Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on

Advancing Privacy Enhancing Technologies

The Rise of Privacy Tech (TROPT)

The Rise of Privacy Tech's (TROPT)

Response to the White House Office of Science and Technology Policy's (OSTP)

Request for Information on Advancing Privacy Technologies

July 8, 2022

AUTHORED BY THE RISE OF PRIVACY TECH (TROPT)

Lourdes M. Turrecha (Founder, The Rise of Privacy Tech)

With leading privacy and technology domain experts and thinkers, including select TROPT Innovators members and TROPT Privacy Tech Visionaries

Melanie Ensign (CEO, Discernible)

John Gevertz (Former Chief Privacy Officer/SVP, VISA and ADP)

Dr. K Royal (Chief Privacy Officer, Outschool, Inc.)

Dr. Mary Berk (Founder, Bluestreak Product Advisors)

Alexandra Ross (Senior Director, Senior Data Protection, Use & Ethics Counsel, Autodesk)

Gilbert Hill (Chief Strategy Officer, Pool Data)

Fatima Khan (Advisor, The Rise of Privacy Tech)

Debra Farber (Advisor, The Rise of Privacy Tech)

In consultation with other unnamed privacy and technology domain experts and thinkers

And researched by

Ece Gumusel (Researcher & Associate, The Rise of Privacy Tech)

TABLE OF CONTENTS

EXECUTIVE SUMMARY OF THE RISE OF PRIVACY TECH'S NATIONAL PRIVACY TECH STRATEGY RECOMMENDATIONS

The Rise of Privacy Tech (TROPT) submits these recommendations to the White House Office of Science and Technology Policy's (OSTP) request for information (RFI)[i] to help inform the development of a national strategy on privacy tech.

TROPT is the only formal privacy tech community. TROPT community members control significant market power to build, invest in, design, and implement emerging privacy technologies. TROPT's mission is to fuel privacy tech and innovation. We do this by breaking down silos and bridging the gaps between privacy tech key players: founders of privacy tech startups, privacy tech investors, privacy domain experts who are privacy tech board advisors, privacy tech buyers and users, and other privacy professionals with the experience to integrate these technologies into corporate systems and consumer products. In this executive summary, we highlight seven (7) critical recommendations for the future of privacy tech and innovation that apply directly to OSTP's stated objectives for developing a national strategy on privacy tech.

1. The White House national privacy tech strategy should standardize definitions.

Words matter. To be effective in the development of a national strategy on privacy tech, there must be clarification and standardization of what mean by *privacy tech*, *privacy enhancing technologies (PETs)*, and related terminology. The lack of a universally accepted definition[ii] brings up questions of scope and allows organizations to misrepresent the purpose, use, and effectiveness of their privacy tech solutions.

There is currently no universally accepted definition of PETs. While PETs have come up in several failed bills and congressional hearing transcripts, it remains undefined under US law. Even in academia, researchers use different PETs definitions, or avoid defining the term altogether.

During the June 7, 2022 Fast Track Action Committee (FTAC) roundtable meeting, there was much debate among attendees about the use of appropriate terminology. The OSTP's RFI acknowledges this tension as follows: "For the purposes of this RFI, privacy-enhancing, privacy-preserving, and privacy-protecting are used as equivalent terms."[iii]

At TROPT, we've kickstarted the work of defining *privacy tech* and exploring its relationship to *PETs* and related terminology in the foundational *TROPT Defining the Privacy Tech Landscape Whitepaper 2021*.[iv] We did this because having a baseline understanding of privacy tech's scope helps facilitate healthy debate and avoid talking past each other. Some may argue that definitions are mere semantics, but being clear about what we're talking about has significant implications, for buyers purchasing privacy tech, investors investing money into privacy tech, and founders building privacy tech. A common starting point saves us valuable time and resources and enables us to instead focus on the greater goal of moving the needle on privacy and true privacy tech solutions. We offer this existing work as a starting point, not the end goal.

2. The White House national privacy tech strategy should broadly address privacy tech in general, not just PETs.

At TROPT, we focus broadly on *privacy tech* (versus solely on *PETs*) because privacy tech appropriately encapsulates the breadth of technical solutions needed to solve privacy problems. We define *privacy tech* as technological solutions to privacy problems or privacy harms.[v]

TROPT PRIVACY TECH DEFINITION

SOURCE: TROPT DEFINING THE PRIVACY TECH LANDSCAPE WHITEPAPER 2021

In addition to refraining from focusing solely on PETs, we've described the relationship between privacy tech and PETs:

> "PETs unfortunately do not have a universally accepted definition. That said, the OECD defines PETs as "a "wide range of technologies that help protect privacy,"[vi] aiming to give the individual user (in a consumer context) or technology manager (in an organizational environment) the capability of controlling if, how much, or under what circumstances

personal information is disclosed. Therefore, based on this commonly used OECD PETs definition, PETs are privacy tech. But privacy tech tools are not necessarily always PETs because privacy tech solves for other privacy problems beyond control over personal information.

Another second widely cited definition of PETs is: a coherent system of technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.[vii] Under this second common PETs definition, a technology that blocks online ad tracking would not be a PET because it interferes with system functionality, but it would certainly be privacy tech because it solves for a privacy problem: an individual's choice not to be tracked. In comparison, a technology that allowed ad personalization while giving users control over their personal information would be a PET under this second definition and, therefore also qualify as privacy tech because it both solves for a privacy problem (individual control over their personal information) without losing ad functionality.

Finally, S.224, the recently introduced Promoting Digital Privacy Technologies Act, defines PETs as "any software solution, technical processes, or other technological means of enhancing the privacy and confidentiality of an individual's personal data in data or sets of data."[viii] S.224's PETs definition also falls under privacy tech because any software solution, technical process, or other technological means that enhances the privacy and

confidentiality of an individual's personal information in data or sets of data qualify as technological solutions to privacy problems."[ix]

3. The White House national privacy tech strategy should broadly address privacy technologies throughout the data lifecycle.

The White House OSTP's RFI focuses on "privacy-preserving data sharing and analytics,"[x] which could suggest that only privacy tech during the data *use* and *sharing* stages of the data lifecycle are in scope of the RFI and the resulting national policy.

Privacy protections must be bound to the data objectives themselves, so that organizations and consumers have reassurance that the appropriate privacy protections are enforced throughout the data lifecycle. By the time data is collected and reaches the data *use* and *sharing* stages of the data lifecycle, transparency, data minimization, and other privacy principles are often violated already.

As such, TROPT proposes that the national policy broadly address privacy tech throughout the data lifecycle, from collection, to and use and sharing, and up to storage, retention, and deletion.

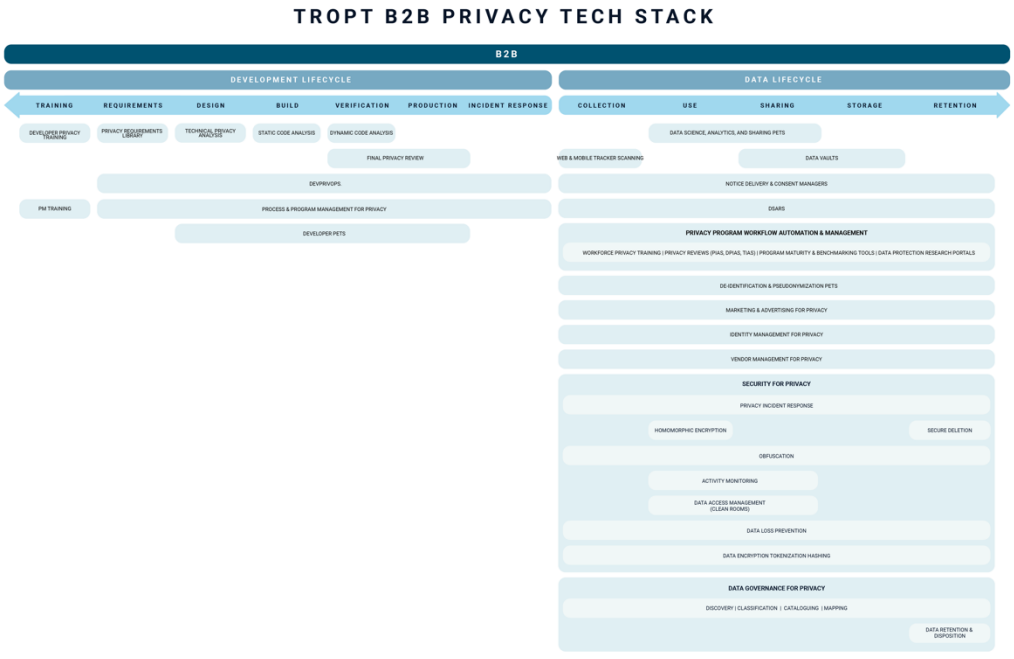
4. The White House national privacy tech strategy should also broadly address privacy technologies throughout the technology development lifecycle.

In addition to broadening the scope to privacy tech that solve privacy problems throughout the entire data lifecycle, we urge the White House to further broaden its scope by "shifting privacy left" to the technology development lifecycle. The technology development lifecycle is where many privacy decisions are made, even before data is collected, used, shared, stored, retained,

and deleted. Many privacy problems arise from the development of technologies without regard to privacy, resulting to decades worth of privacy technical debt.

At TROPT, we reported on the trend involving privacy tech tools during the development lifecycle: from developer privacy training, privacy code scanners, privacy requirements libraries, synthetic data for testing, etc.[xi] These developers are equally—if not more—deserving of strategic highlight and support given they anticipate and solve privacy problems before they're created. Development lifecycle privacy tech tools also help organizations adhere to global data protection rules requiring privacy by design and default.

Figure 1: TROPT B2B Privacy Tech Stack
showing privacy technologies under both the data and development lifecycles.



SOURCE: TROPT DEFINING THE PRIVACY TECH LANDSCAPE WHITEPAPER 2021

5. The White House national privacy tech strategy should prioritize adoption incentives ahead of research initiatives at this time.

Academics, researchers, and technologists have been conducting PETs research since at least the 1980s. There is an existing wealth of PETs research from academia, industry, and the public sector. In academia, we have Carnegie Mellon's CyLab Privacy & Security Institute[xii] and Harvard's Privacy Tools Project[xiii]. From industry, we have Apple's Differential Privacy research[xiv] and Google's differential privacy library.[xv] And in the public sector, the National Science and Technology Council (NSTC) has issued a report[xvi] detailing a national privacy research strategy, and referencing the PETs research initiatives the federal government has engaged in.

While research is clearly important, it's hardly enough to move us to the next stage: widespread privacy tech adoption. Research is not where we fall short on privacy tech. Instead, we need adoption incentives, including the following:

a. Market funding towards privacy tech

In addition to funding privacy tech research, we need to fund privacy tech solutions that are mature enough to go to market. The United States Government can fulfill this need. The same way that In-Q-Tel invested in important cybersecurity developments, the U.S. Government can invest in the emerging privacy tech industry.

The U.S. Government, through the Securities & Exchange Commission (SEC), could also incentivize investors to fund privacy tech—which aligns with the broader Environmental, Social,

and Governance (ESG) and impact investing trends in venture capital—or require them to be more transparent about their investments (or lack thereof) in privacy tech.

b. An equal playing field for privacy-preserving business models

Successful privacy tech adoption depends in part on appropriate business models. Several privacy tech companies that have made it to market have failed because they were competing against companies with anti-privacy business models, such as those rooted in the opaque monetization of personal data. Thus, the national strategy should also encourage an equal playing field for privacy-preserving business models, including those that include ownership-, value-, and profit-sharing with individuals.

c. Economies of scale through incentives and disincentives

To help privacy tech startups entering the market, the national privacy tech policy could play an external role in developing economies of scale. The national policy could pursue the introduction of tax breaks for startups with privacy tech products and/or to privacy tech users, similar to the tax incentives historically offered to climate tech or any other industry that the U.S. Government supports. The national policy could explore preferential treatment for privacy tech vendors in government contracts or introduce actual privacy tech requirements in government contracts through the Federal Acquisition Regulation (FARs).

In addition, the national policy could require or incentivize Big Tech players to accommodate PETs in the infrastructure they build and offer. Some Big Tech companies have already dipped their toes into PETs waters, largely due to brand incentives. But for those which haven't, perhaps

the national policy could pursue the introduction of disincentives, such as disqualification from government contracts and tax breaks.

d. A privacy by design agenda in privacy law

Beyond advancing privacy tech, the national policy should play a bigger role in mandating privacy design and engineering of technologies, in general. Leading privacy thinker, Professor Woodrow Hartzog, outlines this proposal in his book, *Privacy's Blueprint: The Battle to Control the Design of New Technologies.*[xvii] Additionally, there is a wealth of proposals and ideas on privacy by design and privacy engineering from leading privacy technologists and academics, such as former Canadian Privacy Commissioner Dr. Ann Cavoukian,[xviii] Dr. Lorrie Cranor,[xix] Michelle Finneran-Dennedy,[xx] and R. Jason Cronk,[xxi] to name a few. Building on this solid foundation would provide a quicker path to success.

6. The White House national privacy tech strategy should be technology neutral.

Much has been said about the need for privacy tech—and specifically, PETs--in the context of artificial intelligence (AI) and machine learning (ML) technologies. We agree. That said, we urge the White House to develop its national privacy tech strategy in a technology neutral way, and not focus solely on AI and ML (or other specific) technologies.

We urge a technology neutral approach because privacy problems arise with every major technological advancement, from the invention of the portable camera and the proliferation of smart phones, to the advent of cloud computing, the Internet of Things (IoT), and now AI and ML. We are already seeing privacy problems arise with Web 3.0 technologies, as we build the next Internet age. With the benefit of privacy and technology history in mind, the national

privacy tech strategy should be technology neutral, transcending technological trends like AI and ML and applying to emerging technologies.

This means the national strategy needs to go beyond supporting only PETs used in the context of AI and ML and extend to many other privacy tech use cases.

7. Proposed vision for the White House national privacy tech strategy: a world where technology is designed and engineered with privacy in mind, to serve individuals and society, respecting and securing their rights to privacy, self-sovereignty, and self-determination.

At TROPT, we believe that privacy is a critical component in designing and building technology to serve people. Privacy design and engineering are prerequisites for product excellence, creating privacy value. Privacy tech and innovation offers market opportunities to those who can recognize the value of privacy, beyond compliance. We see a world where technology is designed and engineered with privacy in mind, to serve individuals and society, respecting and securing their rights to privacy, self-sovereignty, and self-determination.[xxii] Mainstream privacy tech adoption can help get us there by providing solutions to a broad array of privacy problems that harm individuals and society and infringe on their rights to privacy, self-sovereignty, and self-determination.

TROPT'S RESPONSES TO OSTP'S RFI

Having laid out our seven (7) critical recommendations for a national privacy tech strategy in the previous section, we now turn to our specific responses to each of OSTP's ten (10) requests for information:

1. White House OSTP RFI on specific research opportunities to advance privacy tech

Information about Federal research opportunities that could be introduced or modified to accelerate the development or adoption of PETs. This includes topics for research, hardware and software development, and educational and training programs. This also includes information about specific techniques and approaches that could be among the most promising technologies in this space.

TROPT response to specific research opportunities to advance privacy tech

We recommend the following research opportunities to advance privacy tech:

- Carnegie Mellon University CyLab PETs research initiatives, under Dr. Lorrie Cranor's leadership[xxiii]
- The numerous technical privacy research projects presented at USENIX's PEPR conference[xxiv]
- The upcoming TROPT Privacy Tech Stack Whitepaper 2022

2. White House OSTP RFI on specific technical aspects or limitations of privacy tech

Information about technical specifics of PETs that have implications for their development or adoption. This includes information about specific PET techniques that are promising, recent or

anticipated advances in the theory and practice of PETs, constraints posed by limited data and computational resources, limitations posed by current approaches to de-identification and deanonymization techniques, limitations or tradeoffs posed when considering PETs as well as technical approaches to equity considerations such as fairness-aware machine learning, security considerations based on relevant advances in cryptography or computing architecture, and new or emerging privacy-enhancing techniques. This also includes technical specifications that could improve the benefits or privacy protections or reduce the risks or costs of adopting PETs.

TROPT response to specific technical aspects or limitations of privacy tech

As privacy tech industry leaders and privacy practitioners in the tech industry, we've seen the following privacy tech limitations:

- Immaturity of privacy tech solutions
- Limited scalability of privacy tech solutions
- Commercial viability of privacy tech solutions
- Limited interoperability with existing systems
- Lack of privacy tech awareness and understanding among potential adopters
- False tradeoffs between usability and privacy

3. White House OSTP RFI on specific sectors, applications, or types of analysis that would particularly benefit from the adoption of privacy tech

Information about sectors, applications, or types of analysis that have high potential for the adoption of PETs. This includes sectors and applications where data are exceptionally decentralized or sensitive, where PETs could unlock insights or services of significant value to

the public, where PETs can reduce the risk of unintentional disclosures, where PETs might assist in data portability and interoperability, and sectors and applications where the adoption of PETs might exacerbate risks, including in the areas of privacy, cybersecurity, accuracy of data analysis, equity for underserved communities, and economic competition. This topic covers opportunities to improve the effectiveness of data sharing among specific Federal agencies and between specific Federal agencies and entities outside the Federal Government, including the goals outlined in Section 5 of Executive Order 14058: Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government.

TROPT response to specific sectors, applications, or types of analysis that would particularly benefit from the adoption of privacy tech

As privacy tech industry leaders and privacy practitioners in the tech industry, we've seen the following applications:

- Privacy code scanners to identify privacy problems in products before they're launched
- Privacy tech for secondary use, including in the context of data science and analytics (for marketing, trends, insights, etc.) especially in regulated industries like healthcare, finance, education
- Privacy tech for data retention and end-of-life
- Privacy tech (*e.g.*, tokenization) for payment processing
- Use of synthetic data (instead of real personal data) during product testing
- Privacy tech allowing for the processing of personal data for cybersecurity threat and response analysis

- Privacy tech providing automated and accurate just-in-time transparency
- Privacy tech solutions in smart cities and urban planning
- Privacy tech to facilitate safety in edtech and children-directed technologies

4. White House OSTP RFI on specific regulations or authorities that could be used, modified, or introduced to advance PETs

Information about Federal regulations or authorities that could be used, modified, or introduced to accelerate the development or adoption of PETs. This includes privacy-related rulemaking authorities under the Office of Management and Budget, the Federal Trade Commission, and financial regulatory bodies, as well as acquisition regulations under the Federal Acquisition Regulations. This also includes the Federal authority to set procedures for agencies to ensure the responsible sharing of data. This also covers hiring authorities to recruit Federal employees with expertise to advance PETs, as well as acquisition authorities (*e.g.,* Other Transaction Authority) to procure PETs for development.

TROPT response to specific regulations or authorities that could be used, modified, or introduced to advance PETs:

- Federal privacy authorities like the FTC, CFPB, SEC, HHS, DoT, and DoJ
- Federal privacy laws, regulations, and standards like HIPAA, COPPA, GLBA, FERPA, FARs, FedRAMP, and SEC disclosure requirements
- NIST standards, perhaps a introducing a new framework for privacy technologies

5. White House OSTP RFI on specific laws that could be used, modified, or introduced to advance privacy tech

Information about provisions in U.S. Federal law, including implementing regulations, that could be used, modified, or introduced to accelerate the development or adoption of PETs. This includes provisions, safe harbors, and definitions of use, disclosure, safeguards, and breaches. Information may also include comments on how to advance PETs as part of new or proposed legislation, such as that which would create a National Secure Data Service. Information may also include comments on State law or on international law as it applies to data sharing among international entities.

TROPT response to specific laws that could be used, modified, or introduced to advance privacy tech:

We recommend pursuing the following to promote privacy tech:

- The Promoting Digital Privacy Technologies Act (S.224 / H.R. 847)[xxv] with recommended improvements[xxvi]
- A comprehensive federal data protection law that includes the promotion of privacy tech *and* that closes loopholes on surveillance technologies used in public-private data sharing
- Revisions to COPPA that would promote privacy tech in protecting children, including requirements for educational settings
- Revisions to HIPAA to update the Security Rule and enhance the Privacy Rule to specifically address privacy tech

6. White House OSTP RFI on specific mechanisms, not covered above, that could be used, modified, or introduced to advance privacy tech

This includes the development of open-source protocols and technical guidance, the use of public-private partnerships, prize challenges, grants, testbeds, standards, collaborations with foreign countries and nongovernmental entities, the Federal Data Strategy, and data sharing procedures with State, local, tribal, and territorial governments. This also includes interpretations and modifications of standard non-disclosure agreements, confidentiality clauses, data use or sharing agreements, etc.

TROPT response to specific mechanisms, not covered above, that could be used, modified, or introduced to advance privacy tech

At TROPT, we are open to exploring the following additional mechanisms to advance privacy tech:

- Public-private partnerships to fuel the emerging privacy tech industry
- Privacy tech startup innovation prize challenges, grants, and testbeds, potentially in partnerships with privacy tech startup accelerator and university incubator programs
- Creation of open-source protocols and technical guidance
- Privacy tech education and awareness initiatives, including TROPT whitepapers and TROPT events (*e.g.*, TROPT Data Privacy Day/Week, TROPT Privacy Tech Summit, and TROPT Webcasts) and USENIX's PEPR conferences

7. White House OSTP RFI on risks related to privacy tech adoption

Identification of risks or negative consequences resulting from PETs adoption as well as policy, governance, and technical measures that could mitigate those risks. This includes risks related to equity for underserved or marginalized groups, the complexity of implementation and resources required for adoption, as well as from conceptual misunderstandings of the technical guarantees provided by PETs. This also includes recommendations on how to measure risk of PETs adoption and conduct risk-benefit analyses of use.

