and support more business outcomes—they can gain a competitive advantage over other firms. Take for example, the recent acquisition by Epic Games of parental consent privacy tool SuperAwesome, which allows the gaming company to bring inside their company and tightly integrate one of the very few privacy consent tools that offers third-party consent services.[51] This is especially true where big companies acquire new market entrants whose technologies are not yet widely deployed. This relates to the growing demand for enterprise-wide, better-integrated privacy tech

solutions that buyers can easily deploy in their own information technology environments. This also means big firms may stay big and provide more and more integrated solutions, through both this kind of acquisition strategy and building more technologies in-house to complement existing privacy tech offerings.

Small startups may struggle to gain market traction absent a truly novel or superb solution. In light of the integration and consolidation trends emerging in the privacy tech market, it is possible that small startups will struggle to attract the necessary funding and secure the necessary customers in order to gain market traction, absent a truly novel or superb privacy technology solution that functions or integrates better than other offerings or that achieves business outcomes in ways not yet achieved by other technologies in the privacy tech stack. All of that said, much is uncertain. Newly developed technologies could shift the market playing field. New regulations, too, will remain a driving force for buyer decision-making and as such could push the market in new directions based on new regulatory demands. Startups could struggle in various respects as privacy technologies are integrated between or consolidated among existing, larger vendors. But they might also have new opportunities to introduce innovation as new regulations mandate new technologies be integrated into buyers' privacy tech stacks. "If you're building a solution, a mass-market solution, for a problem that hasn't really gone mass-market…you need to be able to sustain yourself during those years of hunger," one vendor told the authors.

Buyers will face challenges in future-proofing their privacy strategies. The privacy tech stack's outer two layers are business processes and business outcomes, respectively. Processes by definition refer to a series of actions, and in the case of something like risk management, they are a continuous series of actions; to mitigate risk to a business, a risk management process cannot just be executed once. Similarly, outcomes are not static in that they cannot just be 'achieved once' and then maintained forever; an outcome like data ethics and compliance or data protection for people and assets may come under threat or even become undone as a business acquires new data or as regulatory requirements change. Building a mature privacy technology system for a business must therefore be understood as a process of continuous reassessment and evolution, not just as the market evolves, but as new data is collected, new customers are acquired, new third-party cloud technology is leased, the business expands into new regulatory jurisdictions, and so on. This will be one of the biggest challenges for businesses buying privacy tech: future-proofing their strategies in the absence of a regulatory push to do so. The GDPR and the CCPA have undoubtedly driven much of the demand for privacy technology in the current market—on this point, there was virtually unanimous consensus among the experts to whom the authors spoke. Despite the clear fact that the privacy technology market is only to become larger over the coming years, and venture capital firms' continued interest in it, buyers may still tend to be reactive rather than proactive in building and maintaining their privacy tech stack.

Conclusions

While the privacy technology industry is relatively nascent today, it is only poised to grow in the coming years as data privacy becomes more important for businesses. New laws and regulations will be a large driver of this growth, yet so will the maturation of business privacy technology from a Privacy Tech 1.0 or Privacy Tech 2.0 approach, where the primary concern is compliance, to a Privacy Tech 3.0 approach, where compliance and privacy are meshed with business outcomes for personal data like usability and value-generation. This section therefore concludes the report with a number of observations about the state of the privacy tech industry today and its future directions. Unlike the previous section that discussed five clear market trends and their seven main implications for the future, this conclusion section lists out numerous, sometimes discrete, observations about the privacy tech industry.

- The COVID-19 pandemic has globally accelerated marketplace adoption of privacy technology as citizens and consumers worldwide become more heavily dependent on digital technologies and services. Schooling, work, grocery purchasing, social communication with friends and family, and numerous other institutional and individual functions have moved online. This has greatly accelerated dependencies on digital services—and by extension, created much more data through online activity and forced more data to be digitally available—and accelerated business needs for privacy enhancing technologies in the process. It is unclear if this growth is a one-off event or a growth pattern that will sustain, but increased purchasing of privacy tech is clear.
- Common drivers of initial privacy technology purchases are regulatory compliance needs, contractual requirements with customers, and slowly emerging recognition of the reputational risks associated with data privacy breaches, broadly defined. Regulations by and large remain the biggest driver for privacy technology adoption, but the others are growing in importance to the extent that privacy is becoming a competitive differentiator in some sectors. Organizations are also deploying more tools to mitigate potential harms caused by the use of data.[52] These initial drivers, however, often lead purchasers of privacy tech to explore other opportunities to deploy additional privacy tech offerings.

- While jurisdictions around the US and around the globe are likely to incorporate key concepts from other jurisdictions' consumer privacy regulatory schemes into their own, for the foreseeable future, the privacy landscape is likely to become more complex and less homogenous as additional states and countries enact innovative laws or promulgate innovative regulations. The United States currently has a somewhat fractured system with the CCPA in California, several other similar bills in consideration in various states, and no similar federal law that applies to all companies nationally. Globally, data regimes between the United States, the European Union, India, Brazil, Japan, and other countries are in various ways fracturing.
- Even common privacy terms, such as those included in statutes or regulations, are not uniformly defined or understood. Courts may interpret the same terminology differently, just as individual attorneys may have different interpretations of technical privacy terminology. This problem is not helped by a lack of understanding of privacy technologies on the part of some buyers and competitive desires by some vendors to self-preferentially develop terminology for their own marketing purposes.
- The lack of common understanding about privacy terms may be limiting the growth of the privacy tech industry. With respect to some privacy tech offerings, it may be unclear whether vendor-developed privacy tech is sufficient to satisfy the regulatory compliance or business needs of would-be purchasers. Businesses that do not specialize in technology may have a particular challenge with this vernacular problem, as might different stakeholders within a single business who have varied technical expertise.
- In addition to lacking a common vernacular to describe privacy tech, there is no commonly accepted methodology for typifying what technologies and services are part of the privacy technology industry or the so-called privacy stack. Many interviewed for this report, from both the sell-side and buy-side, agreed that it might prove useful to classify privacy tech companies by the "business needs" their offerings satisfy. This can also help to further contextualize particular privacy technology solutions in terms of their interoperability with other products and the extent to which they provide a bespoke versus enterprise-wide technological solution to privacy technology problems.
- The lack of common vernacular and inconsistent typology for the privacy stack may also be causing some misalignment between the privacy tech ideated and brought to market and that which buyers perceive they want, need, and may be willing to pay for. Speaking in different terms can lead a buyer and a seller to very different conclusions about what the other company offers or needs, respectively. This is especially true where technologies like homomorphic encryption and differential privacy are concerned, as no clear certification mechanisms exist for these technologies which leaves some firms unclear about the robustness of a particular solution labeled with that term. Furthermore, there are many different flavors of these technologies, each with their own strengths and weaknesses depending on the use case.
- The market has passed through two initial stages of privacy tech and has entered a third. The first two were typified by technologies engineered natively within some companies and offered by early vendors for sale to achieve a modicum of control over the personal data encountered by a business (Privacy Tech 1.0), and technologies engineered natively within companies well-resourced with enough computer engineers to not only build their core products and services but also engineer regulatory compliance solutions and horizontally-integrated companies or collaborations between companies offering personal data regulatory compliance services and tools for sale (Privacy Tech 2.0).