TROPT response to risks related to privacy tech adoption

As privacy tech industry leaders and privacy practitioners in the tech industry, we've seen the following privacy tech adoption risks:

- Conflicting technologies leading to lack of interoperability, adoption failure, and wasted resources
- Introduction of complexity, including process complexity, leading to adoption failure and wasted resources
- Introduction of new privacy and security vulnerabilities
- Lack of scalability leading to adoption failure and wasted resources
- Limitation or inhibition of future legitimate data uses

We at TROPT are willing to engage in conversations about the risks of privacy tech and PETs adoption, including demystifying false tradeoffs; measuring, quantifying, and remediating legitimate risks; and developing risk-benefit analysis guidance that the industry could use in their

adoption considerations. These could be especially helpful for emerging startups that lack the internal resources to develop their own privacy and security controls.

8. White House OSTP RFI on existing best practices that are helpful for privacy tech adoption

Information about U.S. policies that are currently helping facilitate adoption as well as best practices that facilitate responsible adoption. This includes existing policies that support adoption, including in the areas of privacy, cybersecurity, accuracy of data analysis, equity for underserved communities, and economic competition. This also includes information about where and when PETs can be situated within tiered access frameworks for accessing restricted data, ranging from publicly accessible to fully restricted data.

TROPT response to existing best practices that are helpful for privacy tech adoption

We recommend the following resources for privacy tech adoption best practices:

- The foundational TROPT Defining the Privacy Tech Landscape Whitepaper 2021[xxvii]
- The upcoming TROPT Privacy Tech Stack Whitepaper 2022
- Luk Arbuckle & Khaled El Imam's *Building an Anonymization Pipeline: Creating Safe Data*[xxviii]

9. White House OSTP RFI on existing barriers, not covered above, to PETs adoption

Information about technical, sociotechnical, usability, and socioeconomic barriers that have inhibited wider adoption of PETs, such as a lack of public trust. This includes recommendations

on how such barriers could be overcome. Responses that focus on increasing equity for underserved or marginalized groups are especially welcome.

TROPT response to existing barriers, not covered above, to PETs adoption

As privacy tech industry leaders and privacy practitioners in the tech industry, we've seen the following privacy tech adoption barriers:

- Limited or competing budget and resources for privacy tech acquisition, development, and implementation
- Lack of (business & legal) incentives for privacy tech adoption
- Limited internal technical privacy expertise needed for privacy tech adoption
- Lack of awareness of privacy tech opportunities
- Largely academic versus practical privacy tech focus
- Privacy tech and PETs vendors' own inadequate privacy and security controls, with varying underlying causes (budget, buy-in, market focus, awareness, leadership and team without privacy and security expertise)
- Inconsistent definitions, as discussed in the previous section
- Existing silos between technologists, investors, academic researchers, practitioners, and buyer-users
- Lack of privacy (and greater ethical) development, leading to systemic biases resulting from inequity of available data (in other words, we need cross-functional experts from historically underserved minority populations to be instrumental in developing and addressing privacy tech – as engineers, creators, founders, advisors, and executives)

The solution for many of the above problems is appropriate incentives. Organizations are prone to engage in: 1) what is profitable (or satisfies their corporate mission); 2) what their customers want; and 3) what the law requires.

10. White House OSTP RFI on other information that is relevant to the adoption of PETs

Information that is relevant to the adoption of PETs that does not fit into any of the topics enumerated above.

TROPT response to other information that is relevant to the adoption of PETs

In addition to the above, we recommend exploring the following privacy tech initiatives:

- Small-to-medium business (SMB) insights and incentives in the form of grants, etc.
- Balanced/reasonable/supported barriers to privacy tech entry
- Right-sized privacy tech adoption resources toolkits for different organizations (*e.g.*, startups, SMBs, enterprise, Big Tech)

REFERENCES

[i] *Request for Information on Advancing Privacy-Enhancing Technologies*. (2022, June 9). Federal Register. https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies.

[ii] Office of the Privacy Commissioner of Canada, "Privacy Enhancing Technologies -- A Review of Tools and Techniques," November 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/ (last accessed July 2022).

[iii] *See i.*

[iv] Turrecha, L., Ashley, E., et al. (2021). *The Rise of Privacy Tech Defining the Privacy Tech Landscape 2021*. https://www.riseofprivacytech.com/wp-content/uploads/2021/11/TROPT-Defining-the-Privacy-Tech-Landscape-2021-v1.0-1.pdf.

[v] *See iv.*

[vi] OECD Working Party on Information Security and Privacy, "Inventory of Privacy-Enhancing Technologies (PETs)," January 7, 2002,

https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/ reg%282001%291/final (last accessed July 2022).

[vii] John J. Borking and Charles Raab. "Laws, PETs, and Other Technologies for Privacy Protection." Journal of Information, Law, and Technology, 1:1–14, 2001.

[viii] S.224 Promoting Digital Privacy Technologies Act, Introduced February 4, 2021, https://www.congress.gov/ bill/117th-congress/senate-bill/224/text (last accessed July 2022).

[ix] *See iv.*
[x] *See i.*

[xi] *See iv.*
[xii] Carnegie Mellon University CyLab *Directory*. Retrieved July 8, 2022, from https://www.cylab.cmu.edu/directory/index.html.
[xiii] *Harvard University Privacy Tools Project*. (n.d.). Retrieved July 8, 2022, from https://privacytools.seas.harvard.edu/.
[xiv] Apple Machine Learning Research. Retrieved July 8, 2022, from https://machinelearning.apple.com/research.
[xv] *Differential Privacy*. (2022). [C++]. Google. https://github.com/google/differential-privacy (Original work published 2019).
[xvi] Blumenthal, M., Brooks, S., Lefkovitz, N., & Vagoun, T. (n.d.). *National Privacy Research Strategy*. 34. https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf
[xvii] Hartzog, W. (2018). *Privacy's Blueprint*. Harvard University Press.

[xviii] Cavoukian, A. (2010). Privacy by Design The 7 Foundational Principles. *Information and Privacy Commissioner of Ontario*.
[xix] L. F. Cranor and N. Sadeh, "A Shortage of Privacy Engineers," in *IEEE Security & Privacy*, vol. 11, no. 2, pp. 77-79, March-April 2013, doi: 10.1109/MSP.2013.25.

[xx] Finneran-Dennedy, M., Fox, J., and Finneran, T.R. (2014). *The Privacy Engineer's Manifesto Getting from Policy to Code to QA to Value*. Apress Berkeley, CA.

[xxi] Cronk, R.J. (2022). *Strategic Privacy By Design*. (2nd ed.). International Association of Privacy Professionals.
[xxii] Turrecha, L. (2021, October 7). The "Why?" Behind The Rise of Privacy Tech. *The Rise of Privacy Tech*. https://medium.com/the-rise-of-privacy-tech/the-why-behind-the-rise-of-privacy-tech-2335f96a53be.

[xxiii] *CyLab Security & Privacy Institute*. (n.d.). Retrieved July 8, 2022, from https://www.cylab.cmu.edu/index.html.
[xxiv] *PEPR '22*. (2021, December 14). USENIX. https://www.usenix.org/conference/pepr22
[xxv] Stevens, H. M. (2022, May 12). *H.R.847 - 117th Congress (2021-2022): Promoting Digital Privacy Technologies Act* (2021/2022) [Legislation]. http://www.congress.gov/.

[xxvi] Turrecha, L. (2021, February 16). On Regulating Privacy Enhancing Technologies (PETs) Through the Promoting Digital Privacy Technologies Act (S.224)—What It Is, What's Good About It, How To Improve It. *Privacy & Technology Publication*. https://medium.com/privacy-

technology/on-regulating-privacy-enhancing-technologies-pets-through-the-promoting-digital-privacy-ad2d63570551.

[xxvii] *See iv.*

[xxviii] Arbuckle, L. and El Emam, K. (2020). *Building an Anonymization Pipeline: Creating Safe Data*. Press by O'Reilly Media, Inc.

NOVEMBER 2021

THE RISE OF PRIVACY TECH

DEFINING THE PRIVACY TECH LANDSCAPE 2021

A FOUNDATIONAL WHITEPAPER TO HELP FUEL PRIVACY INNOVATION

AUTHORED BY

THE RISE OF PRIVACY TECH

Lourdes M. Turrecha and Emily Ashley

In collaboration with the TROPT Privacy Tech Landscape Working Group members:
Nishant Bhajaria, Mary Berk, Michelle Finneran-Dennedy, Melanie Ensign, Debra Farber, Kiran Gopinath, Kelly Huang, Gilbert Hill, Fatima Khan, Cillian Kieran, Carolyn Krol, David Kruger, Caroline McCaffery, Kevin Riggle, and Alexandra Ross.

In consultation with leading privacy & technology domain experts and thinkers, some of whom are quoted in this whitepaper, and others who wish to remain anonymous in their valuable contributions.

THE RISE OF
PRIVACY TECH

The Rise of Privacy Tech's mission is to fuel privacy innovation. We do this by bringing together privacy tech founders, investors, domain experts, and advocates and bridging the tech-capital-expertise gaps in privacy.

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The emerging privacy tech industry is on the rise. For the first time in history, founders, technologists, investors, regulators, consumers, and enterprise customers are in agreement with privacy domain experts and consumer advocates that privacy is one of the most critical issues of our time. We need privacy innovation to help solve our privacy problems and the resulting mounting privacy technical debt. An increasing demand for privacy designed and engineered tools accompanies this fortuitous timing. In turn, an uptick in technologists and founders are rising to the occasion to build solutions to some of these privacy problems and seize the resulting market opportunities.

But at this nascent time, the privacy tech key players—founders, investors, domain experts, and user-buyers—aren't connected enough to move things forward at the pace the market needs. They're not even on the same chapter—let alone page—in their understanding of privacy or privacy tech. In this foundational whitepaper, we start to bridge the gaps between the key players in privacy tech.

We start off by defining privacy tech, which requires understanding privacy. We provide a summary of different privacy conceptualizations from leading privacy thinkers. We do this for several reasons. First, key players are unnecessarily talking past each other as they discuss the emerging privacy tech landscape. Second, this lack of a baseline understanding of privacy introduces friction, and, in certain contexts, prevents key players from moving forward with a partnership, purchase, investment, or other step towards fueling privacy tech and innovation.

As part of this exercise, we also summarize common privacy principles, introduce The Rise of Privacy Tech (TROPT)'s own set of privacy tech principles, and explore privacy tech's relationship with frequently conflated terms like cybersecurity, privacy engineering, privacy by design, and so on.

We then categorize privacy tech. To do so, we introduce the TROPT Privacy Tech Stack, pulling from foundational privacy and technology knowledge. We plan to update and use the TROPT Privacy Tech Stack to categorize the privacy tech landscape as it matures. We expect the privacy tech stack to evolve as the industry evolves, and we welcome feedback to help capture this evolution.

We also surveyed key players in privacy tech to hear about their different pain points, the privacy problems they're solving for, the solutions they're building or buying, and the challenges they face at this early stage in the privacy tech industry.

Lastly, we share insights from the forefront of the privacy tech industry, with recommendations on how we can collectively keep fueling privacy tech and innovation. We outline proposed responses to what we learned from this endeavor. Most importantly, we call for each key player to join us in fueling privacy tech, with specific recommendations on how to do so.

INTRODUCTION

There is increasing interest in the nascent privacy tech landscape.

Entrepreneurs are building solutions in response to privacy and data protection problems. As of the publication of this white paper, multiple indicators point to rapid growth in the privacy tech industry.

The Crunchbase database lists 945 companies that identify themselves as privacy companies.[1] The Rise of Privacy Tech (TROPT)'s own ongoing research identifies 745 privacy tech companies.[2]

Investor interest in funding privacy tech startups is equally strong and growing. Even in the midst of the pandemic when funding was reportedly stalled, funding towards privacy tech startups continued.[3] Investors have reportedly poured in almost six billion US dollars (specifically, $5.9B) in cumulative funding towards emerging privacy companies; four billion ($4B) in the past three years alone.[4]

Recent years saw high growth and demand for privacy tech in the market. Last year, the privacy tech industry produced two unicorns,[5] startups valued at more than a billion dollars. In the midst of the pandemic, the tech industry as a whole also embraced privacy tech in various forms, such as COVID-19 tools touting privacy features,[6] including Apple and Google's joint contact tracing proposal.[7] Apple's recent iOS 14[8] and 15[9] releases included a slew of privacy tech features.

In the consumer space, individuals' concern over their privacy led to their increased adoption of consumer privacy tech, including private messaging app, Signal, which reached peak status as the top downloaded app[10] during last year's wave of national protests in support of the Black Lives Matters movement. Signal downloads surged again during the last US national elections and in early 2021 after Elon Musk urged his Twitter followers to "Use Signal."[11]

Consumers are increasingly becoming aware of other privacy tech tools available on the market and switching to privacy-protective alternatives like Brave, DuckDuckGo, and ProtonMail, which have reported similar increased adoption as privacy preserving alternatives to existing privacy-invasive browsers, search engines, and email. As of September 2021, the privacy-focused web browser Brave reported thirty-six million monthly active users. Brave's ad platform revenue has grown fourteen times in the last eighteen months.[12] The privacy-forward search engine, DuckDuckGo, reported over one-hundred million downloads since 2018, with over half of those downloads taking place in the past year.[13] ProtonMail, which offers encrypted emails, reported five million users in 2018[14] and have now surpassed fifty million users in 2021.[15]

Beyond consumer privacy tech, B2B privacy tech has taken off even faster. Most privacy tech tools are built in—and investments are poured into—the B2B side. This reality is reflected in the TROPT Privacy Tech Stack, which shows a more mature B2B side compared to the B2C and B2B2C sides.

These sample indicators clearly show that privacy tech is on the rise, but the understanding of what constitutes privacy tech remains low.

What exactly is privacy tech?

DEFINING PRIVACY TECH

As the privacy tech landscape continues to grow, it's critical to define and understand what qualifies as privacy tech for several reasons.

First, having a baseline understanding of privacy tech's scope helps facilitate healthy debate and avoid talking past each other. Some may argue that definitions are mere semantics, but being clear about what we're talking about has significant implications, for buyers purchasing privacy tech, investors investing money into privacy tech, and founders building privacy tech. A common starting point saves us valuable time and resources and enables us to instead focus on the greater goal of moving the needle on privacy and true privacy tech solutions.

Second, defining privacy tech forces transparency, which is a key privacy principle. Consumer and business customers deserve to know whether the privacy-branded tools they're using are actually privacy tech solutions.

Privacy tech boundaries also help customers better identify true privacy tech from tools that don't actually solve privacy problems. For example, while tools in the adjacent industries may sometimes overlap with privacy tech, customers deserve to know when they are and aren't privacy tech.

Having a clear understanding of what constitutes privacy tech helps fuel the privacy tech industry's success. By being clear about what privacy tech is, we weed out products that aren't privacy tech. This improves the privacy tech landscape's success as it matures and strengthens the privacy tech market's long-term viability. In turn, this means better privacy tech tools for both businesses and consumers.

DEFINING THE OPERATIVE TERMS

To define and understand privacy tech, we must first understand the operative terms: ***privacy*** and ***technology***. Fortunately, and credit to leading privacy thinkers, both privacy and technology are well-covered and explored concepts.

What is privacy?

Different schools of thought have offered different privacy definitions and conceptualizations. We summarize some of the common ones in Figure 1 in the following page.

WHAT IS PRIVACY?

CONTRARY TO POPULAR MYTH, PRIVACY IS NOT JUST SECRECY OR ANONYMITY.

PRIVACY AS CONTROL

Perhaps the most commonly accepted definition of information privacy focuses on individual control over personal data, including how much of it is disclosed and to whom, as well as how it should be maintained and disseminated. Under this school of thought, privacy is individuals' claim to determine for themselves when, how, and to what extent personal information about them is communicated to others. ***Alan Westin, Privacy and Freedom***

PRIVACY AS OBSCURITY

Obscurity is the idea that information is safe—at least to some degree—when it is hard to obtain or understand. ***Evan Selinger and Woodrow Hartzog, Obscurity and Privacy***

PRIVACY AS TRUST

Privacy has also been conceptualized as trust, with four foundations: (1) the commitment to be honest about data practices, (2) the importance of discretion in data usage, (3) the need for protection of personal data against outsiders, and (4) the overriding principle of loyalty to the people whose data is being used, so that it is data and not humans that become exploited. Trust is important in forging information relationships in today's networked, data-driven society. ***Neil Richards and Woodrow Hartzog, Privacy's Trust Gap***

Trust expectations make privacy expectations reasonable. Trust greases the wheels of effective sharing by encouraging interactions and information sharing. ***Ari Ezra Waldman, Privacy as Trust: Sharing Personal Information in a Networked World***

PRIVACY AS POWER

Privacy as power builds on privacy as choice and provides support for users to exercise their power and take back control over their personal data in a world where personal data is constantly being harvested and exploited through a surveillance economy. ***Carissa Véliz, Privacy is Power***

PRIVACY AS CONTEXTUAL INTEGRITY

Privacy norms or expectations vary by context. Contextual integrity links privacy protection to norms for specific contexts, so that "information gathering and dissemination are appropriate to that context and obey the governing norms of distribution within it. ***Helen Nissenbaum, Privacy as Contextual Integrity***

A TAXONOMY OF PRIVACY

As detailed above, privacy can mean different things to different people. Perhaps the most comprehensive conceptualization of privacy is Daniel Solove's A Taxonomy Privacy, a framework for understanding privacy in a pluralistic and contextual manner, grounded in the different kinds of activities that impinge upon privacy. This conceptualization shifts the focus away from the vague term "privacy" and toward the specific activities that pose privacy problems. ***Daniel J. Solove, Understanding Privacy*** and ***A Taxonomy of Privacy***

Figure 1. What Is Privacy?
Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

TROPT embraces a multi-faceted understanding of privacy covering individual control over personal information,[16] including the exercise of individual power,[17] and facilitating trust in personal information relationships.[18] We also embrace the comprehensive taxonomical approach to conceptualizing privacy based on the activities that impinge upon privacy: information collection, information processing, information dissemination, and invasions.[19] We reject the limited conceptualization of privacy as secrecy, obscurity, or anonymity only.

What are privacy principles?

In addition to the different schools of thought defining privacy, privacy regulators and practitioners have historically talked about privacy in terms of privacy principles, often referred to as fair information practice principles or FIPPs. Different organizations have offered their own set of privacy principles. While these principles are not consistent across the board, they're largely similar and overlap, except for a handful.[20]

Figure 2: Table of Different Privacy Principles[21]
Source: TROPT Defining the Privacy Tech Landscape 2021

	OECD	GDPR	DHS	IAPP	PIPEDA	FTC	TROPT
ACCESS / PARTICIPATION						✓	
ACCOUNTABILITY		✓	✓	✓	✓		✓
ACCURACY / DATA QUALITY	✓		✓	✓	✓		
CHALLENGING COMPLIANCE					✓		
CHOICE / CONSENT					✓	✓	
COLLECTION LIMITATION	✓			✓	✓		
DATA MINIMIZATION		✓	✓				✓
ENFORCEMENT / REDRESS						✓	
INDIVIDUAL PARTICIPATION	✓		✓	✓			
INDIVIDUAL CONTROL							✓
INDIVIDUAL ACCESS					✓		
INTEGRITY / CONFIDENTIALITY		✓					
INTEGRITY / SECURITY						✓	
LAWFULNESS, FAIRNESS, AND TRANSPARENCY		✓					
LIMITING USE, DISCLOSURE, AND RETENTION					✓		
OPENNESS / TRANSPARENCY / NOTICE / AWARENESS	✓	✓	✓	✓	✓	✓	
PURPOSE LIMITATION	✓						✓
PURPOSE SPECIFICATION			✓	✓	✓		
SECURITY	✓		✓	✓	✓		
STORAGE LIMITATION / RETENTION		✓					✓
TRANSPARENCY							✓
USE LIMITATION	✓		✓	✓			✓

What are TROPT's Privacy Tech Principles?

We reviewed existing privacy principles and articulate seven TROPT Privacy Tech Principles. We chose six historical privacy principles that apply to privacy tech: transparency, purpose & use limitation, data minimization, individual control, security for privacy, and accountability. We add privacy by design given its importance in the design and development of products, systems, and processes that touch personal information and therefore impact privacy. We purposefully omitted lawfulness/fairness and individual redress from the TROPT Privacy Tech Principles given these two principles involve legal privacy issues, which are not solvable through technology.

TROPT'S PRIVACY TECH PRINCIPLES

TRANSPARENCY

The Transparency privacy principle requires organizations processing personal data to inform and obtain consent from individuals for the processing of their personal data. Transparency is typically required when information is collected and before the data processing scope is expanded beyond the original scope. That said, many believe that organizations should have transparent data processing practices throughout the entire data lifecycle.

Privacy tech examples: consent managers, just-in-time notices, and audio and video indicator lights that notify a user when an app is accessing audio or a green dot when an app isaccessing video.

INDIVIDUAL CONTROL

The Individual Control privacy principle provides that individuals should have control over their personal data. Global privacy laws have defined individual privacy rights to include individuals' ability to access, delete, correct, and consent or object to the processing of the personal data that organizations have collected about them. Individual control is relevant throughout the entire data life cycle.

Privacy tech examples: data subject access requests (DSARs), consent management tools, data wallets, and the Global Privacy Control (GPC) protocol.

PURPOSE & USE LIMITATION

The Purpose & Use Limitation privacy principle means that organizations must limit the scope of their data processing solely to the purpose and use specified when data was collected from an individual. This principle comes into play after data is collected and remains a factor until that data is deleted.

Privacy tech examples: Data vaults, data wallets, and some privacy enhancing technologies (PETs) like zero knowledge proofs (ZKP).

DATA MINIMIZATION

Data Minimization requires organization to only process personal data that is relevant and necessary to meet their specified purposes. Data minimization applies throughout the data lifecycle, from collection and use to storage and retention.

Privacy tech examples: data disposition tools and PETs like differential privacy, secure multi-party computation (SMPC), ZKP, edge computing, and local processing address data minimization.

SECURITY FOR PRIVACY

The Security for Privacy principle refers to the need to specifically secure individual privacy, including individual personal data. In addition to building proper structures and using reasonable methods to secure data, security requires data accuracy, integrity, and quality.

Privacy tech examples: homomorphic encryption, access controls, and data disposition tools.

ACCOUNTABILITY

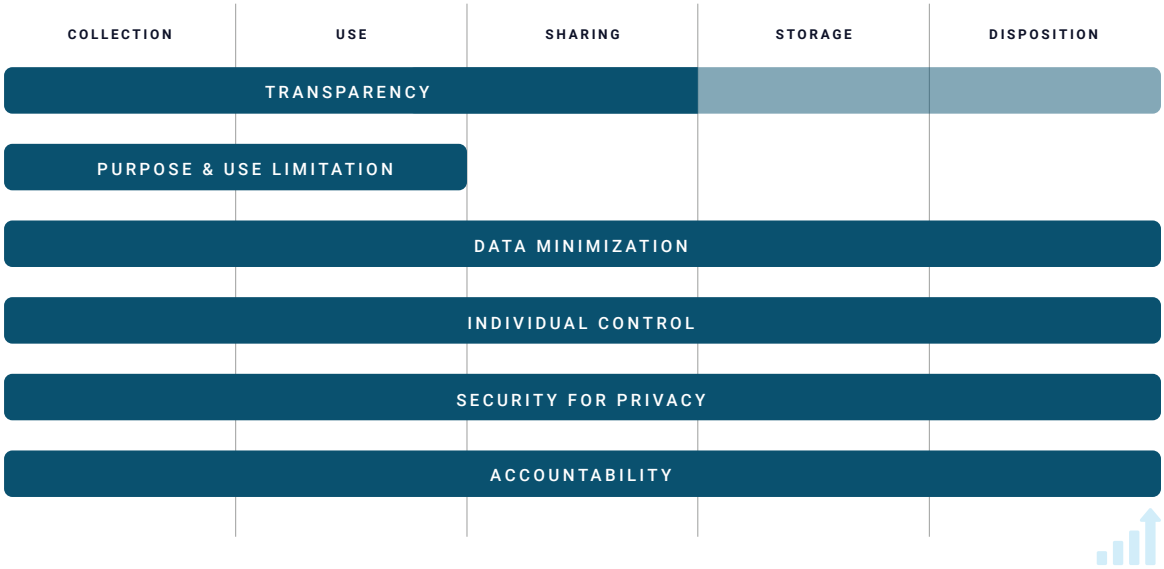
The Accountability privacy principle describes an organization's obligation to demonstrate the internal privacy program, processes, and controls it has in place for processing personal data. The need to be accountable for personal data spans across the entire data life cycle. Organizations need tools to help demonstrate their accountability, spurring many opportunities for privacy tech solutions in recent years, especially in light of global data protection laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Privacy tech examples: data governance for privacy (discovery, inventory, mapping, and cataloging) tools, vendor management tools, privacy program workflow automation tools, and the broader data protection compliance tech solutions that automate privacy program workflows and manage data protection compliance.

Figure 3. TROPT Privacy Tech Principles
Source: TROPT Defining the Privacy Tech Landscape 2021

Each of the TROPT Privacy Tech Principles ties to at least one stage of the data life cycle. We illustrate this in Figure 4 below, which will come in handy in the next section, where we introduce the TROPT Privacy Tech Stack.

Figure 4. TROPT Privacy Tech Principles & the Data Lifecycle
Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021



What is technology?

Technology is "scientific knowledge used in practical ways in industry, for example in designing new machines."[22] Technology is also defined as "the use of science in industry, engineering, etc. to invent useful things or to solve problems."[23]

What is privacy tech, then?

Putting the two operative terms together, privacy technologies are simply solutions to privacy problems.[24]

As explored above, these privacy problems could cover individual control over personal information,[25] including exercises of individual power,[26] or facilitating trust in personal relationships,[27] perhaps through accountability and compliance initiatives. These privacy problems could also cover any one of the seven TROPT Privacy Tech Principles: transparency, purpose & use limitation, data minimization, individual control, security for privacy, accountability, and privacy by design. Privacy technologies solve for any number of these privacy problems, which pop up in many different contexts.

privacy tech

pri·va·cy·tech | \ ˈprī-və-sēˈtek

1 (noun) technological solutions to privacy problems.

2 (noun) emerging industry of tech companies building solutions to privacy problems, in an effort to address the mounting privacy technical debt.

COMPARING PRIVACY TECH TO OFTEN CONFLATED CONCEPTS

Privacy and privacy tech are often conflated with several other concepts and terminologies. Below, we explore privacy tech's relationship with some of these concepts, including data protection, privacy enhancing technologies (PETs), privacy by design (PbD), privacy engineering, security, privacy-first, and anonymity.

Data protection. Some privacy practitioners distinguish between the terms "privacy" and "data protection." For example, the EU defines privacy as the "respect for private and family life" and data protection as the "protection of personal data."[28] In practice, data protection focuses on improving organizations' data protection practices, while privacy focuses on honoring individuals' privacy preferences. While there are merits to making such a distinction, for the purpose of defining the privacy tech landscape, we hold the semantics and opt for simplicity given our intended broad audience of privacy tech founders and investors, in addition to the domain expert-advisors and user-buyers. In other words, we also consider as privacy tech those tools that solve for data protection problems.

PETs. PETs unfortunately do not have a universally accepted definition.[29] That said, the OECD defines PETs as "a wide range of technologies that help protect privacy,"[30] aiming to give the individual user (in a consumer context) or technology manager (in an organizational environment) the capability of controlling if, how much, or under what circumstances personal information is disclosed. Therefore, based on this commonly used OECD PETs definition, PETs are privacy tech. But privacy tech tools are not necessarily always PETs because privacy tech solves for other privacy problems beyond control over personal information. Another second widely cited definition of PETs is: a coherent system of technology measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.[31] Under this second common PETs definition, a technology that blocks online ad tracking would not be a PET because it interferes with system functionality, but it would certainly be privacy tech because it solves for a privacy problem: an individual's choice not to be tracked. In comparison, a technology that allowed ad personalization while giving users control over their personal information would be a PET under this second definition and, therefore also qualify as privacy tech because it both solves for a privacy problem (individual control over their personal information) without losing ad functionality.[32] Finally, S.224, the recently introduced Promoting Digital Privacy Technologies Act, defines PETs as "any software solution, technical processes, or other technological means of enhancing the privacy and confidentiality of an individual's personal data in data or sets of data."[33] S.224's PETs definition also falls under privacy tech because any software solution, technical process, or other technological means that enhances the privacy and confidentiality of an individual's personal information in data or sets of data qualify as technological solutions to privacy problems.

Figure 5. PETs & Privacy Tech
Source: TROPT Defining the Privacy Tech Landscape 2021

PbD. As covered in the previous section, lowercase privacy by design simply means privacy aforethought, whereas Dr. Anne Cavoukian's uppercase Privacy by Design articulates the following specific privacy design goals: 1) privacy should be proactive (not reactive) and preventative (not remedial); 2) privacy should be the default setting; 3) privacy should be embedded into design; 4) privacy should not impair full functionality (thus achieving a positive-sum, not zero-sum); 5) it should include end-to-end security to enable full lifecycle protection; 6) it should allow for visibility and transparency (keeping it open); and 7) design should be user-centric and pay respect to user privacy.[34] Bringing these concepts together, privacy tech is one of the tangible outputs of both theoretical lowercase privacy by design and uppercase Privacy by Design goals.[35]

Privacy engineering. Privacy engineering refers to the discrete discipline or field of inquiry and innovation using engineering principles and processes to build controls and measures into processes, systems, components, and products that enable the authorized, fair, and legitimate processing of personal data.[36] Privacy engineering provides the discipline (or the how) for translating privacy by design principles (or the what), to an output, such as a process, a feature, or even a privacy tech tool.[37]

Security. While security and privacy intersect, the two domains are distinct. Information privacy is concerned with the collection, use, dissemination, retention, and other processing of personal information, including the associated individual rights that empower individuals to take control over their personal information. Information security, on the other hand, is concerned with the confidentiality, integrity, and availability of information (not just personal information, but also trade secrets, intellectual property, and other information that warrants securing) and the systems that process such information. Privacy has its set of principles, as covered above. Security also has its own set of principles, covering confidentiality, integrity, and accuracy (the CIA triad). Security is one of the main privacy principles—in other words, privacy requires security. Given the relationship between the two, there is a category of privacy tech tools that specifically address the security of personal information and therefore overlap with security solutions.

Privacy-first. In addition to PETs, privacy tech also includes "privacy-first" tools, a term used to describe products that provide their service in a privacy-forward way.[38] Their service's primary purpose is not to solve for a privacy problem. Instead, their primary purpose could be anything else, including search (in the case of DuckDuckGo), browsing (Brave), and messaging (Signal). That said, these products solve privacy problems despite their non-privacy primary purpose. Brave solves for privacy problems in web browsing; DuckDuckGo, in search; and Signal, in messaging. Because their primary purpose is not privacy, one could argue that the term "privacy-first" is an ill-fitting term for such tools. Other more appropriate terms could be "privacy-forward," "privacy-friendly," or simply, "privacy tech." Setting aside the appropriate label, at the end of the day, these tools solve privacy problems (albeit as a secondary purpose), and therefore fall under the broader umbrella of privacy tech.

Anonymity. With today's government surveillance and surveillance capitalism double whammy, it's not surprising that a slew of anonymity tech tools have popped up. Anonymity tech are tools that help users remain anonymous online. These

include Tor,[39] certain Zero Knowledge Proofs (ZKPs) roll-ups to blockchain, and other cryptographic technologies that solve for anonymity. As covered above, privacy is by no means anonymity. Under the privacy as choice and privacy as power schools of thought, privacy covers other individual choices and exercises of power over personal information, beyond the choice to remain anonymous. Anonymity is merely one way to exercise privacy choice—it's an incomplete take on privacy but is still an important aspect of it. Anonymity tech solves for an individual's problem stemming from a desire to remain anonymous in certain contexts in this highly connected and surveilled world. Because privacy includes individual choice, the choice to remain anonymous in certain contexts often raises privacy problems when not honored. This means that anonymity tech is covered under the broader umbrella of privacy tech.

COMPARING PRIVACY TECH TO ADJACENT INDUSTRIES

There are several adjacent industries that overlap with privacy tech, but do not fall entirely within privacy tech. These industries include cybersecurity, data infrastructure, identity management, adtech and martech, legaltech, data governance, and Web 3.0. We explore and distinguish these industries from privacy tech below.

Cybersecurity

Privacy and cybersecurity are perhaps the closest overlapping industries, but are not one-and-the-same. Cybersecurity and privacy tech products protect personal information, but cybersecurity goes beyond protecting personal information and extends more broadly to protecting systems, networks, devices, and infrastructure, in their entirety. Conversely, privacy tech products do more than just protect personal information; they also solve other types of privacy problems beyond insecurity, like transparency, data minimization, purpose and use limitation, etc. It bears noting that cybersecurity tools are not privacy-preserving by default; on the contrary, when not designed and engineered with privacy in mind, these tools often raise privacy issues such as surveillance and overcollection of personal information.

Identity management

Identity management technologies are tools for identifying, authenticating, and authorizing an individual or a group of individuals.[40] Identity management products include tools for governing and administering unique user digital representations.[41] Identity management overlaps with privacy tech because both solve for problems relating to individual control over their identity, accuracy of personal information relating to identity, and secure access tied to identity-based personal information. That said, identity management tech goals extend beyond solving for privacy problems.

Data infrastructure

Data infrastructure tools promote data sharing and consumption.[42] They cover data sources like SQL databases, cloud storage providers, data warehouses, and business intelligence tools. These tools process personal information, among other information types. Data infrastructure products were not historically built with privacy in mind. The data infrastructure space overlaps with the privacy tech space because some privacy tech tools address data infrastructure privacy problems.

Martech & adtech

Marketing technology, or "martech" is "a set of software solutions used by marketers to support mission-critical business objectives and drive innovation within their organizations. Martech solutions focus on content and customer experience, advertising, direct marketing, marketing management and marketing data and analytics."[43] Martech products solve marketing problems and include digital asset management, marketing automation, chatbots, and social media monitoring tools. Advertising technology, or "adtech," refers to analytics and technical tools used in the advertising space that help advertisers reach their target audiences.[44] Because adtech solutions generally rely on consumer data, privacy is a necessary consideration when building these products, especially in light of increasing global data protection laws. Similar to the data infrastructure space, adtech is adjacent to privacy tech because adtech raises privacy problems, some of which require privacy tech solutions. That said, the two spaces are distinct: adtech primarily solves for advertising problems, whereas privacy tech solves for privacy problems. Overlapping adtech and privacy tech startups provide solutions for privacy problems in advertising. Adtech and martech are getting disrupted by privacy tech, partly due to Google's phasing out of third-party cookies, Apple's rollout of platform privacy requirements and restrictions, and the passage of global data protection laws.

Legal tech

Legal tech generally covers products that legal teams use to facilitate their processes and improve their effectiveness, including maintaining simple, efficient legal operations. Legal tech provides operational and administrative solutions for document or contract management, legal research, case or practice management, and client intake automation. Legal tech is also on the rise and has already seen over $1billion in funding in 2021.[45] Legal tech overlaps with privacy tech by offering data protection law compliance tools and privacy legal workflow automation tools.

Data governance

Data governance is "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods."[46] Data governance for privacy tools cover products that help Information Technology (IT), Governance, Risk, and Compliance (GRC), and privacy teams govern data, including data discovery, inventory, mapping, cataloging tools. Data governance overlaps with privacy tech where it uses technical solutions to manage privacy program management or data protection compliance, which often involve governing personal information.

Web 3.0

Web 3.0 is the next stage of the Internet. Because this stage is currently still being built, it has no universal definition yet. In practice, however, Web 3.0 refers to an Internet that is made possible by decentralized networks. The Web3 Foundation refers to Web 3.0 as "a decentralized and fair internet where users control their own data, identity, and destiny."[47] Web 3.0 and privacy tech both have the shared goal of enabling user control over their personal information and identity. That said, privacy tech covers more than just Web 3.0 technologies, and vice versa.

Notwithstanding the intersections with the aforementioned adjacent industries, privacy tech is an emerging industry on its own, focusing on technical tools that specifically aim to solve privacy problems.

CATEGORIZING PRIVACY TECH: THE TROPT PRIVACY TECH STACK

But What is a Tech Stack?

A technology stack is simply a collection of different technologies that work together for some purpose, usually as a foundation for systems such as websites, mobile apps, and standalone desktop software.

Figure 6. Sample Existing Tech Stacks
Source: TROPT Defining the Privacy Tech Landscape 2021

In addition to defining privacy tech in the previous section, we now introduce the TROPT Privacy Tech Stack as a framework for categorizing privacy tech startups.

The challenge with creating a privacy tech stack is that personal information runs through almost every type of system: websites, mobile, desktop software, and SaaS. There are existing tech stacks for these different systems, into which different privacy tech tools can fit neatly.

Despite the challenge, we've taken a stab at visually articulating the emerging privacy tech stack, pulling from foundational privacy and technology knowledge.

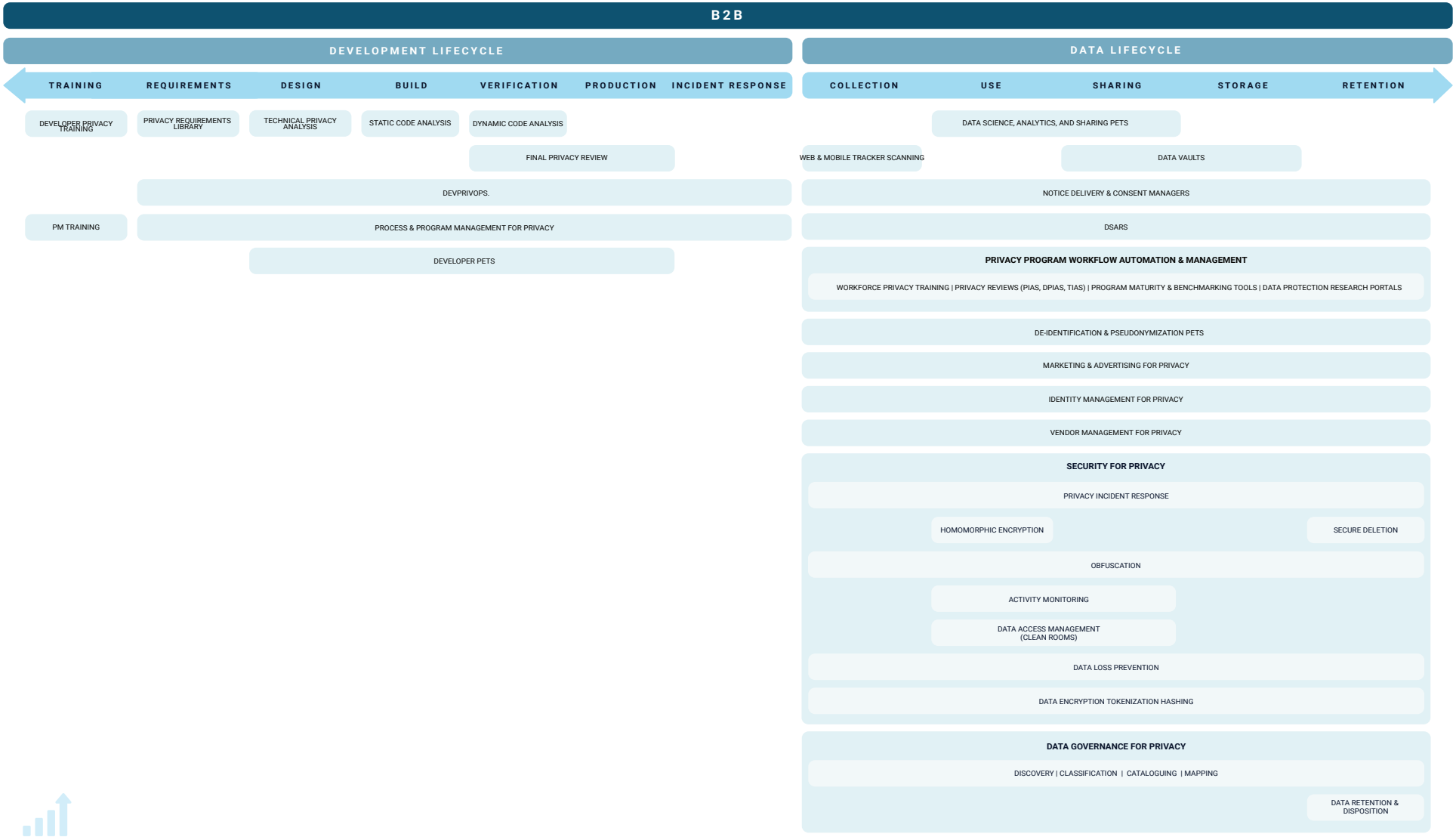
We start with the B2B side of the TROPT Privacy Tech Stack, which organizes the privacy tech tools that organizations use to solve privacy problems throughout the personal data lifecycle. Data lifecycle privacy tech products are built for privacy lawyers, Information Security (InfoSec) Governance, Risk, and Compliance (GRC) professionals, data scientists, and other professionals whose work involves personal information. Then, we took a first stab at fleshing out the B2B development lifecycle side of the TROPT Privacy Tech Stack in line with the "shift left privacy" trend, which reflects the desire to solve privacy problems earlier on, shifting left from the data lifecycle to the development lifecycle. This side includes privacy tech tools needed during the development cycle, when products and systems are built, before personal information is processed. Development lifecycle privacy tech products are built for professionals involved in the development lifecycle, which primarily include developers, program managers, and privacy engineers.
We then cover the B2C and B2B2C privacy tech developments we're seeing. B2C and B2B2C privacy tech are trailing behind the B2B side of privacy tech, which has seen most of the action in product development and investment dollars.

THE TROPT PRIVACY TECH STACK

The TROPT Privacy Tech Stack categorizes privacy tech based on where they fall under the data lifecycle (because data privacy is concerned with personal data) and the development lifecycle (because many privacy problems arise even before personal information is collected, when decisions are made at the development stage).

Figure 7. TROPT B2B Privacy Tech Stack

Source: TROPT Defining the Privacy Tech Landscape 2021



B2B PRIVACY TECH TOOLS: DATA LIFECYCLE TOOLS

Most of the mature privacy tech solutions fall under the B2B data lifecycle side of the TROPT Privacy Tech Stack. We break down the data lifecycle according to the following phases: collection, use, sharing, storage, and disposition. We cover some data lifecycle privacy tech categories in the following sections.

Notice delivery and consent managers

Notice delivery privacy tech tools inform individuals when their data is being collected or, if notice is required at a later stage of the data lifecycle, when their data is processed for a new purpose or shared with third parties beyond the scope of the original purpose. Examples include just-in-time notifications or the colored lights that indicate when an application is using a device's microphone or camera. Consent management tools are another example; they request, store, and enforce individual consent preferences. Cookie consent managers are a specific and common example of consent management tools. Notice delivery and consent managers apply throughout the data lifecycle.

Web & mobile tracker scanning

In 2020, at least eighty-seven percent (87%) of the most popular websites in the world engaged in some form of digital tracking, even when the website visitor did not sign into an account on the site.[48] Web and mobile tracking scanners are tools that give organizations visibility into the trackers on their websites, apps, and other assets. These tools scan websites and apps to reveal cookies, beacons, pixels, etc. crawling on the site or app.[49] These products typically sit at the data collection points.