- Recently, privacy tech offerings are expanding well beyond products and services that assist in regulatory compliance into products and services that assist businesses in making the personal data they encounter both maximally available and maximally valuable for various components throughout the business (Privacy Tech 3.0). For example, privacy tech tools are increasingly available to assist with business needs across the business enterprise: (i) CIOs in making PII/Personal Data accessible; (ii) CMOs in making PII/Personal Data available for marketing and advertising; (iii) Chief Data Scientists in unlocking unexpected value from PII/Personal Data; and (iv) CISOs in securing data; etc. This is a critical development to note as businesses increasingly view personal data as an enterprise asset and come to view privacy technology as unlocking data value *alongside* compliance, not just meeting compliance needs themselves.
- Because we have entered the Privacy Tech 3.0 market phase, the key buyers of privacy tech within large companies have shifted from the Chief Privacy Officer (Privacy Tech 1.0), to the General Counsels, Chief Information Security Officers, and Chief Technology Officers (Privacy Tech 2.0), to the Chief Marketing Officers, Chief Strategy Officers, and Head Data Scientist (Privacy Tech 3.0). The individual who continues to have the budget for software purchases tends to be the Chief Technology Officer, despite these changes. The Chief Privacy Officer continues to be an influencer of these purchases, but should recognize this development as a call to embrace the skills and scope of responsibilities to maintain a leadership mandate. The size of a buyer is also important here, not just for budgetary reasons but for infrastructural reasons too; large enterprises, for example, are far more likely to manage their own servers in-house than a smaller enterprise (though many firms, in any case, are making relatively big shifts to cloud computing).
- For many companies, especially small- or medium-sized businesses and those that tend to serve individuals only residing in one country, Privacy Tech 2.0 or even 1.0 solutions and vendors may be sufficient to meet their needs. Increasingly, buyers need to build or buy privacy tech that accomplishes their business' needs for control, regulatory compliance, and data availability and value. In short, while the market for privacy tech is maturing there is likely market segmentation between buyers, and the most sophisticated companies will need all three evolutions of privacy tech solutions. "Stacking" these privacy technology layers atop one another enables a more mature privacy technology model.
- Buyers of privacy tech often prefer to buy integrated privacy tech products that accomplish numerous business needs rather than one-off, standalone privacy tech solutions. This is because standalone solutions can be more costly to implement on the business side; they can also produce a risk of vendor lock-in if the technology is proprietary and becomes a source of dependency. The exception to this rule is when a privacy tech vendor offers a "breakthrough" or "highly innovative" technology or service, which can justify a contract with a vendor for just one niche product or service.
- Because of buyers' increasing preference to buy horizontally-integrated privacy tech services, more well-resourced privacy tech companies with numerous, fully developed tools and services may more quickly attract more customers and perhaps grow their market share at the expense of niche privacy tech startups. That is, of course, considering several other factors, including whether there is presently a demand for the integrated service; even if useful for businesses, not all privacy tech solutions are widely recognized as important in today's market.

- This buyer preference for horizontally-integrated privacy tech services may lead to industry consolidation in the near term. For example, recently, some privacy tech companies have merged or acquired rivals or offerors of adjacent privacy tech products. Further, some private equity companies appear to be "rolling up" privacy tech startups into larger offerings. Some providers are employing a third strategy of formally entering into partnerships, joint ventures, cross-selling, or similar collaborations. It is perceived by some that niche providers may increasingly struggle unless they are able to offer an entire suite of services.
- While the privacy tech market and privacy vendors' strategy for ensuring longevity and growth is undergoing transformation, there is striking consensus about the determinative factors of how buyers choose whether to buy or build privacy tech. Our surveys found commonality among forms in who in the corporate organizational structure often has the budget to purchase privacy tech, who in that structure identifies the business needs to be met by privacy technologies, and who must be consulted for successful privacy tech contracts to be signed. The size of a business and its particular information technology infrastructure, as mentioned, is an important factor in this equation as well.
- Some purchasers expressed concerns about the "lock-in" effect of buying any privacy tech solution. In other words, some admitted they might not make a purchase for fear that doing so might lead their companies to be beholden to that vendor for numerous, future budget cycles even if better, competitor technologies emerge or the enterprise needs change. That some larger vendors are moving to cooperate or partner with others in the industry may demonstrate growing recognition of this fact.
- Market needs differentiation seems likely for small- or medium-sized buyers of privacy tech when compared to large scale enterprises. Small- and medium-sized buyers may be operating with not just different budgets and organizational structures but also different information technology infrastructure, in some cases notably differentiating their exact privacy tech needs from those of larger enterprise buyers.
- While large enterprises are the common purchasers of privacy tech services, the world's most sophisticated and complex businesses that view themselves as tech companies, and who have the greatest number of computer engineers, recognize their own complex and unique data needs. As a result, they are more likely to build privacy tech natively and purchase fewer services from privacy tech vendors.

All told, the privacy technology industry is on a clear growth trajectory. Regulatory and competitive drivers, growing business recognition of personal data as an enterprise asset, continued venture capital interest in privacy tech investment, and newly emerging technologies for personal data management will continue the evolution of the privacy technology industry. In a feedback loop, business' privacy technology stacks will only continue to mature, moving from the innermost layer of simply using personal data to the outermost layer of simultaneously maximizing different business outcomes for that data. All the while, though, many impediments to growth and gaps between the buy and sell side of the market remain—making an understanding of the market's present and future states all the more important.

Recommendations

This report makes the following seven recommendations to address the issues identified within:

- Privacy tech stakeholders should develop and promote voluntary, shared, consensus-driven vernacular in the privacy technology market for the benefit of both buyers and sellers. Consensus definitions should then be used to facilitate developing a common typology for descriptions of the tools and services developed natively or made available for sale in the privacy tech marketplace.
- A trusted body should provide common definitions and standards for privacy enhancing technologies (PETS) such as differential privacy, homomorphic encryption, federated learning, and similar technologies, and should indicate the maturity and utility of these technologies for different business cases, as well as to how the uses of these PETS map to legal requirements.
- Further research should be conducted to identify market segmentation and stratification in buyers based on the size of the corporate entity, the sophistication of the buyer, the industry sector, and other factors.
- Further research should explore what unique needs, if any, small- or medium-sized enterprises may have relative to those of large enterprise buyers of privacy tech.
- Future research might also explore whether the needs for privacy tech solutions differ between industry types in a meaningful way.
- Future research might also consider whether businesses that solely or primarily interact with the personal data of individuals from just one country or region have different privacy tech interests and needs than do businesses interacting with personal data on a multinational level.
- Vendors should recognize the need to provide adequate support to customers to increase uptake and speed time from contract signing to successful integration. Buyers will often underestimate the time needed to integrate privacy technologies and services into their existing business operations and may therefore need further assistance in realizing that integration.