Data science, analytics, and sharing PETs

Data science, data analytics, and data sharing privacy enhancing technologies (PETs) allow organizations to analyze and share personal information--and thus unleash its value—in a privacy—respectful way. These PETs provide data scientists, marketers, customer service teams, and any data-driven organization, insights about people, including their customers, while building in privacy into the analytics and sharing environment. Data science, analytics, and sharing PETs are used during the use and sharing phases of the data lifecycle.

These include products that incorporate differential privacy, Secure Multi-Party Computation (SMPC), Zero Knowledge Proofs (ZKPs), and other PETs.[50]

Data vaults

Data vaults are secure data storage and data sharing systems that allow organizations to interoperate across different systems while minimizing data privacy and security risks.[51] Data vaults often leverage PETs. Data vaults are used during the sharing and storage phases of the data lifecycle.

Data subject access rights (DSARs)

B2B Data Subject Access Rights (DSAR) tools facilitate organizations' responses to individual exercises of their data subject rights provided under global data protection laws, such as the General Data Protection Regulation (GDPR), the California Privacy Rights Act (CPRA), and the Virginia Consumer Data Protection Act (VCDPA).[52] Data

subject rights empower people to access, correct, delete, port, or otherwise exercise control over the personal information that organizations have collected on them. B2B DSAR tools help organizations handle intake, routing, execution, and/or response to DSAR requests. These tools are used throughout the data lifecycle.

Identity management for privacy
As covered under the adjacent industries section, the scope of identity management extends beyond privacy, but privacy is a growing component of identity management programs, and incorporating privacy into these programs is becoming strategic for organizations who want to protect both their users and their companies.[53] Privacy goals can be achieved through identity management by verifying user identities with authentication solutions, and through awareness and education.[54] These tools are used throughout the data lifecycle.

Privacy program workflow automation & management
Privacy program workflow automation and management tools help privacy program teams manage compliance with data protection laws, regulations, and requirements, which are constantly evolving. Several privacy tech tools have been built in response to these compliance obligations and privacy program management pain points. These tools cover privacy reviews (privacy impact assessments, data protection impact assessments, transfer impact assessments, etc.), workflow automation tools, privacy program maturity and benchmarking tools, privacy and data protection research portals, etc. These tools are used throughout the data lifecycle.

Vendor management for privacy
Vendor management for privacy tools help assess third-party vendors' privacy and security policies, access controls, and information storage practices. They include tools that automate vendor privacy questionnaires, score or benchmark vendor privacy controls, and audit vendor privacy controls. These tools are used throughout the data lifecycle.

Security for privacy
Security for privacy tools is a category intersecting both cybersecurity and privacy tech. It covers tools that specifically secure personal information. It includes incident response, data loss prevention (DLP), obfuscation, and access management tools. Data obfuscation includes techniques meant to "camouflage [personal data] in ways that render it useless if it were accidentally exposed or stolen."[55] Data obfuscation includes encryption, tokenization, and hashing technologies. Access management tools govern access to personal data (and other types of data). DLP tools ensure that personal data or other sensitive data is not lost or misused. These tools are used throughout the data life cycle.

Data governance for privacy
Data governance tools help with process or policy management, data glossaries, metadata management, or document classification.[56] There is a subset of data governance tools that solve for data protection problems. They include data discovery, classification, and cataloging tools, which are the building blocks for managing data processing and data

protection compliance. Data discovery tools help identify personal data. Discovery should be continuous, as definitions and practices evolve. Data classification tools help categorize personal data and match discovered personal data to the specific categories. Once classified, data cataloguing helps establish safeguards to properly protect personal data.

Data disposition tools help organizations dispose of personal data, taking into consideration data protection and other regulatory requirements,[57] retention policies, consumer requests, legal holds and legitimate business needs.[58] Automated records retention tools, in particular, can help organizations track retention policies and schedules, to determine whether to retain or dispose of personal data. These tools are used throughout the data lifecycle.

De-identification, pseudonymization, and anonymization PETs

De-identification and pseudonymization PETs help render individuals less identifiable, while anonymization PETs render them anonymous. From a data level, de-identification removes identifying data associated with a particular data subject from a data set.[59] Whereas, pseudonymization masks direct identifiers from personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.[60]
Meanwhile, anonymization goes further to render personal data anonymous in such a way that the data subject is not or no longer identifiable. De-identification, pseudonymization, and anonymization PETs include encryption, tokenization, hashing, differential privacy, etc.[61] These tools are used throughout the data lifecycle.

Marketing & advertising for privacy

Marketing & advertising rely heavily on personal data, raising privacy problems. These adjacent industries are experiencing an upheaval, resulting to privacy tech solutions popping up at the intersection of these industries to address marketing and advertising privacy problems.

B2B PRIVACY TECH: DEVELOPMENT LIFECYCLE TOOLS

Perhaps one of the more exciting developments we're seeing in privacy tech—at least in the B2B space—is the emergence of developer privacy tech tools. We break down the development lifecycle according to the following phases: training, requirements, design, build, production, and incident response. Development lifecycle privacy tech tools help solve for privacy problems before they materialize, or at least before data is collected, shifting left from the data lifecycle to the development lifecycle. This B2B development lifecycle privacy tech trend is in line with the adjacent shift left security trend.[62] These products equip developers, privacy engineers, and other technical privacy teams with the tools they need to design and engineer privacy into the development lifecycle, build privacy-respecting products, and avoid common privacy pitfalls in developing products, software, systems, and technologies, in general.

Developer privacy training & awareness

Developer privacy training & awareness platforms provide training and awareness tools for developers, engineers, and other technical teams on common privacy problems that may arise during the development process. These tools are used during the training phase of the development lifecycle.

Privacy requirements library
Privacy requirements libraries provide developers with a library of privacy rules and requirements to translate into code in developing products and systems that touch personal information. These tools are used during the requirements phase of the development lifecycle.

Technical privacy analysis
Technical privacy analysis tools help engineers identify potential privacy problems. The tools help create repeatable rules to address privacy gaps, which developers in turn can implement during the build stage. Technical privacy analysis tools help scale privacy engineers and other technical privacy domain experts by making guidance available across the platform to engineers. These tools are used during the design phase of the development lifecycle.

Developer PETs
Developer PETs are tools developers use to enhance privacy during the development lifecycle. For example, developers could use "dummy data," or data sets with randomly generated, made-up data points. Developers could also choose to use "synthetic datasets," which are data created artificially instead of being generated from the world. Or they could choose to deploy other PETs like differential privacy, SMPC, homomorphic encryption, etc. in the development of new systems and products. These tools are used during the design, build, QA, and production phases of the development lifecycle.

DevPrivOps
DevPrivOps tools are a suite of tools for developers to help build in privacy design and engineering into products. They cover tools from the requirements stage to the production stage of the development lifecycle.

Process and program management for privacy
Process and program management for privacy tools are tools for technical privacy program managers and privacy engineers. They cover the entire development lifecycle.

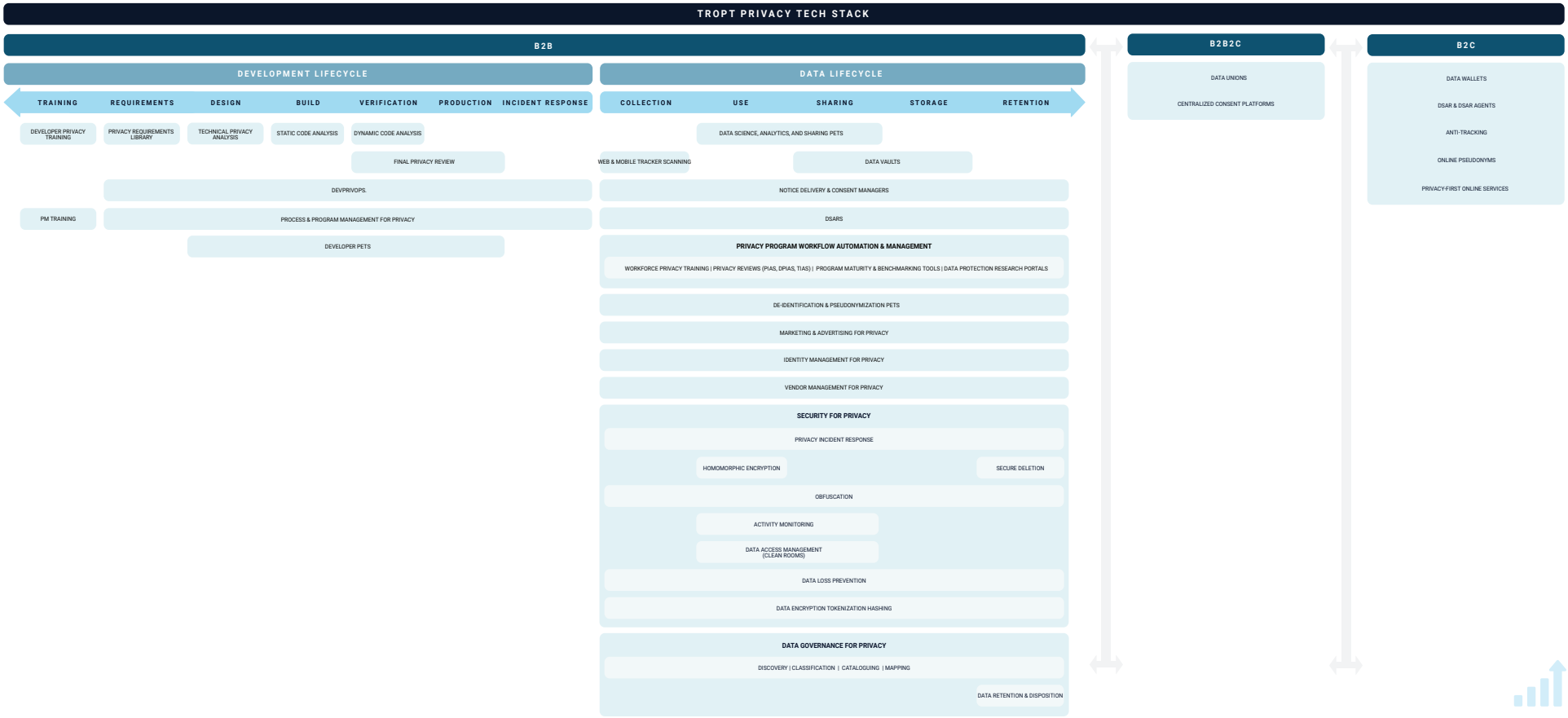
Static code analysis
Static code analysis privacy tech tools scan static (non-running) source code for privacy bugs or privacy problems in the code. These tools analyze code against a set (or multiple sets) of coding rules for privacy. They're typically used during the build stage of the development lifecycle.

Dynamic code analysis
Dynamic code analysis tools scan code while the software is running to improve the identification and correction of privacy bugs. They're typically used during the verification stage of the development lifecycle.

Final privacy review
Final technical privacy review tools facilitate the examination of all privacy requirements, privacy problems raised, privacy bugs identified in the code, and mitigations put in place during the early stages of the development lifecycle. Final technical privacy review tools are used just before or at the beginning of production.

Despite privacy's central focus on individuals, privacy tech tools for organizations (i.e. B2B) as outlined above have gained more momentum than their consumer privacy (B2C) counterparts, which we turn to in the next section. This is due to several factors, including global data protection laws regulating organizations' privacy practices, budget, competing business models in the consumer space, etc.

Figure 8. TROPT Privacy Tech Stack
Source: TROPT Defining the Privacy Tech Landscape 2021



B2C PRIVACY TECH

Despite trailing behind their B2B counterparts, B2C privacy tech products are slowly emerging and gaining increasing adoption. Common B2C privacy tech products include data wallets, data subject access rights (DSARs) and DSAR agents, anti-trackers, online pseudonyms, and privacy-first online services.

Data wallets

Data wallets allow users to securely store and encrypt all of their personal data in one unique electronic ecosystem, like a wallet, and then choose which third parties can access which data points through the wallet. Their goal is to give individuals complete control over who can access their personal data.[63]

DSARs & DSAR agents

In addition to the B2B DSAR tools previously covered, there are also available DSAR tools for individuals that empower them to exercise their rights to access, correct, delete, port, and exercise general control over their personal information. DSAR agents are services that execute DSARs on consumers' behalf. B2C DSAR tools currently have not gained as much traction as their B2B counterparts. This is likely due to a couple of factors: 1) the general sentiment that consumers should not be paying for privacy; and 2) perhaps relatedly, the historical investment focus on the B2B side of privacy tech.

Anti-trackers

Anti-tracking tools help consumers block tracking of their personal information, activities, and behavior in different contexts, including at the browser, app, and device levels. Anti-trackers include private browsers, browser plug-ins, operating system features blocking cross-app tracking, and VPNs. Anti-trackers address consumer problems relating to control, including the preference to remain anonymous in certain contexts.

Online pseudonyms

Online pseudonyms are tools that allow individuals to interact pseudonymously online. Avatars are a common example of these tools. Other examples include products that automatically generate random email addresses, phone numbers, or other personal information, in lieu of sharing real information.

Privacy-first online services

We're also seeing privacy-first online services emerge as alternatives to the surveillance-heavy status quo. In the private messaging space, as covered above, Signal gained widespread adoption among consumers. Among email service providers, ProtonMail provides an end-to-end encrypted email platform. Brave addresses private Internet browsing and video conferencing. DuckDuckGo provides a search engine that doesn't collect personal information, track online search, or deliver ads.

B2B2C PRIVACY TECH

B2B2C privacy tech tools bridge the B2B and B2C sides of the privacy tech landscape. These tools service both business and consumer-side users. Today, the most common B2B2C privacy tech platforms we're seeing are centralized consent platforms and data unions.

Centralized consent platforms

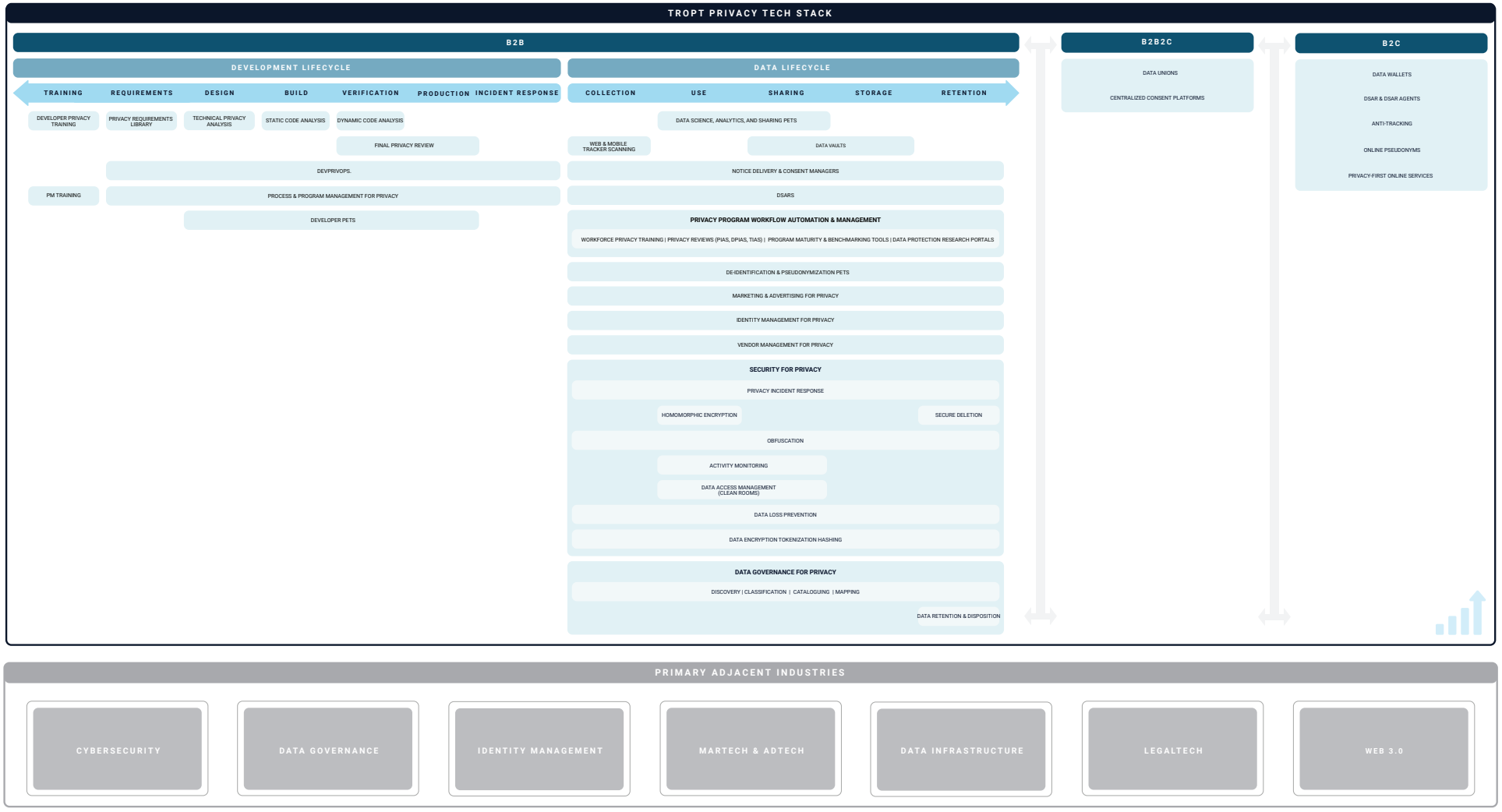
Centralized consent platforms aggregate consumer consent preferences. Organizations that wish to process personal information for various reasons can engage with centralized consent platforms to source data that has been collected legitimately, oftentimes with explicit consent and specific parameters for data processing purposes.

Data unions

Beyond centralized consent platforms, there are data union platforms that allow for the bundling of personal information with others. They distribute a share of the revenue when someone pays to access it. Some studies have shown that individual personal information on its own fetches a nominal price. When combined in a data union, aggregated data increases in value. Data unions typically allow individuals to choose which types of personal information they want to share and the amount of value they wish to receive in exchange for sharing their data, if any. Oftentimes, the data union dividend is in the form of cryptocurrencies. Data unions allow individuals to have more control over the monetization of their personal information.

Figure 9. TROPT Privacy Tech Stack + Adjacent Industries

Source: TROPT Defining the Privacy Tech Landscape 2021



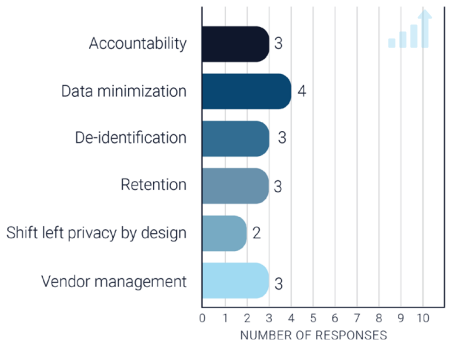
BRIDGING GAPS BETWEEN PRIVACY TECH KEY PLAYERS

In addition to defining and categorizing privacy tech in the previous sections, we also surveyed privacy tech key players to bridge the tech-capital-expertise gaps in privacy tech. We highlight some of the findings in this section and share the full survey responses in the Appendix towards the end of this whitepaper. As this is the first year that we're conducting this research, we anticipated receiving a small sample size of responses to our inaugural survey. We addressed this by conducting more in-depth interviews with select privacy tech leaders, some of whom we quote in the following sections.

WHAT PRIVACY TECH BUYERS AND USERS SAY

B2B privacy tech users and buyers—from engineers to lawyers—shared their insights on the privacy tech space. They shared the following privacy problems for which they're trying to find technology solutions: data minimization, retention, vendor management, de-identification, accountability tools, and "shift left privacy" tools for developers. We highlight some of these pain points in the following sections.

Figure 10. Privacy Tech Buyers and Users Survey: Privacy Problems They Need Solved Through Tech



Source: TROPT Defining the Privacy Tech Landscape 2021

Data Minimization. With today's data-driven business models, strategies, and products, cross-functional teams (typically privacy, security, IT, and data governance professionals) are oftentimes faced with the uphill battle of pushing their organizations to adopt data minimization, the privacy principle and legal requirement to only collect, use, and store personal information that is relevant and necessary to meet specific legitimate purposes. They are looking for tools that address data minimization in an automated fashion, at earlier stages in both the data and development lifecycles. Such tools not only help minimize privacy risks; they also force organizations to only process relevant data that truly holds value for them, making it easier for them to unleash such data's value, instead of incurring data liabilities and drowning in proverbial data lakes.

Data Retention and Disposition. It's unsurprising that respondents listed data retention as a privacy problem for which they need privacy tech solutions. End-of-life data retention and disposition is one of the more difficult problems privacy, data governance, and GRC professionals are facing. There are a few reasons for this. First, these practitioners are going up against the default resistance to getting rid of data, partly due to the ingrained Big Data mindset of collecting all the data, all the time. Second, data retention and disposition sit at the very end of the data lifecycle, away from the prying eyes of customers and the public. Privacy practitioners tend to prioritize more public-facing privacy problems like transparency (notice and consent)

and DSARs. Third, most data protection laws contain retention and deletion obligations, which add to their criticality. Lastly, the proliferation of shadow IT systems makes retention and deletion technically difficult to solve.

Vendor and Third-Party Management. Privacy tech users and buyers raised vendor and third-party management as another problem area that requires privacy tech solutions. This is unsurprising given the increased regulatory[64] and customer scrutiny over how organizations govern personal information sharing with their vendors and other third parties.

DevPrivOps (or Shift Left Privacy Tools for Developers). Perhaps one of the most exciting trends we're seeing in the privacy tech space is the desire to solve privacy problems earlier on in the data lifecycle. We see the "shift left privacy" trend extend even before the ingestion point or the beginning of the data lifecycle. We're seeing the trend move further left, before data is collected, shifting as early as the development lifecycle, when products are developed and critical decisions affecting privacy are made. Privacy tech users and buyers want visibility into how code and algorithms affect privacy. They want code governance tools for developers to use. In other words, they want to stop the privacy problems before they're created.

"Vendor and third-party management have been one of the most challenging things. I can't build a team of developers that is so big that we're able to build everything in house, to ensure that everything is built with privacy by design. We have to use other services and, unfortunately, there are not that many options yet in all those services to find something that is also building with privacy by design … Privacy and security reviews are particularly painful, not just painful for vendors, but also for the companies asking for such reviews. They're causing internal strife. They're causing tension between stakeholders because the privacy team, or information security team, or whoever's requiring the privacy and security reviews, enter into conflict with their own co-workers. They're slowing down their co-workers from getting the tools that they need."

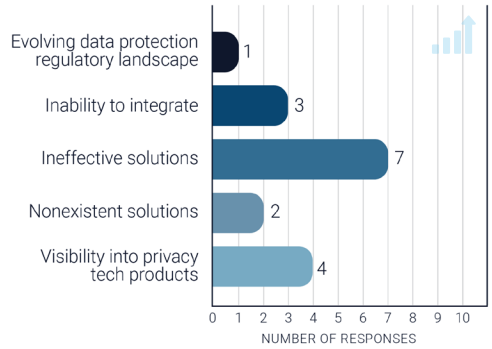
Caroline McCaffery, CEO & Founder, ClearOPS

"A lot of existing tech startups tend to optimize for privacy when it comes to data at rest. They will look at the warehouse and they'll say we'll do deletion, we'll do categorization, inventory, and discovery. The problem is at that point, think of a horizontal funnel going from left to right, the narrow end on the left-hand side, if you approach it on the right-hand side, the size of data has grown significantly. I'm asking privacy tech startups, 'Can you intercept data at the point of ingest, before any engineer gets their hands on it?' so you can tag the data early on, you can delete some data before it gets used, made copies of, or before—heaven forbid it—data gets shared with a third party. I'm looking at startups that are trying to catch data right at the point of ingestion … 'shift left' as people say." That's something I optimize for."

Nishant Bhajaria, Head of Privacy Engineering and Architecture, Uber

Privacy tech buyers and users reported the following challenges in navigating the privacy tech space in general: ineffective solutions, visibility into privacy tech products, inability to integrate with existing systems, nonexistent solutions, and evolving data protection landscape.

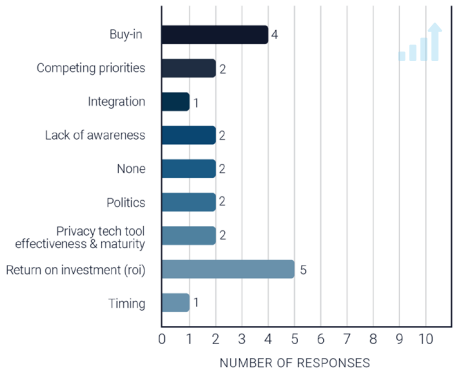
Figure 11. Privacy Tech Buyers and Users Survey: Challenges in Navigating the Privacy Tech Space



Source: TROPT Defining the Privacy Tech Landscape 2021

They also disclosed facing the following specific challenges in securing budget for privacy tech tools: return on investment (ROI), buy-in, competing priorities, politics, product maturity, integration, and timing. Their reported team and company budgets varied widely, as illustrated in Figures 13 and 14.

Figure 12. Privacy Tech Buyers and Users Survey: Challenges in Securing Privacy Tech Budget

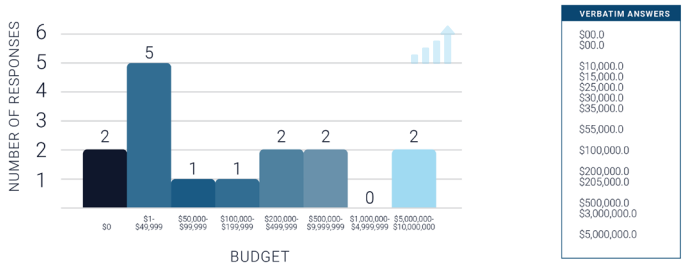


Source: TROPT Defining the Privacy Tech Landscape 2021

"If you buy a tool, who is going to wield the political clout within the company to make sure that there is onboarding? It's very critical before you onboard a third-party [privacy tech] tool, that you have a clear understanding of how onboarding is going to work. What is the tech stack looking like? Is there any platform compatibility? It's important to make sure that the engineers are in the room and the decision is being made. What typically happens is the engineers have to do a proof of concept after somebody else has made the decision to acquire the tool. This creates inefficiencies and disconnect. So, my recommendation would be, bring the engineers to the discussion sooner, because at the end of the day, if you don't, the engineers will leave. Or they'll do a bad job of onboarding it."

Nishant Bhajaria, Head of Privacy Engineering and Architecture, Uber

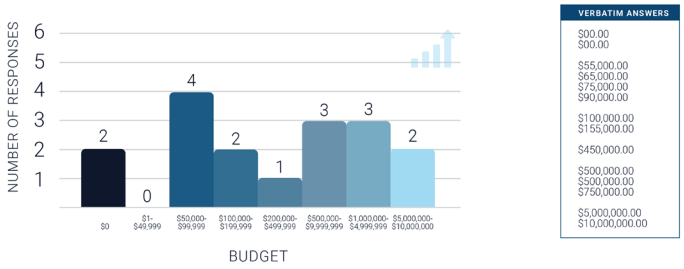
Figure 13. Privacy Tech Buyers and Users Survey: Privacy Tech Team Budget



Average team privacy tech tool budget: $655,357.14
Median team privacy tech tool budget: $45,000.00

Source: TROPT Defining the Privacy Tech Landscape 2021

Figure 14. Privacy Tech Buyers and Users Survey: Privacy Tech Company Budget



Average company total privacy tech tool budget: $1,267,142.86
Median company total privacy tech tool budget: $127,500.00

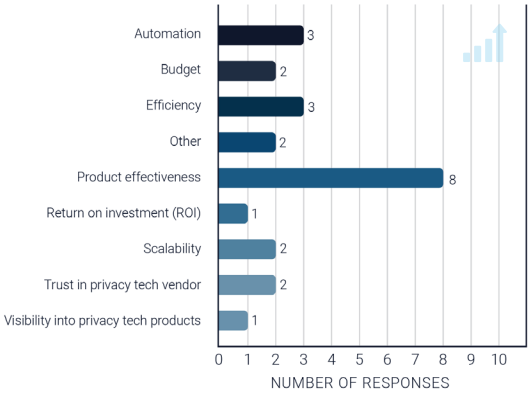
Source: TROPT Defining the Privacy Tech Landscape 2021

Buyers and users shared the following factors that affect their interest in buying privacy tech tools: product effectiveness, automation, efficiency, budget, scalability, vendor trust, and ROI.

"The privacy tech space is ripe for growth and opportunity - it's very important that new solutions focus on creating scalable processes that cleanly interoperate with an organization's existing tech stack."

Fatima Khan, Director, Corporate Counsel, Privacy & Product, Okta

Figure 15. Privacy Tech Buyers and Users Survey: Factors Affecting Interest in Buying Privacy Tech



Source: TROPT Defining the Privacy Tech Landscape 2021

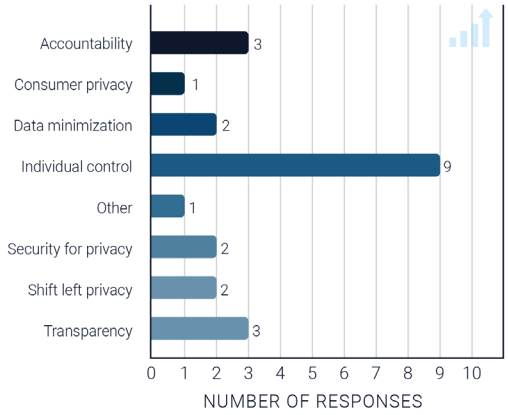
"I think there's a lot of pitches and there's a lot of promises that the vendors generally make and that's their business. I don't fault them for doing that. But I think when you're out laying some money and you're working on implementation of a new product especially in the privacy sphere where there's just not a lot of history there, you're trusting that what the marketing speak is around a particular feature or functionality of privacy tech is actually going to work in practice and it's going to make somebody's life better or easier. Someone who's working in the privacy program, a privacy engineer or data analyst, whoever you have on your operations team, it's going to make their life better, easier, get them the information in an easier way … I'm not expecting perfection, I'm not expecting the silver bullet. I'm not expecting that a particular product is going to make a company compliant. I actually don't appreciate when the privacy tech guarantees compliance because I think there's always going to be some choices that you're going to have to make in terms of how you implement a tool."

Alexandra Ross, Senior Director, Senior Data Protection, Use, & Ethics Counsel, Autodesk

WHAT PRIVACY TECH STARTUP FOUNDERS & OPERATORS SAY

Privacy tech startup founders & operators also shared their own takes on the privacy tech landscape. Respondents shared that they are building tech solutions to address the following privacy problems: individual control, demonstrating accountability, transparency, security for privacy, shifting privacy left, and data minimization, amongst other things.

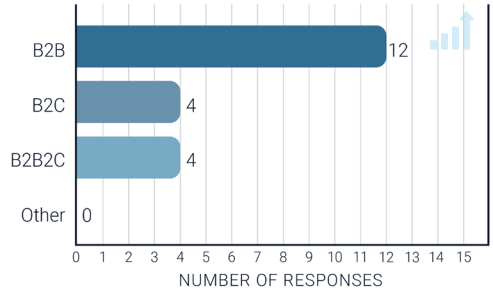
Figure 16. Privacy Tech Startup Survey: Privacy Problems They're Solving



Source: TROPT Defining the Privacy Tech Landscape 2021

Most surveyed privacy tech founders reported building for the B2B side of the privacy tech market. This aligns with the maturity of the TROPT B2B Privacy Tech Stack, compared to the B2C and B2B2C sides. Founders on the B2B side indicated that they were building primarily for Legal & Compliance and IT & Data Governance teams, with Marketing, Engineering, InfoSec, and other teams trailing behind. B2C privacy tech startups are also lagging behind their B2B counterparts.

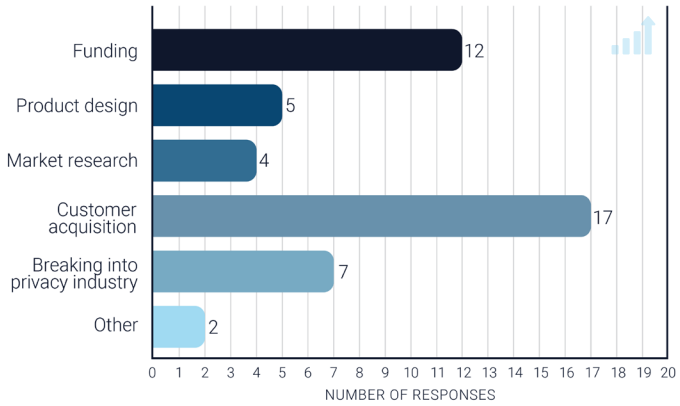
Figure 17. Privacy Tech Startup Survey: Business Model



Source: TROPT Defining the Privacy Tech Landscape 2021

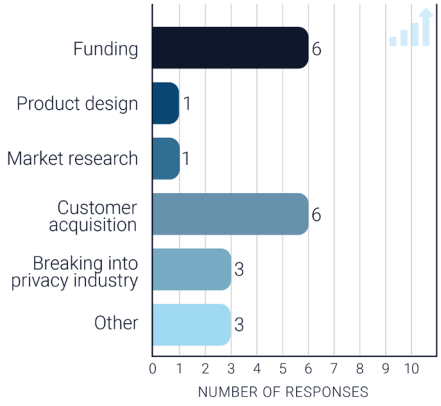
Responding privacy tech startup founders & operators named customer acquisition, funding, breaking into the privacy field, product design, and market research as their pain points, with funding and customer acquisition tied as their single biggest pain points.

Figure 18. Privacy Tech Startup Survey: Startup Pain Points



Source: TROPT Defining the Privacy Tech Landscape 2021

Figure 19: Privacy Tech Startup Survey: Single Biggest Startup Pain Points



Source: TROPT Defining the Privacy Tech Landscape 2021

"Two years ago, no one understood the pain-point we were solving. About 6 months ago, if you were trying to raise funding as a privacy tech company, you were immediately put in the bucket of a cybersecurity company. However, when we got to cybersecurity investors, they didn't think we qualified as a true cybersecurity [startup] investment, either, because we're not a product that plugs neatly into the security tech stack, so that was a big challenge. Right now, in talking to investors, I'm finding that there is a huge variation in the levels of research that they have done into the privacy tech landscape. Their levels of understanding vary and there's no cohesion yet. I have rarely met an investor who has dug into privacy tech as a standalone sector."

Caroline McCaffery, CEO & Founder, ClearOPS

WHAT PRIVACY DOMAIN EXPERTS SAY

We also surveyed and interviewed privacy domain experts who are involved in the privacy tech space. They cited the following reasons for their interest in the emerging privacy tech landscape: advisory roles, consulting roles, in-house privacy roles, purchase opportunities, and Angel investment opportunities. Most offer direct privacy tech experience, while others cite their experience in building privacy programs, working in relevant industries (B2B, B2C, adtech, etc.) as additional expertise they offer.
Privacy domain experts named development of privacy thought leadership and privacy product design as the top challenges with which they can help privacy tech startups.

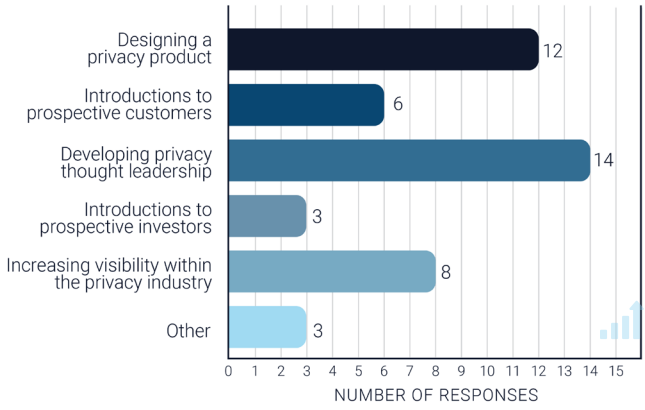
"I've learned that you really want to make sure that you've got a great working relationship with the founders. So, I now ask myself, "Are these founders people I want to work with long term? Are they coachable? Do they want my advice or does the team simply want to use my name and reputation for fundraising and marketing purposes?"

Debra Farber, CEO, Principled LLC

"When assessing whether to work with a privacy tech startup, I think a lot of the personality of some of the founders and the people that you're going to be working with at that startup ... So much of it comes down to the actual execution, the founders, and whether I click with them. Do I get a sense that they're really going to pursue some of their goals? That's what sort of attracted me and led me to partner with some of the companies that I have advised over the years ... It's really that sort of human connection with the people involved that are working on implementing that technology."

Alexandra Ross, Senior Director, Senior Data Protection, Use, & Ethics Counsel, Autodesk

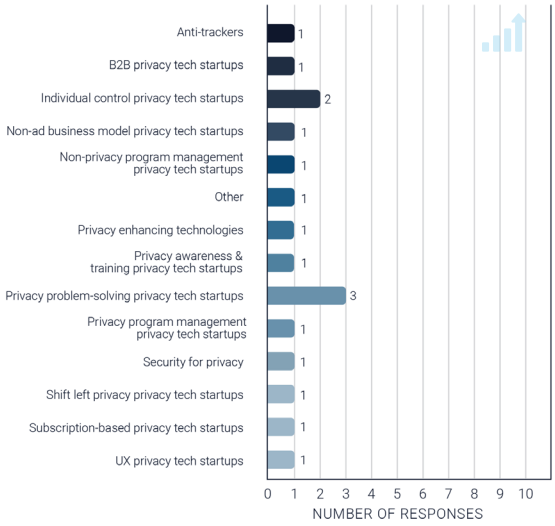
Figure 20. Privacy Domain Expert Survey: Challenges Experts Help Privacy Tech Startups With



Source: TROPT Defining the Privacy Tech Landscape 2021

Most experts viewed privacy tech startups that focus on solving for privacy problems in general and, specifically, individual control problems, as the most promising ones. This is noteworthy given our definition of privacy tech as *technological solutions to privacy problems*. Other experts picked startups working on anti-trackers, PETs, security for privacy, and, in line with the trends we're seeing, "shift left privacy" as most promising.

Figure 21. Privacy Domain Expert Survey: Privacy Tech Startups Experts Deem Promising



Source: TROPT Defining the Privacy Tech Landscape 2021

"I will not promote privacy tech vaporware or unsubstantiated privacy claims, so the first step is to conduct a technical analysis so we're all on the same page about what the technology does and doesn't do. That gives us a single source of truth in terms of what is real from a technical perspective, which allows our clients to maintain credibility in their communications."

Melanie Ensign, CEO, Discernible Inc.

When asked about their biggest challenges in working in the privacy tech space, they named ineffective solutions, low privacy tech understanding, mistrust in privacy tech vendors, rapid pace of innovation, immaturity of solutions, and unpaid advisory roles as some of their prominent pain points.

WHAT INVESTORS DIDN'T OUTRIGHT SAY

We surveyed investors, but we didn't receive enough responses to report any significant insights from them. Amongst the key players in privacy tech—founders, investors, expert-advisors, and buyers—investors are seemingly the least interested in digging into and understanding privacy. Most of the investors we've engaged with through TROPT view privacy tech as an insignificant niche falling under cybersecurity, which, as we've discussed earlier in this whitepaper, is wholly inaccurate. We predict that as more and more privacy tech unicorns emerge and as the current ones prepare for IPO, investors will necessarily follow. We salute the early visionaries who were first to funding privacy tech, at its nascency. We encourage emerging privacy tech investors to jump in and help fuel privacy tech by funding the next round of privacy tech unicorns.

FUELING THE FUTURE OF PRIVACY TECH

As we move from defining and categorizing the privacy tech landscape, we take the next steps in bridging the gaps between privacy tech key players and fueling privacy innovation. Each privacy tech key player has a part to play in this endeavor. We lay out our recommendations for how each key player can help fuel the future of privacy innovation.

WHAT PRIVACY TECH FOUNDERS CAN DO

We need more privacy tech founders to build solutions to today's privacy problems. We outline some specific recommendations for privacy tech founders as follows:

More privacy tech founders should build privacy tech products that address privacy problems earlier in the data and development lifecycles. As the data lifecycle side of the privacy tech stack gets crowded and as existing solutions mature, plenty of remaining privacy problems—or privacy tech opportunities—remain in the development lifecycle side. In line with the "shift left privacy" trend, development lifecycle privacy tech needs to catch up with data lifecycle privacy tech.

More privacy tech founders should solve for consumer privacy problems. Consumer (B2C) privacy tech sorely needs to catch up with business (B2B) privacy tech. Privacy is inherently about people, after all. Moreover, there is a clear marketplace demand for privacy, not just in the B2B space, but also in the B2C space.[65]

Privacy tech founders should start with understanding privacy problems before building technical solutions for them. Founders should begin with understanding the privacy problems that privacy tech buyers and users have, and then build privacy tech solutions that address those problems. Further, they should understand that privacy problems go beyond compliance, security, or other limited takes on privacy. By understanding privacy, the breadth of privacy problems that exist, and the specific privacy problems that privacy tech users-buyers have, founders can build better privacy tech products.

Privacy tech founders should walk their privacy talk in building their startups. It's critical that privacy tech founders demonstrate their commitment to privacy, not just in their marketing speak, but also in terms of outcomes and metrics. Founders need to be thoughtful about how they build their products, choose their business model, and conduct their business operations. As previously covered, trust is central to privacy. Privacy tech founders who fail to walk their privacy talk will break customer and public trust in their startup, products, and brand.

"It's very challenging to see the difference between a company that is taking advantage of privacy, whether it's a regulation or a branding type of exercise, to gain customers versus a startup that actually believes in pushing privacy forward as a human right. I do think of those as two very different types of companies... I would actually hope that they would be doing both, but the ones that are sort of exploiting are the ones I think are challenging specifically for investors because they may be doing very well from a revenue perspective or show promise on that side, and yet they're not actually pushing the rights that someone like myself so strongly believes in... I think it's very difficult, on the investor side, for them to assess and do due diligence on a company's own privacy."

Caroline McCaffery, CEO & Founder, ClearOPS

Privacy tech founders should learn to effectively communicate privacy tech's value proposition. Doing so means being able to help customers and prospects make the case for privacy tech and secure the budget and buy-in they need.

"I see two common challenges among privacy tech startups when learning to communicate their product's value proposition. First, they don't always understand what's valuable from the perspective of their user or customer. Often, their messaging is optimized for investors with a heavy emphasis on compliance requirements, but that's usually not what differentiates your product from a sales perspective. Things like interoperability, auditability, quick and painless implementation, and support for cross-functional stakeholders don't typically make it into the pitch deck for investors, but they're critical factors for customers considering a vendor solution. The second challenge I see often is not being able to effectively engage with the technical privacy community directly. This community right now is so small, in terms of where the influence comes from and whose opinion matters in driving adoption of new technologies, that if you are not actively involved in the community, you miss the opportunity to build relationships with folks who can not only lend your product technical credibility, but also advise your product teams on what the market is eager to buy."

Melanie Ensign, CEO, Discernible, Inc.

WHAT INVESTORS CAN DO

As much as we need more privacy tech founders to build solutions to some of today's privacy problems, we equally need investors to recognize the rise of privacy tech and invest in the emerging privacy tech industry.