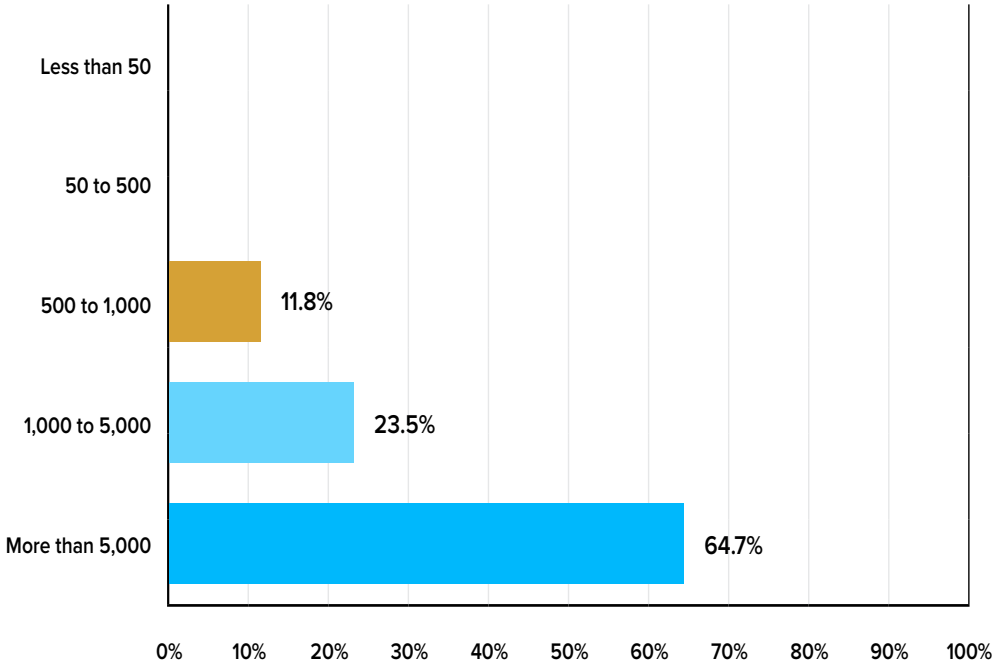
APPENDIX: Privacy Technology Buyer Survey Results

Methodology

FPF Members were invited to complete the Privacy Technology Survey about their organization's experience as privacy technology buyer. The survey was created in SurveyMonkey and made available via email. We received a total of 17 responses. The survey responses were de-duped and aggregated.

Question 1: How many people are employed at your corporation? Select one answer.

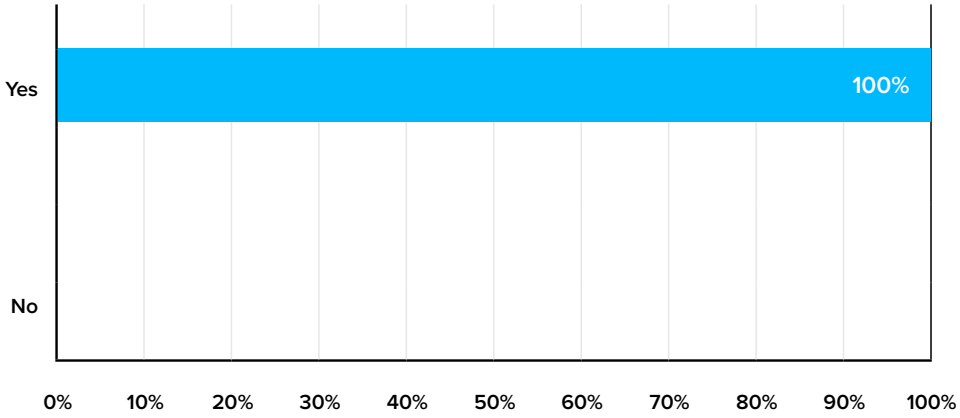
Answered: 17



ANSWER CHOICES	RESPONSES	
Less than 50	0.0%	0
50 to 500	0.0%	0
500 to 1,000	11.8%	2
1,000 to 5,000	23.5%	4
More than 5,000	64.7%	11
TOTAL RESPONDENTS		17

Question 2: Has your company ever purchased privacy-enhancing technologies, whether software or hardware, from a third-party provider? Select one answer.

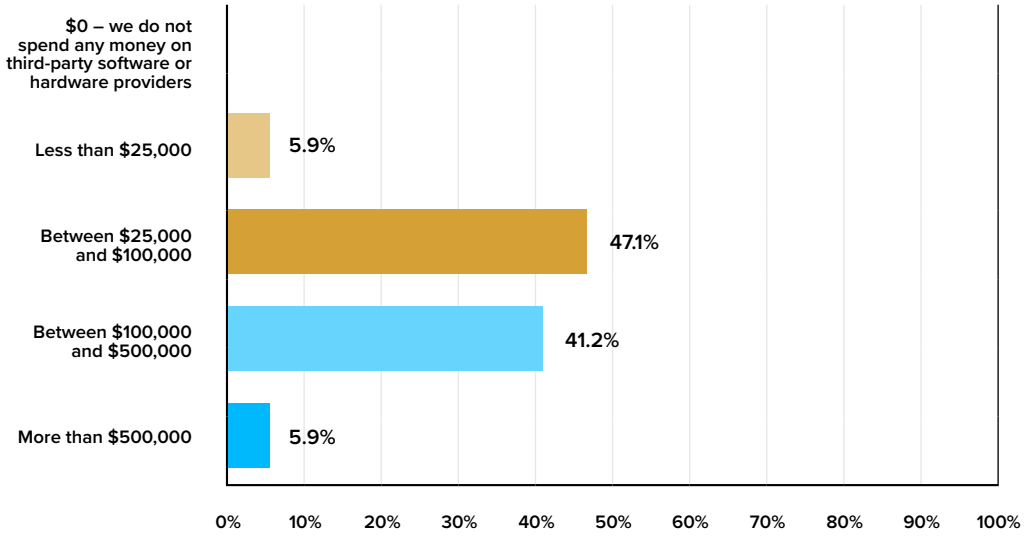
Answered: 17



ANSWER CHOICES	RESPONSES	
Yes	100.0%	17
No	0.0%	0
TOTAL		17

Question 3: What amount describes your corporation's annual total corporate spend on privacy technologies provided by third-party software or hardware providers? Select one answer.

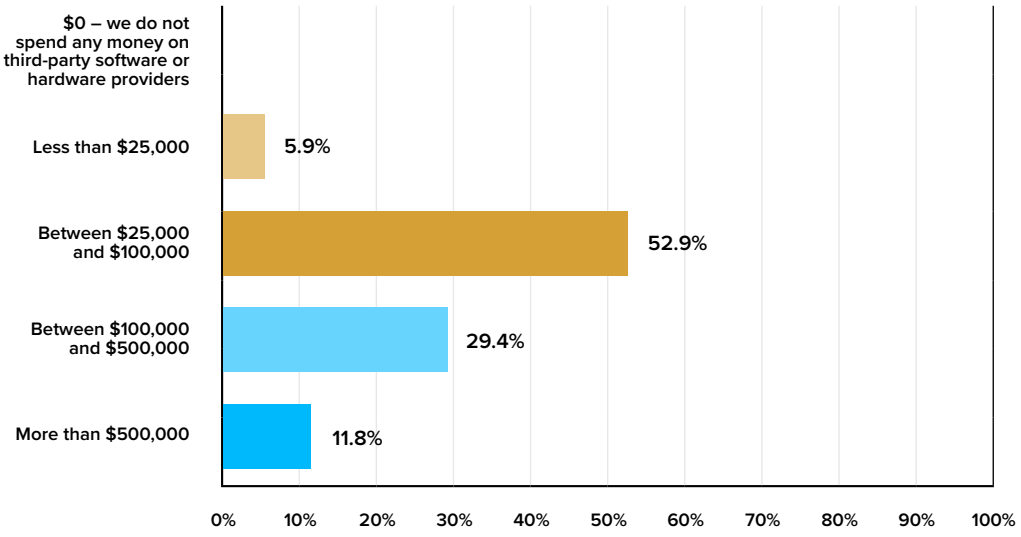
Answered: 17



ANSWER CHOICES	RESPONSES	
$0 – we do not spend any money on third-party software or hardware providers	0.0%	0
Less than $25,000	5.9%	1
Between $25,000 and $100,000	47.1%	8
Between $100,000 and $500,000	41.2%	7
More than $500,000	5.9%	1
TOTAL RESPONDENTS		17

Question 4: What is the most your corporation has ever spent on a single acquisition of a privacy technology provided by third-party software or hardware providers? Select one answer.

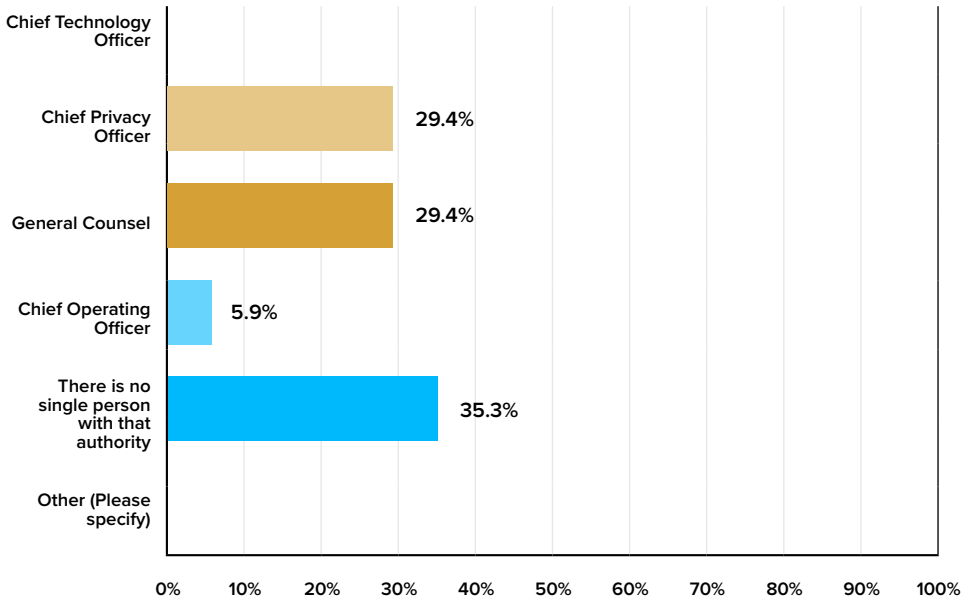
Answered: 17



ANSWER CHOICES	RESPONSES	
$0 – we do not spend any money on third-party software or hardware providers	0.0%	0
Less than $25,000	5.9%	1
Between $25,000 and $100,000	52.9%	9
Between $100,000 and $500,000	29.4%	5
More than $500,000	11.8%	2
TOTAL RESPONDENTS		17

Question 5: What is the title of the person in your corporation who has final budget authority for purchasing privacy-enhancing technology? Select one answer.

Answered: 17

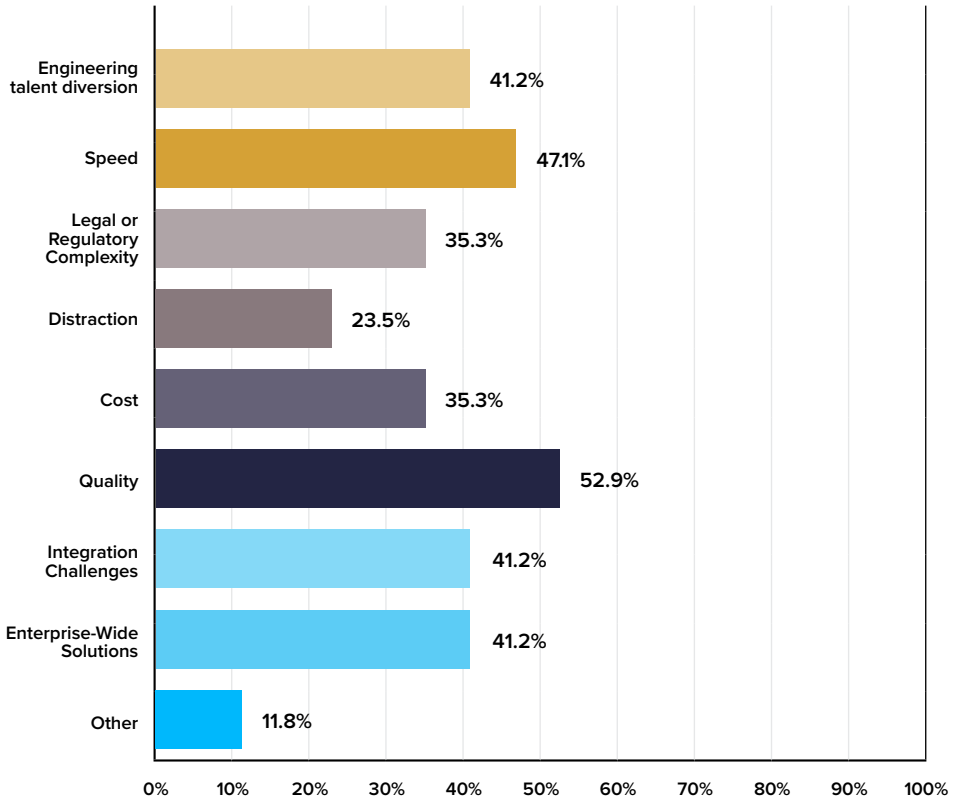


ANSWER CHOICES	RESPONSES	
Chief Technology Officer	0.0%	0
Chief Privacy Officer	29.4%	5
General Counsel	29.4%	5
Chief Operating Officer	5.9%	1
There is no single person with that authority	35.3%	6
Other (please specify)	0.0%	0
TOTAL RESPONDENTS		17

[Question 6 was a question about background report interviews and has been omitted.]

Question 7: Discussions with privacy leaders within FPF supporter companies suggest that there are several key factors that determine whether a company will purchase privacy technologies from a third-party software or hardware provider. This is often described as the question of whether to build or buy, i.e., whether the company should direct its engineers to code its own privacy solutions or whether to buy them from a vendor. In discussions with companies that choose to buy privacy technologies from a third-party provider, these are some of the more common responses we hear. Please note those factors that influence your decision of whether to buy tools from a third party or build them internally. Check all that apply.