Investors should understand that there is a clear marketplace demand for privacy, both in the B2B and B2C sides.[66] Failing to do so means missing out on investing in upcoming privacy tech unicorns. It also means failing to step up and address the mounting privacy technical debt created by the tech industry, particularly by technologies that were built without much regard to privacy. This mounting privacy technical debt partly fuels the marketplace need for privacy tech.

Investors should recognize that privacy tech opens up environmental, social, and governance (ESG), social responsibility investments (SRI), and impact investing opportunities. This is game-changing for venture capital. Today's limited partners (LPs) demand that their money make a positive impact on society and the world at large.

By now, investors should understand that privacy tech is its own emerging industry. Privacy tech is not a cybersecurity or other industry subcategory. We hope that this whitepaper helps illustrate the big picture of this nascent but emerging space.

Put simply: investors should invest in privacy tech. There's a clear marketplace demand for privacy tech. Investing in startups that solve privacy problems is the right thing to do. Other forward-thinking investors have already poured almost six billion US dollars (specifically, $5.9B) in cumulative funding towards emerging privacy companies, with four billion ($4B) in the past three years alone.[68]

"Today's investors no longer care solely about returns. More and more limited partner (LP) investors — investors who invest in venture funds — want their money to make a positive impact on society and the world at large, including when it comes to privacy.
It turns out that SRI accounted for more than $1 out of every $4 under professional management in the United States. Investors also used ESG criteria to evaluate companies for investment, and these accounted for $16.6 trillion in investment assets in 2020. It seems LPs care enough about their investment dollars to the tune of a $715 billion impact investing market, and some LPs are even looking to link a fund's carried interest to quantifiable impact metrics."[67]

Lourdes M. Turrecha, TROPT Founder and privacy tech Angel investor

WHAT PRIVACY DOMAIN EXPERTS CAN DO

Privacy domain experts should help build privacy tech solutions. We need more privacy domain experts to jump in as privacy tech founders, advisors, operators, and even investors. Why? Because they are intimately familiar with privacy and understand the biggest privacy problems. With privacy domain experts helping build privacy tech, we avoid with ineffective privacy tech solutions or, worse, privacy tech vaporware.

Privacy domain experts should help better articulate the biggest privacy pain points they're seeing that need privacy tech solutions. Their intimate understanding of privacy and privacy problems will immensely help guide the privacy industry.

Privacy domain experts should weigh in on both the promising and the ineffective privacy tech products they're seeing. To help highlight the best privacy tech products in each category and weed out ineffective products, privacy domain experts should weigh in on the privacy tech products that are effectively solving privacy problems. Conversely, they should voice when they see products that market themselves as privacy tech but don't actually do a good job at solving privacy problems. This saves privacy tech user-buyers from wasting their valuable privacy tech budget, internal political capital, and other resources required to implement such products.

WHAT B2B PRIVACY TECH BUYERS AND USERS CAN DO

Privacy tech buyers and users should better articulate their biggest privacy pain points. This will not only help guide privacy tech founders in building tools that solve privacy problems, but also directly help buyer-users get the tools they need to solve their privacy problems.

Privacy tech buyers and users should provide public feedback on what works and doesn't work in the privacy tech products they're testing, using, and buying. This will help ensure that privacy tech startups have the information they need to improve their products. Even if they don't act on this information, this gives competitors the insight required to build better, competing products. In the end, this direct feedback helps fuel the privacy tech landscape.

Privacy tech buyers should learn how to better articulate the value of solving some of their privacy problems through privacy tech tools. This will help get cross-functional teams on board with privacy tech goals and help secure the privacy tech budget they need.

Privacy tech buyers and users should work cross-functionally in selecting and implementing privacy tech products. This will help ensure that their investment in their privacy tech purchase is not wasted and avoid internal strife.

"Even within companies, you see privacy engineers being disconnected from other engineers. You see legal and privacy engineering being disconnected and then public policy is further separate. And the comms team is sitting again, further out. You have all of these different folks trying to do the same thing, the right thing, which is find that balance between customers, between trust and compliance, but they don't talk to each other. So sometimes when it comes time to make the decision, "Do I or do I not onboard this tool?" Do I or do I not collect this data?" Sometimes those decisions are left to an engineer who may not have the right context."

Nishant Bhajaria, Head of Privacy Engineering and Architecture, Uber

TROPT'S PART

At TROPT, we will endeavor to continue our mission of fueling privacy tech and innovation. We specifically make the following commitments.

We commit to continuing to define and categorize the privacy tech landscape as it matures. Next year, we will begin categorizing startups into the TROPT Privacy Tech Stack.

We commit to continuing to bring together the privacy tech key players—founders, investors, experts, and user-buyers—to bridge the tech-capital-expertise gaps in privacy innovation. As covered in the previous section, startups disclosed funding, customer acquisition, and breaking into the privacy space as some of their biggest challenges. To address these challenges, we will continue connecting privacy tech startups with privacy domain experts and investors through our startup-advisor matching program and our startup-investor matching program.

We commit to continuing to spread awareness on privacy tech and innovation. We already do this through our events and programs. Current TROPT events include our conferences, TROPT Data Privacy Day (in January) and TROPT Virtual Summit (in June). Current programs include TROPT Innovators, our membership program for privacy tech key players who want year-round involvement with the TROPT privacy tech community in between events. Beyond our existing initiatives, we have several projects in the works, and we are open to feedback from the privacy tech community on how to best help privacy tech key players fuel privacy innovation.

We commit to helping increase privacy tech investments. We will do so by increasing investor awareness in and understanding of this nascent privacy tech industry. We will also continue to make available the TROPT privacy tech deal flow tool[69] for investors who want to invest in privacy tech startups and support the TROPT privacy tech community.

"The TROPT Defining the Privacy Tech Landscape Whitepaper is a necessary foundational step towards understanding, defining, and categorizing the nascent privacy tech industry. Now that we've set a baseline understanding of what constitutes privacy tech, we are better equipped to identify privacy tech products and act on the resulting marketplace opportunities. And because we believe in privacy's value, we see the numerours opportunities for privacy tech key players: privacy tech product ideas for founders, partnerships for privacy tech startups, investments for investors, privacy tech solutions for buyer-users, and advisory roles for domain experts, just to name a few. TROPT was founded to create a place for the industry key players to come together, realize privacy tech's value, and move the needle on privacy. With law typically lagging behind technology, we don't have to keep waiting for policymakers and regulators to give us the privacy solutions we've been asking for. As privacy innovators, we can build technological solutions to some of our privacy problems, and help fuel the privacy tech industry."

Lourdes M. Turrecha, TROPT Founder and privacy tech Angel investor

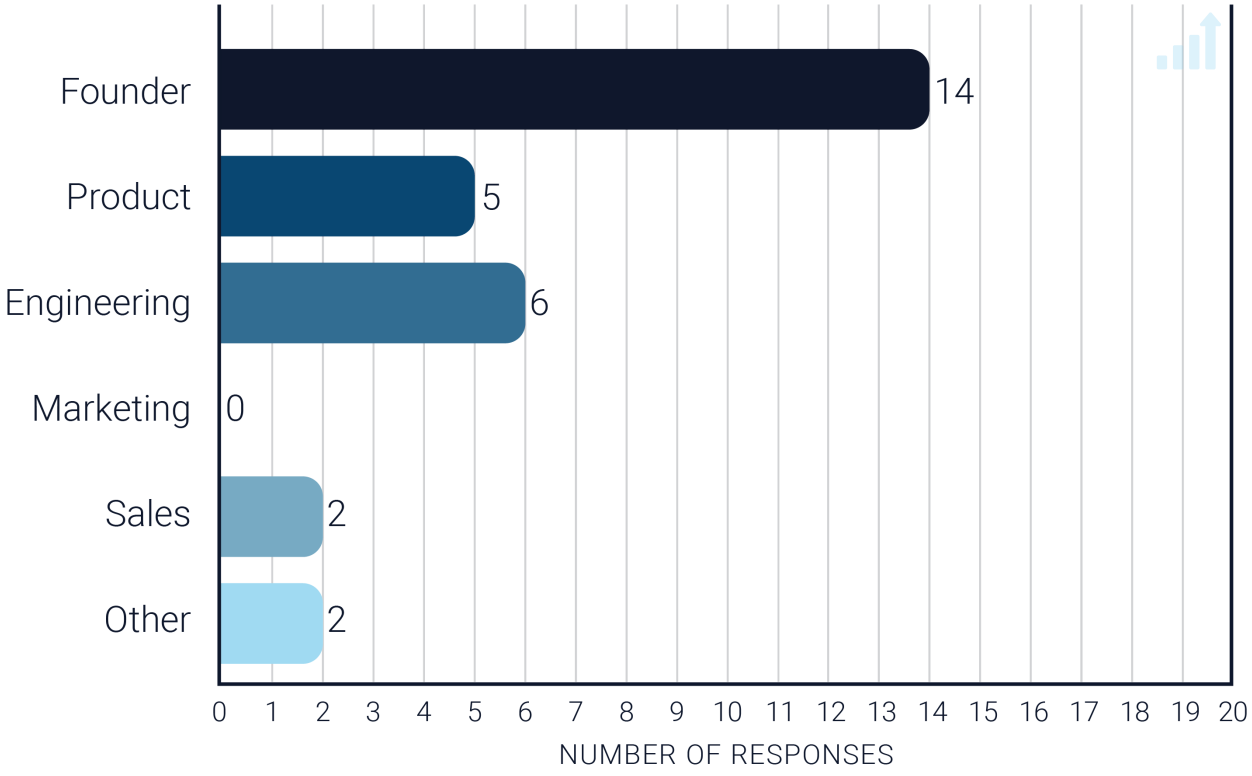
CONCLUSION

Our primary aim for this whitepaper is to define and categorize privacy tech. In the process of doing so, we ended up creating the TROPT Privacy Tech Stack to visually articulate the breadth of privacy tech, beyond defining its scope. We also sought to demonstrate privacy tech's value by seeking qualitative feedback from the different privacy tech key players. Future versions of this whitepaper will explore how the different key players' pain points, challenges, and focus change over time. TROPT will continue to work with TROPT Innovators members and the greater TROPT community of privacy tech key players to define, categorize, and fuel the privacy tech landscape. For additional information about TROPT's privacy tech industry research, please contact community@riseofprivacytech.com.

APPENDIX: SURVEY RESULTS

What is your role at your privacy tech startup?

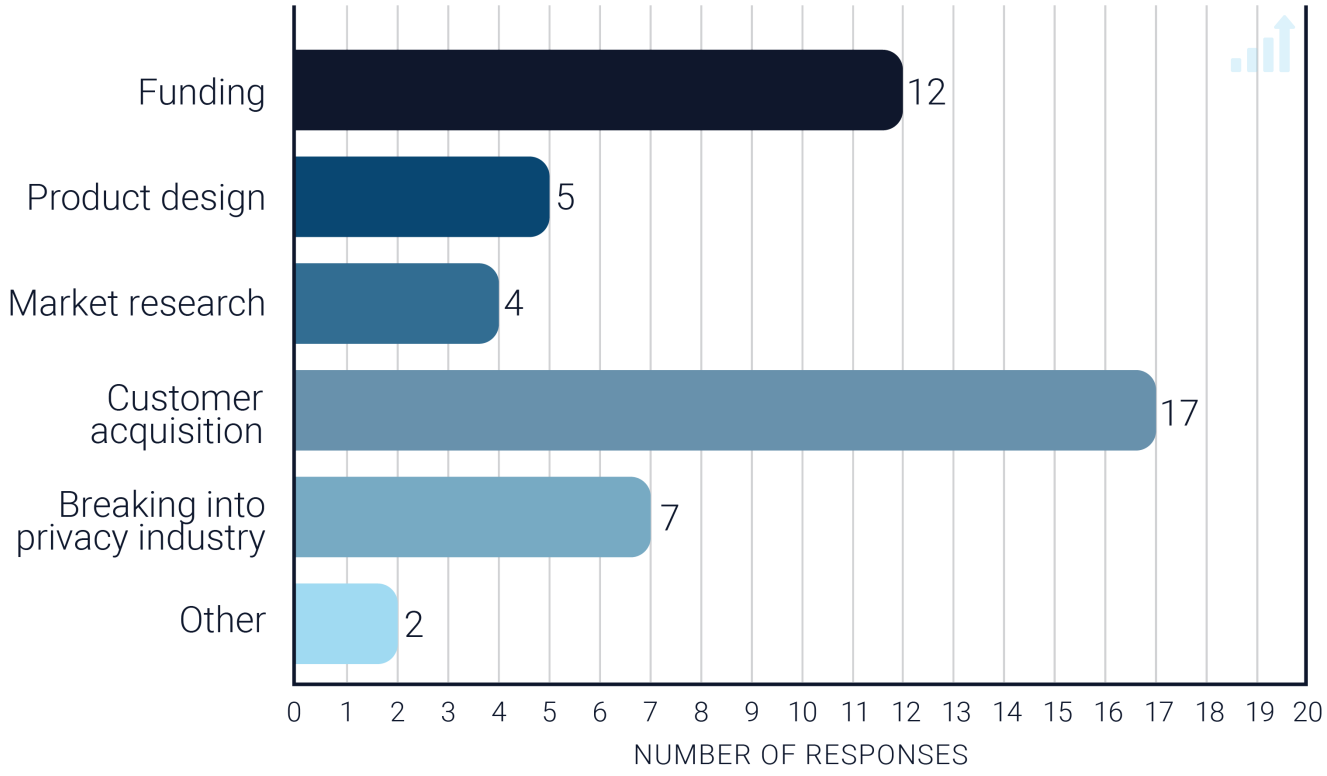
Privacy Tech Startup Survey
Answered: 20



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Which of the following are pain points for you? (You can pick more than one)

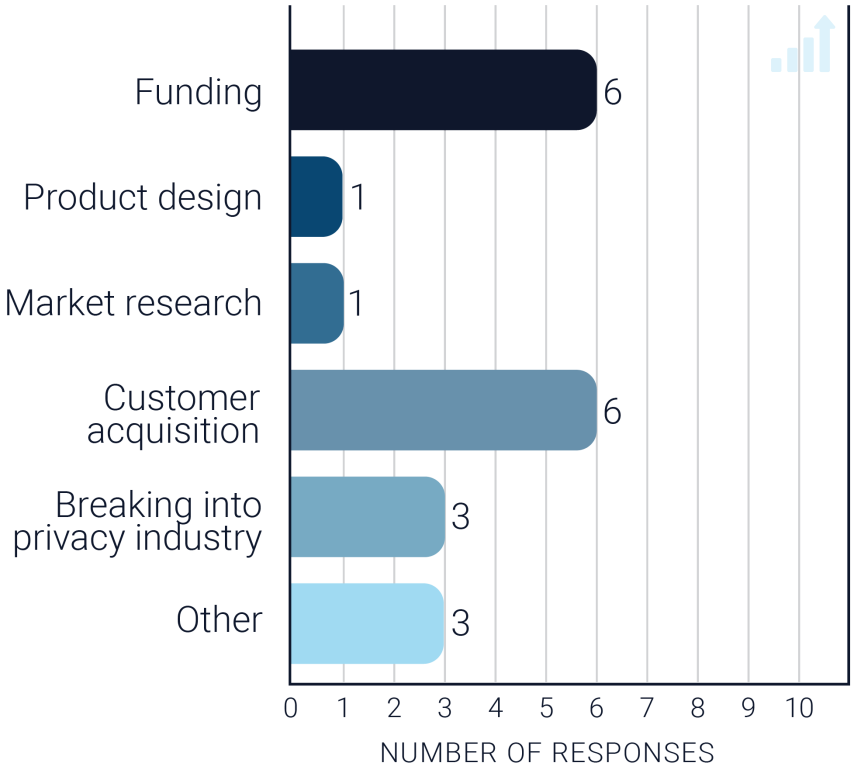
Privacy Tech Startup Survey
Answered: 20



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What is your single biggest privacy tech pain point? (Pick one)

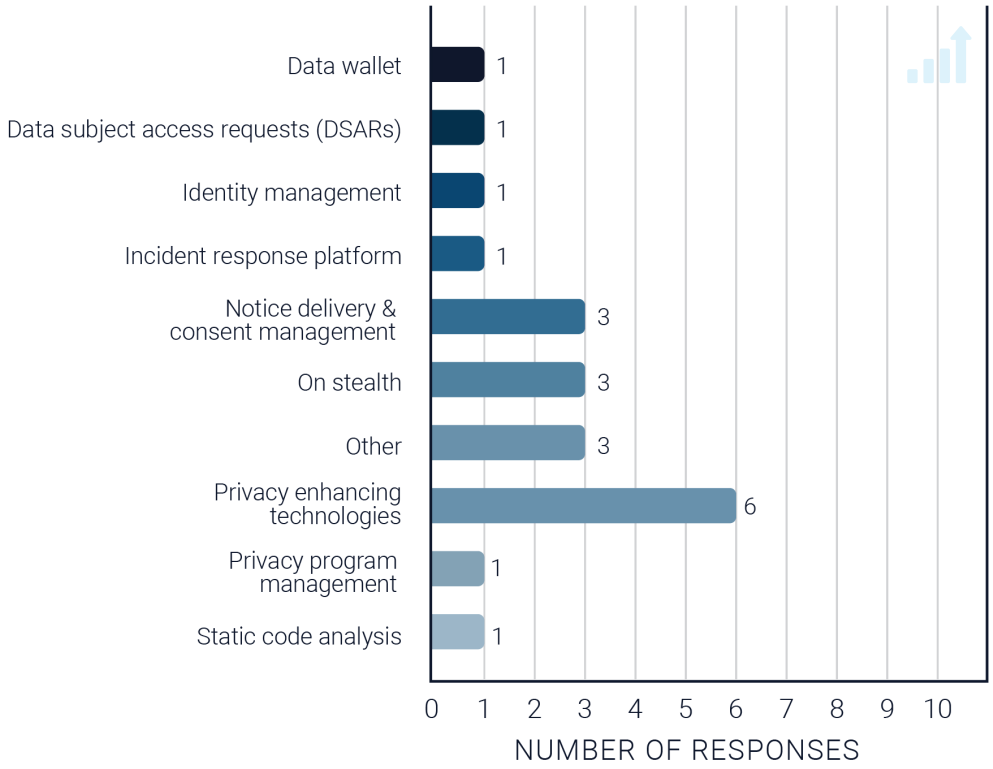
Privacy Tech Startup Survey
Answered: 20



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What privacy tech product are you currently working on?

Privacy Tech Startup Survey
Answered: 20

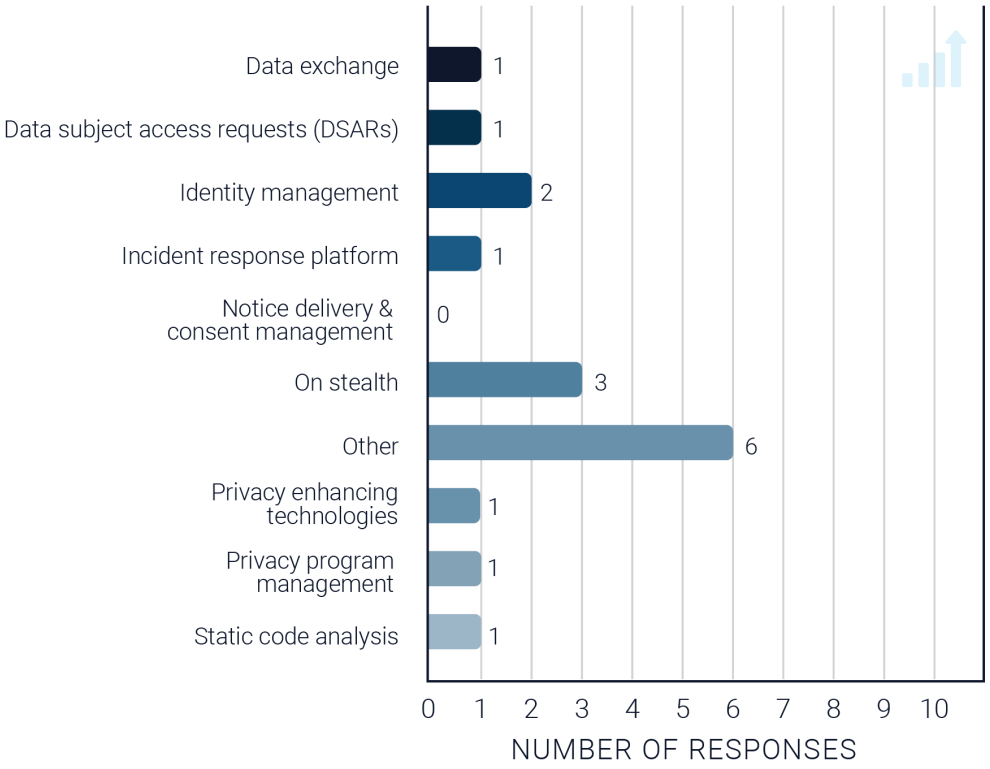


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Privacy Policy Evaluation Item	Notice Delivery and Consent Management
Legal compliance tech	Privacy Program Management
Zero-Party Data collection, unification, and activation to power Privacy-First Personalization.	PETs
Private data layer for decentralized applications	PETs
Confidential	On stealth
A Platform for Private Cloud Apps	Other
Consumer subscription service to help people take back control of their personal data from companies that shouldn't have it	DSARs
On stealth	On stealth
Data wallet	Data wallet
Privacy Incident Response Platform	Incident Response Platform
[redacted]	Other
The one	Other
Synthetic data	PETs
Computation over encrypted data - we have two products: [redacted] and [redacted]	PETs
Homomorphic encryption	PETs
Static Code Analysis for Privacy	Static Code Analysis
On-device contextual targeting for advertisers that does not rely on identifiers	PETs
Decentralized Identity	Identity management
T&Cs for SMBs, and Consent Management for SMBs	Notice Delivery and Consent Management
Consent management, privacy policy automation	Notice Delivery and Consent Management

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What privacy tech product are you planning to build in the future, if any?