Answered: 17

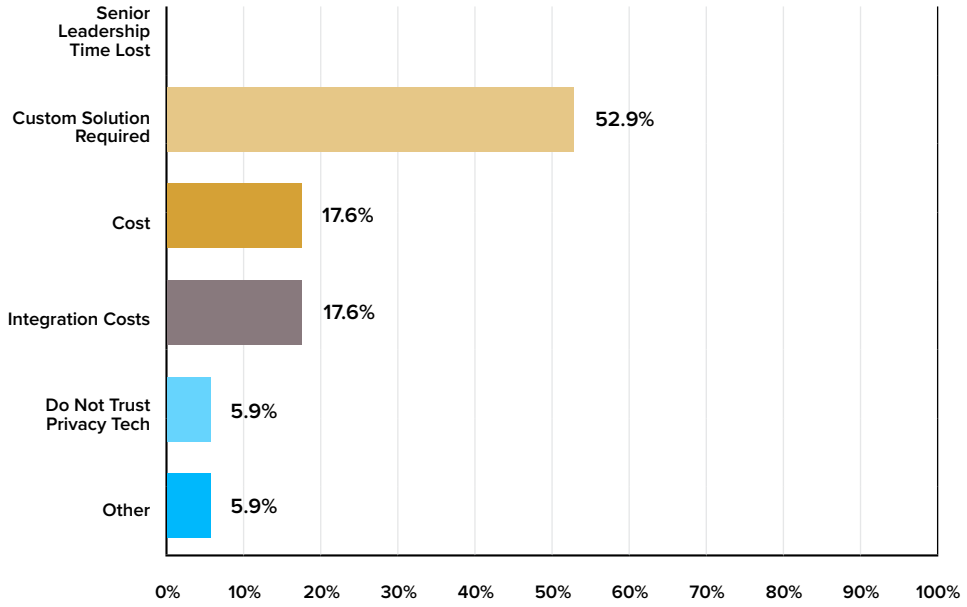


ANSWER CHOICES	RESPONSES	
Engineering talent diversion — it's costly to have our engineers building privacy compliance tools instead of our core product and service	41.2%	7
Speed — we want to get privacy tools in place quickly	47.1%	8
Legal or Regulatory Complexity — we want a third-party regulatory or legal expert to tell us what needs to be done	35.3%	6
Distraction — we just want to focus on our core products or services	23.5%	4
Cost — cost of deployment is more important than other factors	35.3%	6
Quality — we're concerned about a technology's functionality, security, and privacy measures. which may vary depending on who built it	52.9%	9
Integration Challenges — we find that integration of third-party software with our current technology stack is difficult, time-consuming, and/or resource-intensive	41.2%	7
Enterprise-Wide Solutions — we prefer to use multi-pronged technologies that work across the enterprise, rather than multiple bespoke solutions each used by different parts of the organization	41.2%	7
Other (please specify)	11.8%	2
TOTAL RESPONDENTS		17

Responses to "Other" (verbatim):

- Vendor background and capabilities
- Willingness of 3rd party to agree to contractual liability arising from processing personal information/data breaches.

Question 8: What might lead your company to decide to build your own privacy tools, rather than buy them from a third-party provider? Select one answer.



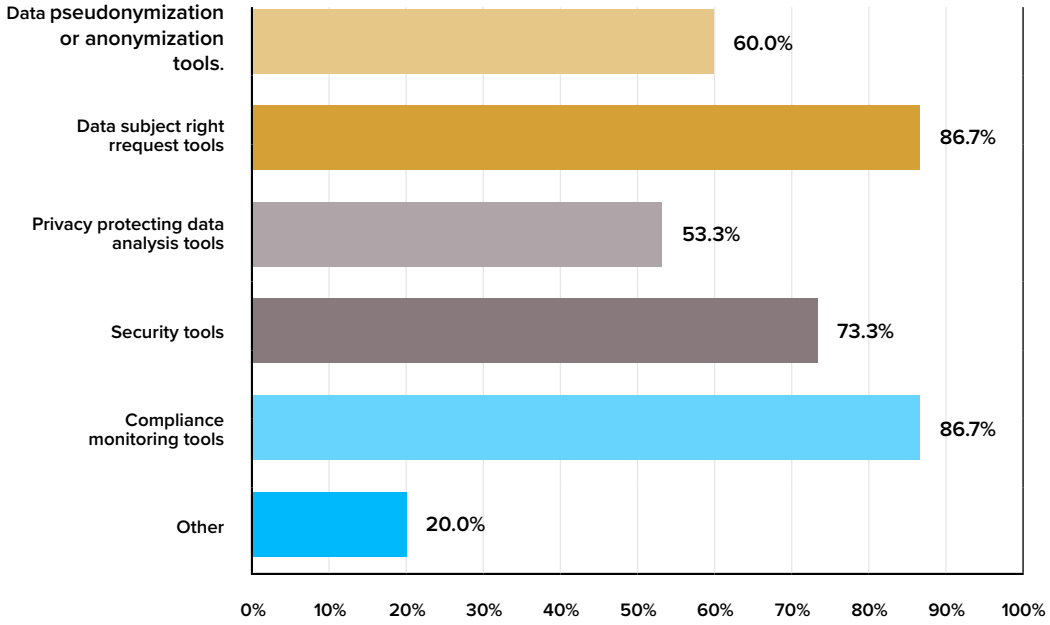
ANSWER CHOICES	RESPONSES	
Senior Leadership Time Lost — explaining our needs to third-party provider will take a precious time from our senior leadership that is needed for their core functions	0.0%	0
Custom Solution Required Due to Technical Complexity — our technologies or tools are not suited to off-the-shelf solutions, so we need to build this ourselves	52.9%	9
Cost — outsourcing this simply costs too much	17.6%	3
Integration Costs — integrating a third-party company's tools with our own distracts our engineers and/or takes too long	17.6%	3
Do Not Trust Privacy Tech — our company or leadership has had a bad experience previously with a third-party privacy service in the past	5.9%	1
Other (please specify)	5.9%	1
TOTAL RESPONDENTS		17

Responses to "Other" (verbatim):

- More flexibility with frameworks and controls

Question 9: Which privacy services would you consider purchasing from a third-party provider? Check all that apply.

Answered: 15



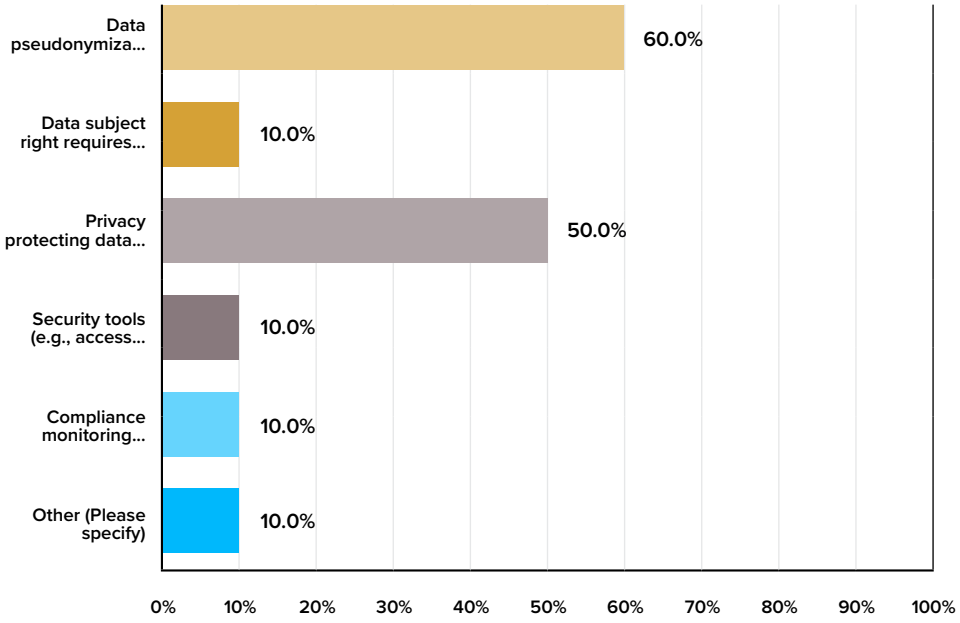
ANSWER CHOICES	RESPONSES	
Data pseudonymization or anonymization tools (e.g., de-identification)	60.0%	9
Data subject right request tools (e.g., portability)	86.7%	13
Privacy-protecting data analysis tools (e.g., differential privacy)	53.3%	8
Security tools (e.g., access controls)	73.3%	11
Compliance monitoring tools (e.g., for internal assessments)	86.7%	13
Other (please specify)	20.0%	3
TOTAL RESPONDENTS		15

Responses to “Other” (verbatim):

- Accountability tools
- Cookie management, data mapping
- Data mapping tools, cookie and consent management/tracking

Question 10: Are there any types of privacy-preserving technologies that you are considerably hesitant about purchasing or building in general, due to skepticism of their effectiveness or functionality? Check all that apply.

Answered: 10



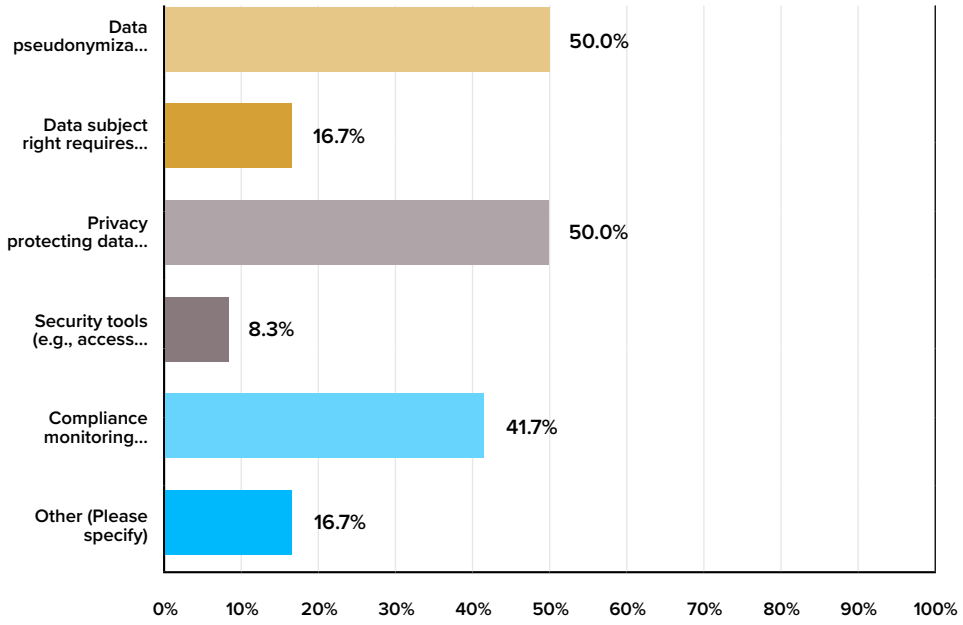
ANSWER CHOICES	RESPONSES	
Data pseudonymization or anonymization tools (e.g., de-identification)	60.0%	6
Data subject right request tools (e.g., portability)	10.0%	1
Privacy-protecting data analysis tools (e.g., differential privacy)	50.0%	5
Security tools (e.g., access controls)	10.0%	1
Compliance monitoring tools (e.g., for internal assessments)	10.0%	1
Other (please specify)	10.0%	1
TOTAL RESPONDENTS		10

Responses to “Other” (verbatim):

- Data discovery tools - they do not seem very mature yet

Question 11: Are there any types of privacy-preserving technologies which stand out as insufficiently supplied in the market? Check all that apply.

Answered: 12



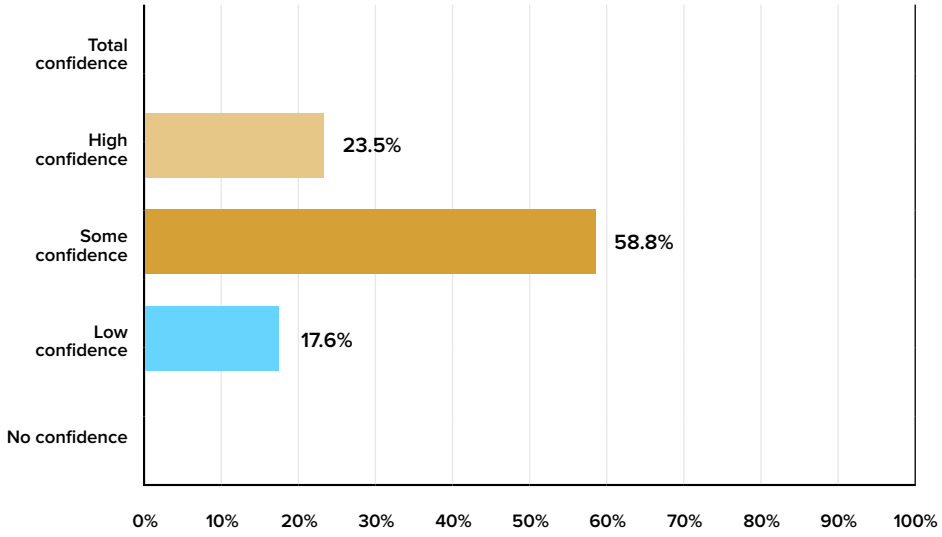
ANSWER CHOICES	RESPONSES	
Data pseudonymization or anonymization tools (e.g., de-identification)	50.0%	6
Data subject right request tools (e.g., portability)	16.7%	2
Privacy-protecting data analysis tools (e.g., differential privacy)	50.0%	6
Security tools (e.g., access controls)	8.3%	1
Compliance monitoring tools (e.g., for internal assessments)	41.7%	5
Other (please specify)	16.7%	2
TOTAL RESPONDENTS		12

Responses to “Other” (verbatim):

- Software development kits that provide individual rights requests, data retention, etc. functionalities that can be leveraged
- ID verification services

Question 12: Rate your confidence in third-party privacy technology suppliers' understanding of your organization's needs and resources. Select one answer.

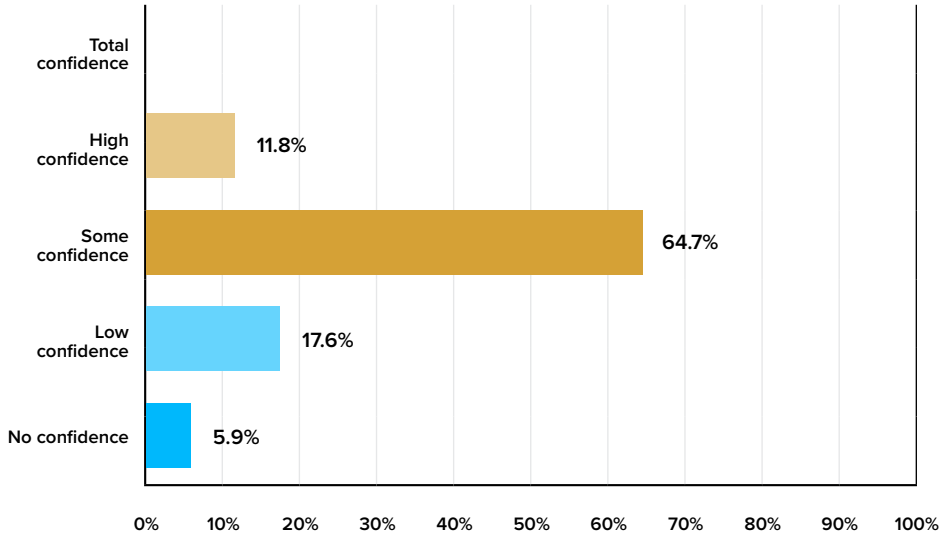
Answered: 17



ANSWER CHOICES	RESPONSES	
Total confidence	0.0%	0
High confidence	23.5%	4
Some confidence	58.8%	10
Low confidence	17.6%	3
No confidence	0.0%	0
TOTAL RESPONDENTS		17

Question 13: Rate your confidence in third-party privacy technology suppliers' integration with other privacy technologies—e.g., enabling of interoperability across multiple vendors and with different kinds of enterprise-side technologies and systems.