Privacy Tech Startup Survey
Answered: 20

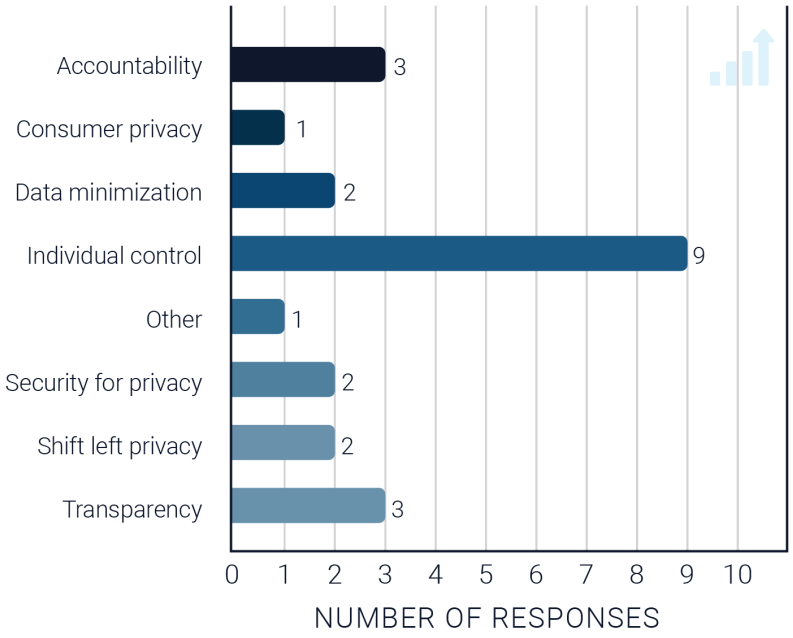


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Automatic Privacy Policy Evaluation & Consent Management	Notice Delivery and Consent Management
Full privacy management software	Privacy Program Management
Product is in market now, & we are actively scaling go-to-market.	Other
Self sovereign identity	Identity Management
Confidential	On stealth
A Platform for Private Cloud Apps	Other
Consumer subscription service to help people take back control of their personal data from companies that shouldn't have it	DSARs
On stealth	On stealth
Decentralized data marketplace	Data Exchange
Continually improving our Privacy Incident Response Platformt	Incident Response Platform
N/A	Other
A social net	Other
N/A	Other
We will develop out the suite around our two launched products.	Static Code Analysis
N/A	Other
Extending the use cases around static code analysis for privacy.	Static Code Analysis
Can't disclose at the moment	On stealth
Decentralized Identity	Identity management
T&Cs for SMBs, and Consent Management for SMBs	Notice Delivery and Consent Management
Consent management, privacy policy automation	Notice Delivery and Consent Management

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What privacy problem are you currently solving for?

Privacy Tech Startup Survey
Answered: 20

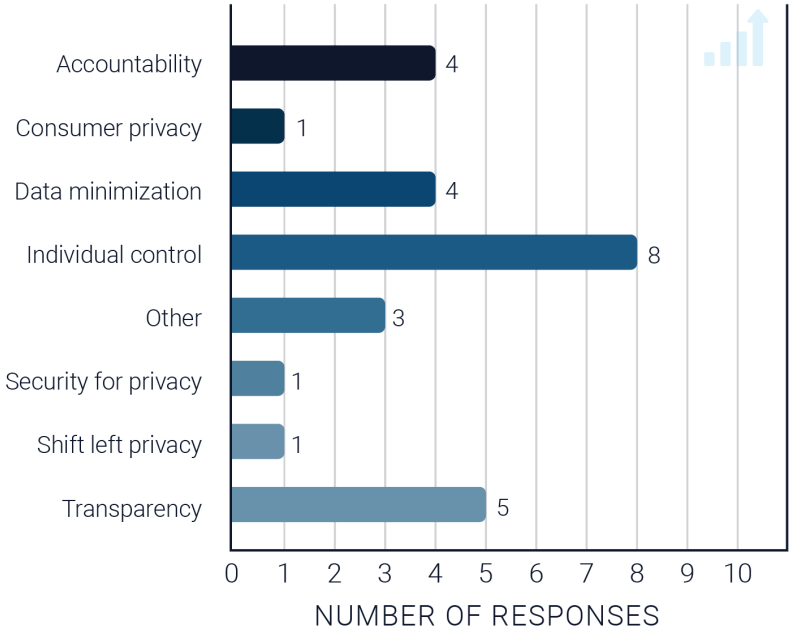


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Obscure Privacy Policy	Transparency
How to plan a full management scheme	Accountability
Enabling brands to deliver customer experiences that are always welcome, relevant and compliant. Empowering consumers with transparency,choice and control over the data they share with a given brand in order to improve their experience with that brand.	Transparency, Individual Control, Accountability
Consumer control of data (automate the 8 rights of individuals) & GDPR compliance automation for organizations	Individual Control
Personal Privacy	Individual Control
Consumers need options to own & control their data, not just software for-rent behind an EULA	Individual Control
Consumer lack of control over their personal data	Individual Control
Consumer privacy	Consumer Privacy, Individual Control
Individual Personal data monetization	Individual Control
Incident Response	Security for Privacy
Ugandans who can't have access to cheap quick loans	Other
Dev	Shift Left Privacy
The need for safe and useful data for testing and development	Shift Left Privacy
Browser based encryption, privacy and security issues around cookie deprecation	Security for Privacy
Analytics privacy	Data minimization
Privacy by Design. We help companies ship code fast without breaking user privacy. We do this by scanningthe source code continuously and alerting privacy teams when a code change has privacy issues. We detect personal data, third party and hidden data flows.	Shift Left Privacy
Eliminating the reliance of digital identifiers to deliver personalized ads (and content)	Data minimization
Allowing patients to control their identity attributes and by extension provide granular consent of their health data	Individual Control
T&Cs for SMBs, and Consent Management for SMBs	Accountability
Automating consent	Transparency, Individual Control

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What privacy problem are you interested in solving with these future products?

Privacy Tech Startup Survey
Answered: 20

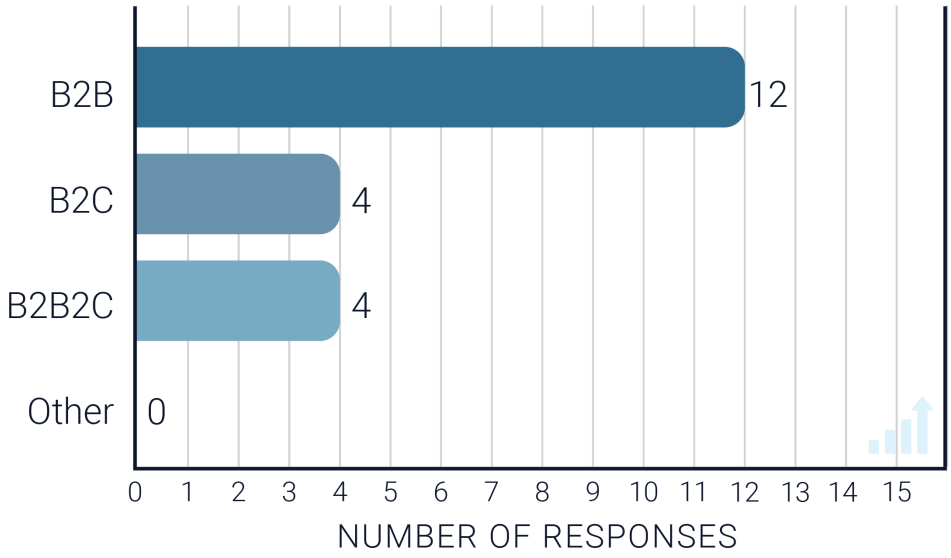


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Explicit User Consent	Transparency
Easy step-by-step guidance in legal compliance	Accountability
Enabling brands to deliver customer experiences that are always welcome, relevant and compliant. Empowering consumers with transparency, choice and control over the data they share with a given brand in order to improve their experience with that brand.	Transparency, Individual Control, Accountability
Minimizing data exposure; zero-knowledge identity verification	Data Minimization
User Experience	Individual Control
Most privacy problems are amenable to giving users private ownership & control of their data, and making it easy for non-experts to run decentralized software.	Individual Control
Consumer lack of control over their personal data	Individual Control
Consumer privacy	Consumer Privacy
Lack of equity for consumers	Individual Control
Incident Response	Security for Privacy
Marketing	Transparency, Individual Control, Data Minimization
Social net	Other
N/A	Other
Better data privacy in the advertising industry.	Other
Big data privacy	Data minimization
Automatically update RoPA and PIA/DPIAs with code scans.	Shift Left Privacy, Accountability
Privacy first mobile advertising	Transparency, Individual Control, Data Minimization
Lack of privacy and consent	Transparency, Individual Control
T&Cs for SMBs, and Consent Management for SMBs	Accountability

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What is your business model?

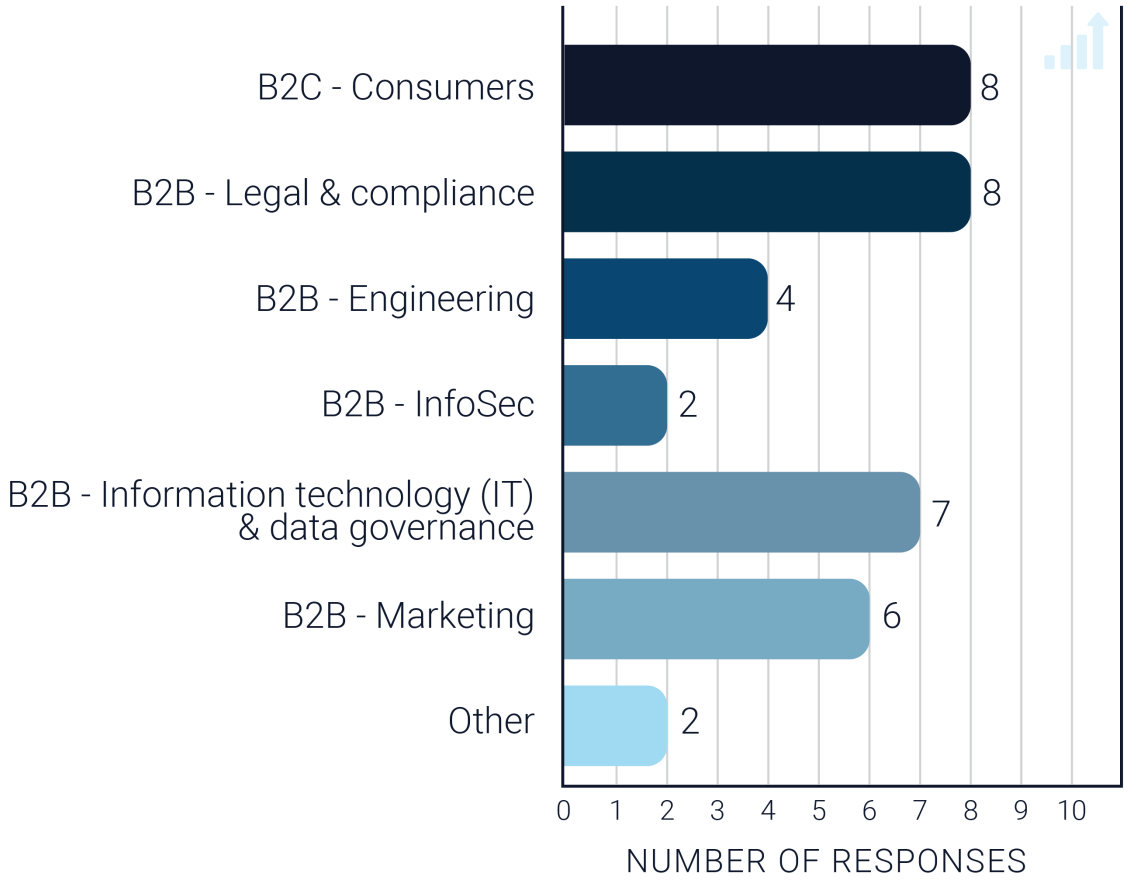
Privacy Tech Startup Survey
Answered: 20



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Who is your privacy tech startup building for?

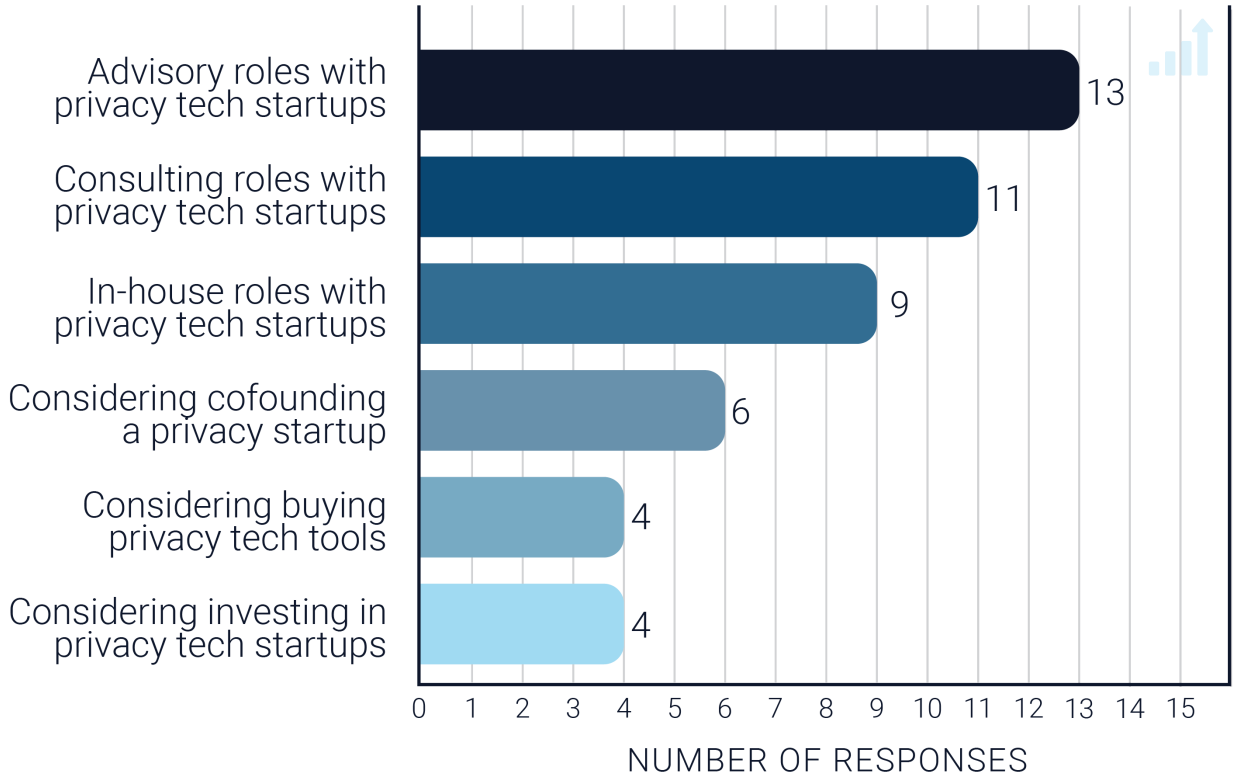
Privacy Tech Startup Survey
Answered: 20



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What interests you about the emerging privacy tech landscape?

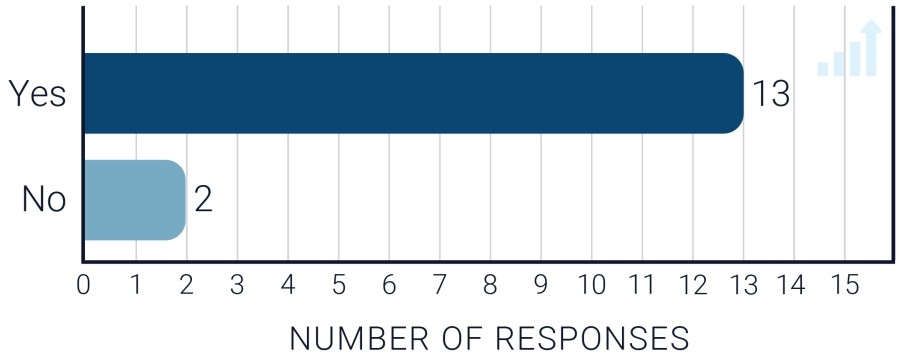
Domain Experts Survey
Answered: 15



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Are you currently working in the privacy tech landscape?

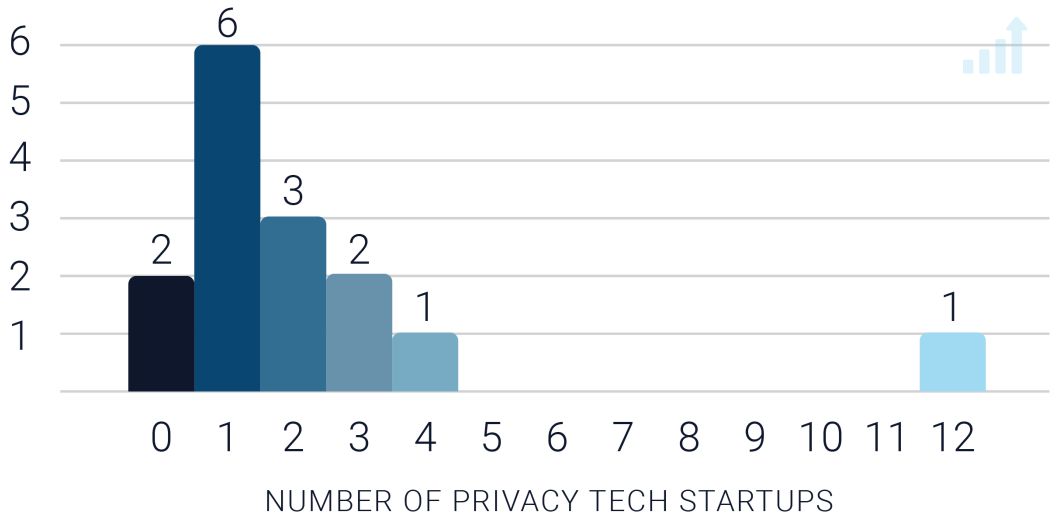
Domain Experts Survey
Answered: 15



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

How many privacy tech startups are you working with?

Domain Experts Survey
Answered: 15

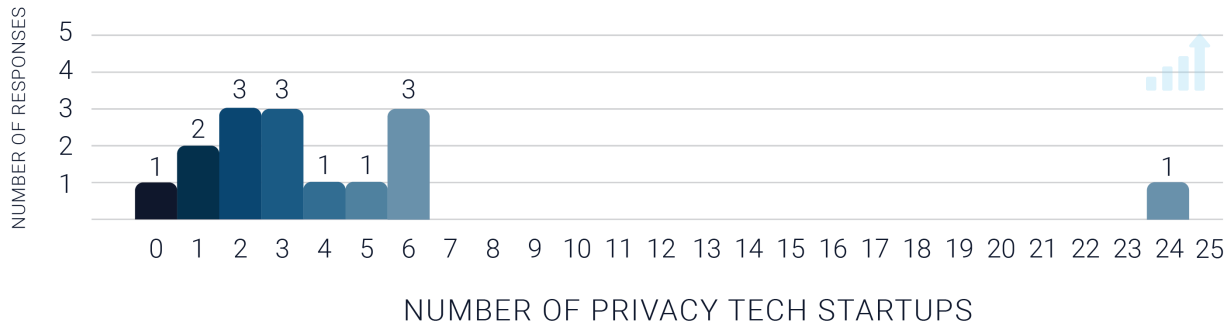


Average number of privacy tech startups: 2.27
Median number of privacy tech startups: 1.00

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

How many privacy tech startups do you anticipate working with in the next 12 months?