Answered: 17



ANSWER CHOICES	RESPONSES	
Total confidence	0.0%	0
High confidence	11.8%	2
Some confidence	64.7%	11
Low confidence	17.6%	3
No confidence	5.9%	1
TOTAL RESPONDENTS		17

Question 14: Please share your experience with privacy technology purchases? What should we know and what would you want privacy technology vendors to know?

Answered: 4

- Companies trust vendors that offer these services to support compliance with complex laws. But often the solutions are too simplistic or occasionally entirely unfit to support compliance. Buyers are becoming wary of this and the trust is eroding.
- The biggest issue we have when engaging vendors is scale. Only a few are ready to take on supporting the heterogeneous ecosystems of massive media companies.
- SAAS solution providers must be willing to bear the degree of risk presented from processing personal information in their own environments. With private rights of action across multiple states, the common "take it or leave it" refrain today will lead organizations to "leave it."
- The hype and marketing is absurd. The tools are decent, but they're tools, not magic bullets. Legwork is still required.

ENDNOTES

1 Although this report focuses on the business market, users of these services include government agencies, not for profits, and other sectors that manage personal data. However adoption in these sectors lags the business market and may provide future opportunities.

2 One leading vendor described Privacy Tech 3.0 as facilitating the embedding and enforcement of policies developed during the immediately preceding Layer 2 processes of "Information and data governance" and "Privacy management" into the data to enable predictable, auditable, and verifiable compliance while maximizing data utility and value to achieve data-driven business goals and objectives in a lawful and ethical, sustainable manner.

3 Acknowledgements: The authors would like to thank all of the experts, on both the buy and sell sides of the privacy tech market, who spoke on background for this report. Their insights were invaluable in better understanding the market, its present challenges, and its future directions. The authors would also like to thank the Future of Privacy Forum's Jules Polonetsky, John Verdi, and Barbara Kelly for their support and Limor Shmerling Magazanik, Managing Director of the Israel Tech Policy Institute and Senior Fellow at the Future of Privacy Forum, and Omer Tene, Vice President of Research for the International Association of Privacy Professionals, for their insights

4 Jules Polonetsky and Jeremy Greenberg, *NSF Convergence Accelerator: The Future of Privacy Technology* (C-Accel 1939288) (Washington, D.C.: Future of Privacy Forum, March 2020), https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel1939288_Public.pdf.

5 ISO standard ISO/IEC 20889:2018 for "Privacy enhancing data de-identification terminology and classification of techniques" addresses this in part, but it does not seem to be well-known to the relevant buyers.

6 General Data Protection Regulation. Text available online at: Intersoft Consulting, n.d., accessed July 24, 2020, https://gdpr-info.eu/.

7 "Step Aside GDPR, Brazil has a New Privacy Law That's Changing the Game," JD Supra, October 14, 2020, https://www.jdsupra.com/legalnews/step-aside-gdpr-brazil-has-a-new-19894/.

8 Rogier Creemers, Mingli Shi, Lauren Dudley, and Graham Webster, "China's Draft 'Personal Information Protection Law' (Full Translation)," New America, October 21, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/; Constantine Karbaliotis and Dustin Moores, "Federal privacy reform in Canada: The Consumer Privacy Protection Act," International Association of Privacy Professionals, November 18, 2020, https://iapp.org/news/a/federal-privacy-reform-in-canada-the-consumer-privacy-protection-act/.

9 California Consumer Privacy Act (CCPA). Text available online at: State of California Department of Justice, n.d., accessed July 24, 2020, https://oag.ca.gov/privacy/ccpa.

10 Geoffrey A. Fowler and Tonya Riley, "The Technology 202: Privacy advocates battle each other over whether California's Proposition 24 better protects consumers," *The Washington Post*, August 4, 2020, https://www.washingtonpost.com/politics/2020/08/04/technology-202-privacy-advocates-battle-each-other-over-whether-california-proposition-24-better-protects-consumers/.

11 Emerging Patchwork or Laboratories of Democracy? Privacy Legislation in Virginia and Other States, FPF, February 12, 2021, https://fpf.org/blog/emerging-patchwork-or-laboratories-of-democracy-privacy-legislation-in-virginia-and-other-states/

12 See, for example, Stacey Gray, Pollyanna Sanderson, and Katelyn Ringrose, "A New U.S. Model for Privacy? Comparing the Washington Privacy Act to GDPR, CCPA, and More," Future of Privacy Forum, February 12, 2020, https://fpf.org/2020/02/12/a-new-model-for-privacy-in-a-new-era-evaluating-the-washington-privacy-act/.

13 FTC Prepares to Expand Rulemaking, Including on Privacy and Data Use, JDSUPRA, Mar 31, 2021 https://www.jdsupra.com/legalnews/ftc-prepares-to-expand-rulemaking-7281226/.

14 Gené Teare, "Almost $10B Invested In Privacy And Security Companies In 2019," CrunchBase, January 29, 2020, https://news.crunchbase.com/news/almost-10b-invested-in-privacy-and-security-companies-in-2019/.

15 Paul Sawers, "5 data privacy startups cashing in on GDPR," Venture Beat, July 23, 2019, https://venturebeat.com/2019/07/23/5-data-privacy-startups-cashing-in-on-gdpr/.

16 "Privacy Tech Alliance," Future of Privacy Forum, https://fpf.org/privacy-tech-alliance/.

17 https://fpf.org/pepr21/; https://www.riseofprivacytech.com/.

18 Author conversation with Limor Shmerling Magazanik, July 30, 2020.

19 Tom Foster, "'A Growth Industry Like I've Never Seen': Inside America's No. 1 Fastest-Growing Company," *Inc*., September 2020.

20 See, for example, Jules Polonetsky and Elizabeth Renieris, Privacy 2020: 10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade (Washington, D.C.: January 2020), https://fpf.org/blog/privacy-2020-10-privacy-risks-and-10-privacy-enhancing-technologies-to-watch-in-the-next-decade/.

21 "Gartner Says Over 40% of Privacy Compliance Technology Will Rely on Artificial Intelligence in the Next Three Years," Gartner.com, February 25, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-02-25-gartner-says-over-40-percent-of-privacy-compliance-technology-will-rely-on-artificial-intelligence-in-the-next-three-years.

22 Jules Polonetsky and Elizabeth Renieris, Privacy 2020: 10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade (Washington, D.C.: January 2020), https://fpf.org/blog/privacy-2020-10-privacy-risks-and-10-privacy-enhancing-technologies-to-watch-in-the-next-decade/.

23 "Privacy Tech Alliance, https://fpf.org/privacy-tech-alliance/.

24 NIST is leading a number of privacy engineering initiatives. Further work may be needed to understand whether the NIST initiatives will support the short terms gaps identified by the vendors. See: U.S. National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

25 Extracting value is used in this report to capture a wide range of business activities, including analytics, research, improving the quality of services, and developing new products. Increasingly, the availability and utility of data for machine learning projects is an important consideration.

26 *How Privacy Tech Is Bought and Deployed* (Portsmouth: International Association of Privacy Professionals, 2019), https://iapp.org/media/pdf/resource_center/privacy_tech_bought_and_deployed_IAPPTrustArc_2019.pdf.

27 *Personal Data and the Organization: Stewardship and Strategy* (Washington, D.C.: Future of Privacy Forum, May 2019), https://fpf.org/wp-content/uploads/2019/05/FPF_DataRiskFramework_illo04.pdf.

28 The U.S. Sentencing Guidelines direct federal prosecutors and sentencing judges to evaluate corporate compliance programs, including consideration of "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one. See DOJ Updates Guidance on the Evaluation of Corporate Compliance Programs. https://corpgov.law.harvard.edu/2020/06/20/doj-updates-guidance-on-the-evaluation-of-corporate-compliance-programs/

29 That said, in non-legal terminology, most if not all data is personal data in the sense that data from one dataset which may seem unlinked to a particular individual can be paired with data from innumerable other datasets to identify specific individuals. See Dr. Latanya Sweeney's research: "Policy and law: Identifiability of de-identified data," http://latanyasweeney.org/work/identifiability.html.

30 Nate Velarde, "ESG Investing and Data Privacy," UC Berkeley School of Information, March 31, 2019, https://blogs.ischool.berkeley.edu/w231/2019/04/02/esg-investing-and-data-privacy/.

31 For instance, the firms might be talking about different levels of noise added to data. See: ISO - ISO/IEC 20889:2018 - Privacy enhancing data de-identification terminology and classification of techniques, https://www.iso.org/standard/69373.html; Isabel Wagner and David Eckhoff, "Technical Privacy Metrics: a Systematic Survey," arxiv.org, June 2018, https://arxiv.org/abs/1512.00327; and Josep Domingo-Ferrer, David Sánchez, Alberto Blanco-Justicia, "The Limits of Differential Privacy (and its Misuse in Data Release and Machine Learning)," arxiv.org, November 2020, https://arxiv.org/abs/2011.02352.

32 This reflects previous findings in a study conducted by FPF for the National Science Foundation: Jules Polonetsky and Jeremy Greenberg, *NSF Convergence Accelerator: The Future of Privacy Technology* (C-Accel 1939288) (Washington, D.C.: Future of Privacy Forum, March 2020), https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel1939288_Public.pdf.

33 For example: "Auritas and BigID Announce Strategic Partnership," MarTechSeries, August 21, 2020, https://martechseries.com/analytics/data-management-platforms/auritas-bigid-announce-strategic-partnership/; "Crownpeak and WireWheel Partner to Offer Powerful CCPA Privacy Tools," *BusinessWire*, November 14, 2019, https://www.businesswire.com/news/home/20191114005333/en/Crownpeak-and-WireWheel-Partner-to-Offer-Powerful-CCPA-Privacy-Tools; "OneTrust and The DMA Announce Strategic Partnership to Equip Marketers for GDPR and CCPA Success," OneTrust.com, August 12, 2019, https://www.onetrust.com/company/news/press-releases/onetrust-dma-uk-responsible-marketing-partner/.

34 Michael Vizard, "BigID's quick $1 billion-plus valuation shows rise of data intelligence and privacy," VentureBeat, December 17, 2020, https://venturebeat.com/2020/12/17/bigids-quick-1-billion-plus-valuation-shows-rise-of-data-intelligence-and-privacy/.

35 "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule," U.S. Department of Health & Human Services, n.d. (accessed October 2, 2020), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

36 See, for instance, Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman, "Exposed! A Survey of Attacks on Private Data," *Annual Review of Statistics and Its Applications* 4(12), 2017, https://privacytools.seas.harvard.edu/files/privacytools/files/pdf_02.pdf; Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets," University of Texas at Austin, https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf; Michael Barbaro and Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749," The New York Times, https://www.nytimes.com/2006/08/09/technology/09aol.html.

37 "Auritas and BigID Announce Strategic Partnership," MarTechSeries, August 21, 2020, https://martechseries.com/analytics/data-management-platforms/auritas-bigid-announce-strategic-partnership/.

38 "Crownpeak and WireWheel Partner to Offer Powerful CCPA Privacy Tools," BusinessWire, November 14, 2019, https://www.businesswire.com/news/home/20191114005333/en/Crownpeak-and-WireWheel-Partner-to-Offer-Powerful-CCPA-Privacy-Tools

39 "BigID and WireWheel Introduce Expanded Integration For Scaling DPIAs and RoPAs," https://wirewheel.io/resources/bigid-and-wirewheel-introduce-expanded-integration-for-scaling-dpias-and-ropas/, May 1, 2020.

40 Annie Greenley-Giudici, "TrustArc Partners with Alibaba Cloud," TrustArc, July 25, 2017, http://trustarc.com/blog/2017/07/25/trustarc-partner-alibaba-cloud/; "Evident Releases Mobile Application to Address Health Risks as Businesses Reopen," https://www.businesswire.com/news/home/20200515005057/en/Evident-Releases-Mobile-Application-to-Address-Health-Risks-as-Businesses-Reopen, May 15, 2020; "TrustArc and RADAR Partner to Power Comprehensive Privacy Solutions," https://trustarc.com/trustarc-and-radar-inc-partner-to-power-comprehensive-privacy-solutions-to-manage-global-compliance-requirements/, May 16, 2018.

41 "OneTrust and The DMA Announce Strategic Partnership to Equip Marketers for GDPR and CCPA Success," OneTrust.com, August 12, 2019, https://www.onetrust.com/company/news/press-releases/onetrust-dma-uk-responsible-marketing-partner/.

42 "OneTrust Announces Acquisition of Integris Software," International Association of Privacy Professionals, June 30, 2020, https://iapp.org/news/a/onetrust-announces-acquisition-of-integris-software/.

43 "Aura Acquires Digital Privacy and Security Company Pango: Expands Business Portfolio and Enhances Product Suite by Also Incorporating Figleaf and PrivacyMate Acquisitions," PR News Wire, https://www.prnewswire.com/news-releases/aura-acquires-digital-privacy-and-security-company-pango-301088715.html, July 7, 2020.

44 "Atlanta-Based OneTrust Raises $210M Series B, More Than Doubles Valuation to $2.7B," CrunchBase, February 20, 2020, https://news.crunchbase.com/news/atlanta-based-onetrust-raises-210m-series-b-more-than-doubles-valuation-to-2-7b/.

45 Onetrust hits $5.3 billion valuation, *Pitchbook*, April 9, 2021, https://pitchbook.com/newsletter/onetrust-hits-53b-valuation.

46 https://tracxn.com/d/companies/wirewheel.io, February 18, 2020.

47 "Securiti.ai Scores $50 million Series B to Modernize Data Governance," *TechCrunch*, January 28, 2020, https://techcrunch.com/2020/01/28/securiti-ai-scores-50m-series-b-to-modernize-data-governance/.

48 "BigID Raises $50 Million Series D," *CrunchBase*, January 6, 2020, https://news.crunchbase.com/news/bigid-reportedly-raises-50m-series-d/.

49 Michael Vizard, "BigID's quick $1 billion-plus valuation shows rise of data intelligence and privacy," *VentureBeat*, December 17, 2020, https://venturebeat.com/2020/12/17/bigids-quick-1-billion-plus-valuation-shows-rise-of-data-intelligence-and-privacy/.

50 "Almost $10 billion Invested in Privacy and Security Companies in 2019," *CrunchBase*, January 29, 2020, https://news.crunchbase.com/news/almost-10b-invested-in-privacy-and-security-companies-in-2019/.

51 "Epic Games Acquires Kid Tech Platform SuperAwesome," VentureBeat, September 25, 2020, https://venturebeat.com/2020/09/25/epic-games-acquires-kid-tech-platform-superawesome/.

52 Polonetsky and Greenberg, *NSF Convergence Accelerator*.

1400 EYE STREET NW | SUITE 450 | WASHINGTON, DC 20005 FPF.ORG | 202-768-8950