Domain Experts Survey
Answered: 15

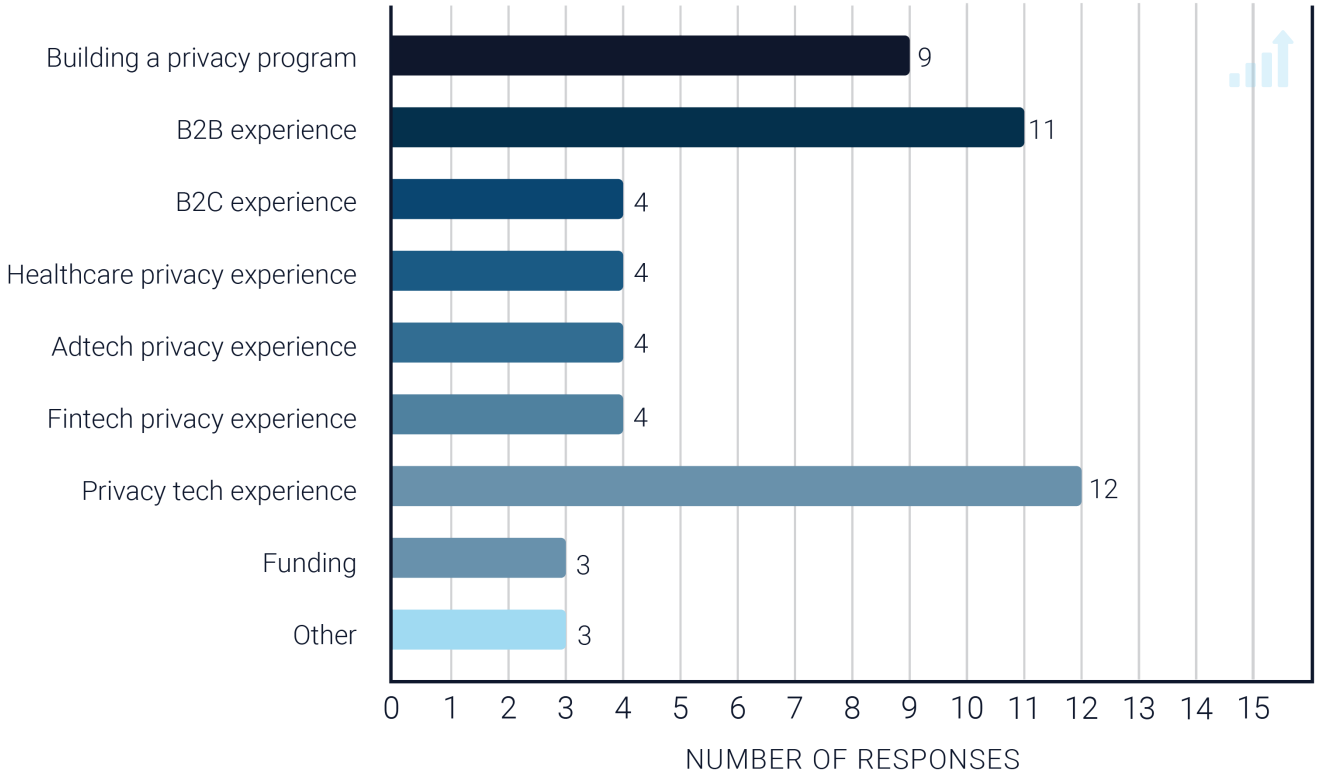


Average number of anticipated privacy tech startups: 4.53
Median number of anticipated privacy tech startups: 3.00

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Which areas of expertise do you offer privacy tech startups?

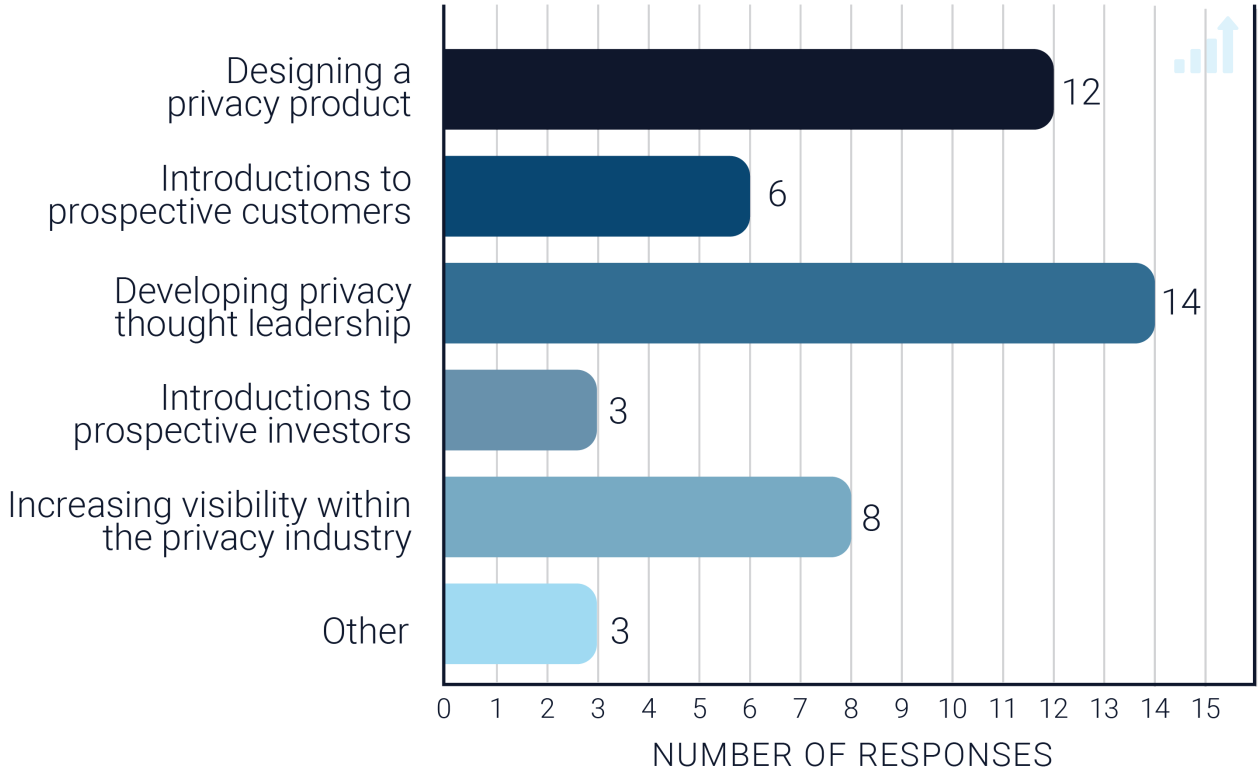
Domain Experts Survey
Answered: 15



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Which challenges can you help privacy tech startups with?

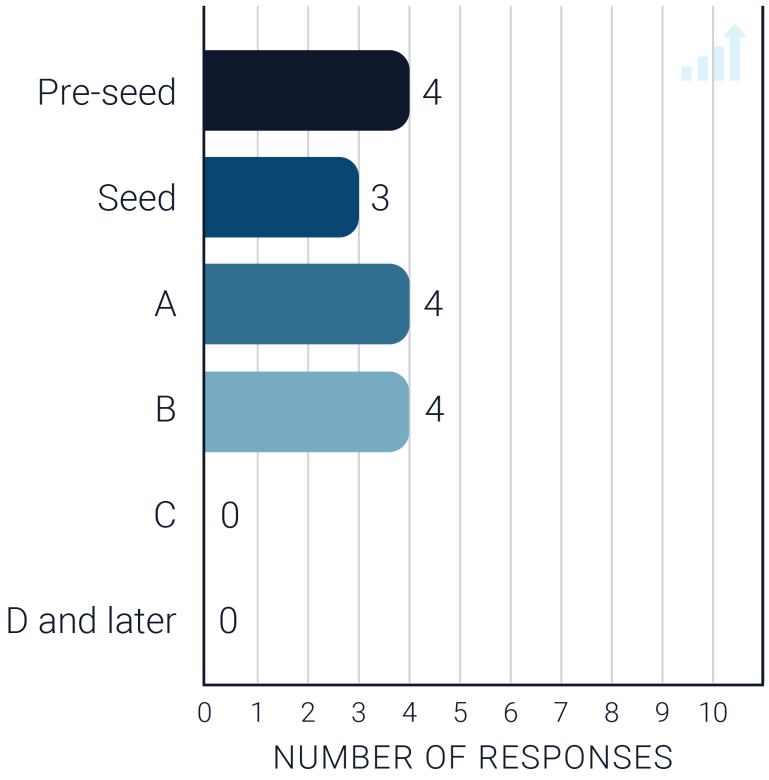
Domain Experts Survey
Answered: 15



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What startup stage are you interested in?

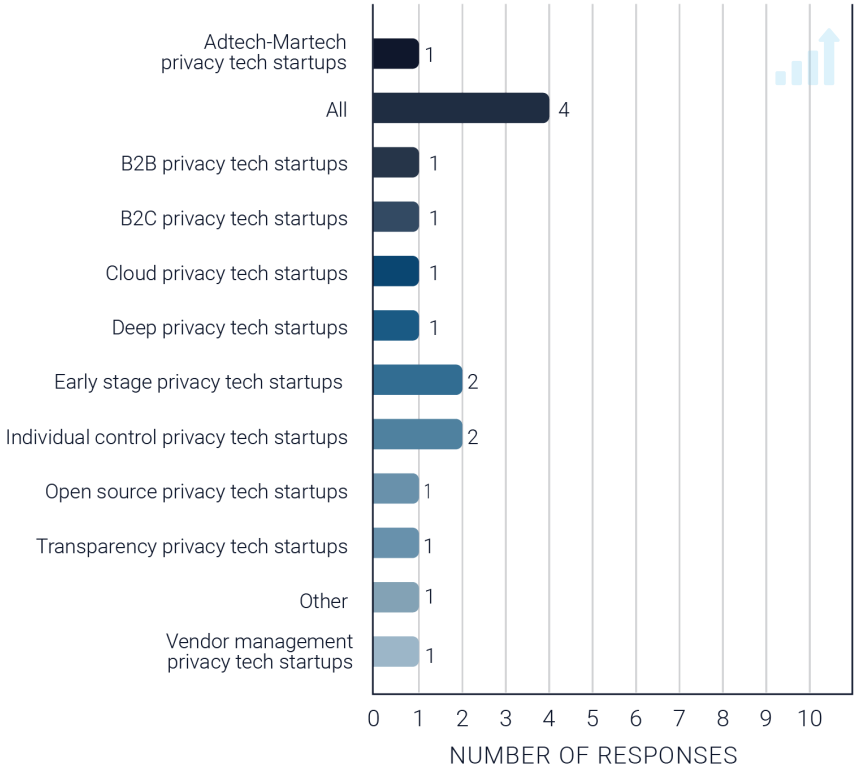
Domain Experts Survey
Answered: 15



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What types of privacy tech startups are you looking to work with?

Domain Experts Survey
Answered: 15

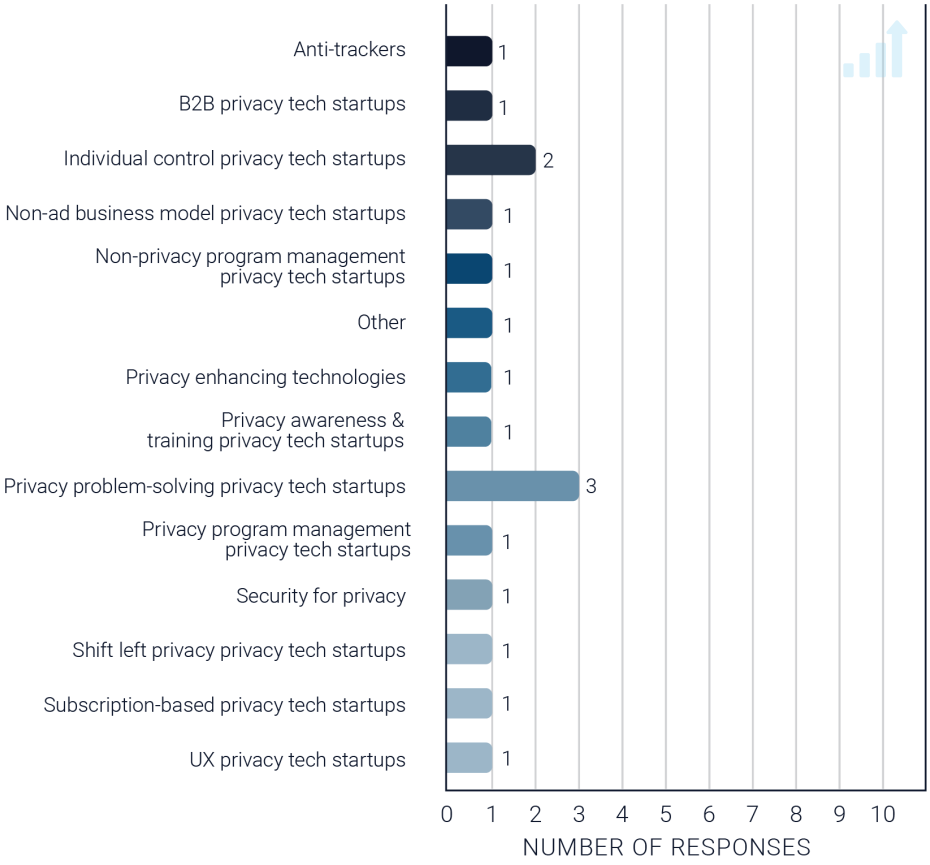


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Pre-Series A, B2C	B2C Privacy TechStartups, Early Stage Privacy TechStartups
All	All
Data ownership, Synthetic data, Digital identity, Blockchain & privacy, other emerging privacy tech	Individual Control Privacy Tech Startups
Ground-breaking innovative martech/adtech	Adtech-Martech Privacy Tech Startups
Those that need help understanding the privacy implications of their products	All
B2B privacy tech startups that are solving current business problems vs. theoretical ones.	B2B Privacy TechStartups
Those addressing consent and data control challenges	Transparency Privacy Tech Startups, Individual Control Privacy Tech Startups
Those operating in the cloud with a SAAS service	Cloud Privacy Tech Startups
Engagement and education	Other
Deep privacy tech	Deep Privacy Tech Startups
Hardware, open-source	Open Source Privacy Tech Startups
Open source project, NGO, probably role in round A startup	Early Stage Privacy Tech Startups
Really all kinds, especially given the vast number that will come under privacy law purview	All
Vendor management tools.	Vendor Management Privacy Tech Startups
Any!	All

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Which types of privacy tech startups do you think are most promising?

Domain Experts Survey
Answered: 15

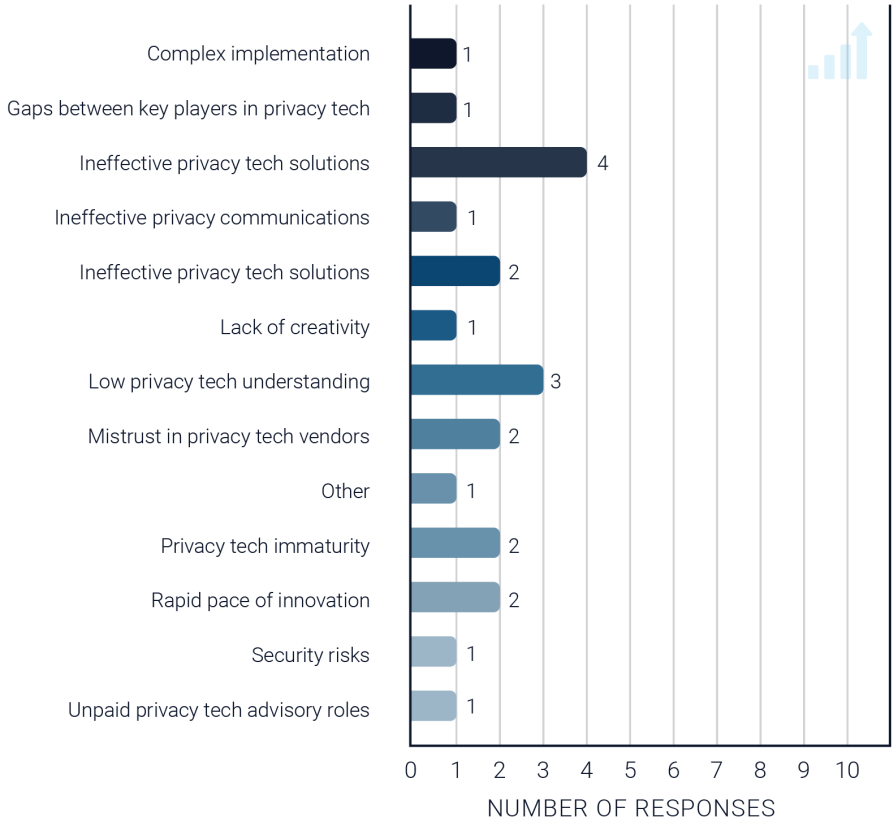


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Anti-tracking and encryption	Security for Privacy, Anti-Trackers
Those solving immediate needs of customers	Privacy Problem-Solving Privacy Tech Startups
Data ownership	Individual Control Privacy Tech Startups
Rethinking the role of adtech/martech and giving back the control to the user	Individual Control Privacy Tech Startups
Anyone doing something other than compliance	Non-Privacy Program Management Privacy Tech Startups
Those that are solving real pain for businesses	Privacy Problem-Solving Privacy Tech Startups
Those with strong UX chops, even if not consumer facing	UX Privacy Tech Startups
Those that compete with OneTrust and help organize, coordinate, and automate compliance needs.	Privacy Program Management Privacy Tech Startups
Engagement and education	Privacy Awareness & Training Privacy Tech Startups
DevPrivOps	Shift Left Privacy Privacy Tech Startups
Subscription-based models not relying upon ad revenue	Subscription-based Privacy TechStartups, Non-Ad Business Model Privacy Tech Startups
SaaS with MPC, HE, FL and synthetic data solutions	Other
Ones that combine data monetization with purpose-driven use they will endure tough challenges	Privacy Problem-Solving Privacy Tech Startups
Privacy Techstartups that solve privacy problems of users, at scale	Vendor Management Privacy Tech Startups
B2B	B2B Privacy Tech Startups

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What are your biggest challenges in working in the privacy tech space?

Domain Experts Survey
Answered: 15

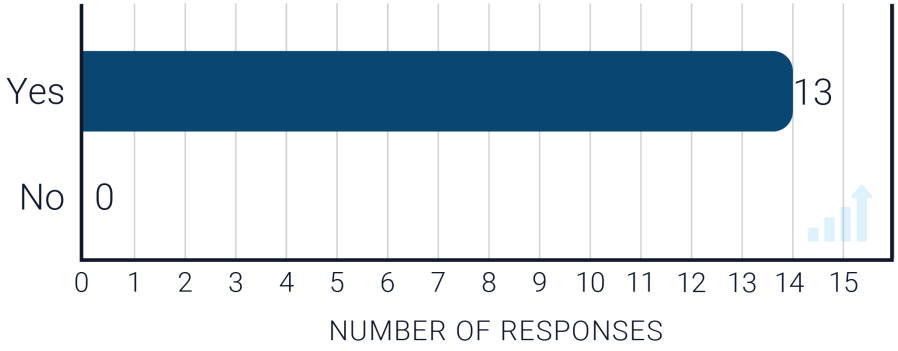


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Rapidly changing tech landscape and lack of understanding by the global community (low tech individuals/consumers)	Rapid Pace of Innovation, Low Privacy Tech Understanding
Thinking out of the box	Lack of Creativity
The biggest challenge in privacy tech is keeping up with the pace of innovation -while- finding the best implementations of those ideas and identifying the real breakout ideas in that mess of creativity.	Rapid Pace of Innovation, Privacy Tech Immaturity
Confusion! It's the intersection of security, engineering, marketing, legal... Lots of misleading/incomplete info, very complex ecosystem, etc.	Low Privacy Tech Understanding, Ineffective Privacy Tech solutions
Misunderstanding by new entrants	Low Privacy Tech Understanding
[redacted] sucks, we need better technology options	Ineffective Privacy Tech solutions
A few advocates in the community with a lot of passion forget that it's not a substitute for effective messaging	Ineffective Privacy Communications
Doing my current advisory roles pro bono	Unpaid Privacy Tech Advisory Roles
Application	Unknown
Bridging gaps	Gaps Between Key Players in Privacy Tech
Avoiding snake oil	Ineffective Privacy Tech solutions
Explainability: the complexity of the services and products and that it's hard to get a overview from the user/business perspective (legal, data scientists and business roles). That it's hard to match a specific business need to a specific pet, and to assess the maturity of the product or service. To create trust in the Privacy Enhancing Technologies products and services of the end user side (creating the right pr spin).Match security and privacy in the pet space (during development lifecycle and knowledge of Privacy Enhancing Technologies among infosec people)	Ineffective Privacy Tech solutions, Mistrust in Privacy Techvendors
Too many players who are just faking it	Ineffective Privacy Tech solutions, Mistrust in Privacy Techvendors
Implementation is a huge issue. It shouldn't take 6-8 months. Internal resources and political capital to deploy.Ease/riskof implementation (will it break or negatively impact other systems). Risks include security, availability of systems.	Ineffective Privacy Tech solutions, Complex Implementation, Security Risks
A one-stop vendor that has many viable features to help in the b2b space	Privacy Tech Immaturity

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Are you interested in buying privacy tech?

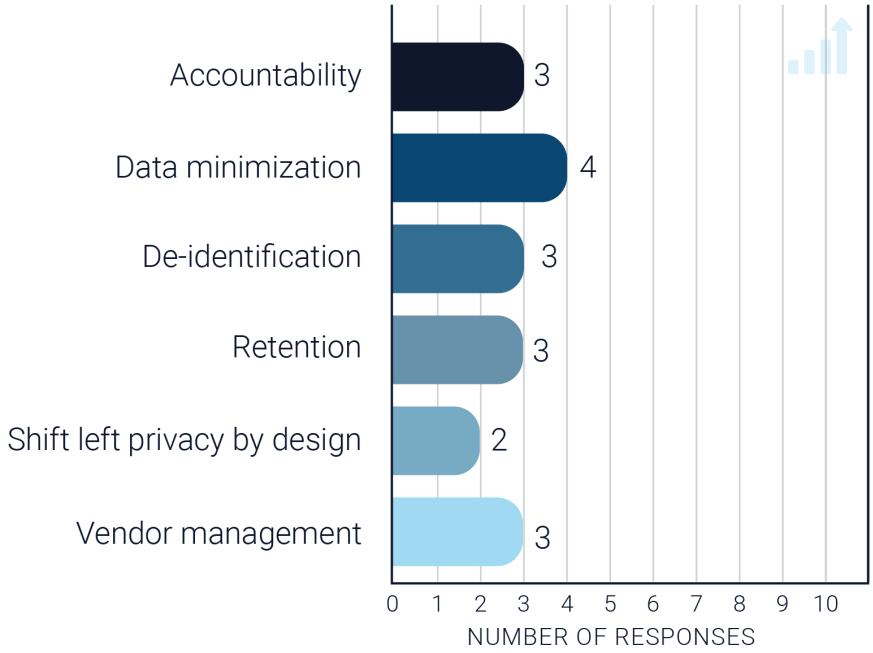
User or Buyer Survey
Answered: 14



Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What types of privacy problems do you have that you wish there was a tool for?

User or Buyer Survey
Answered: 14

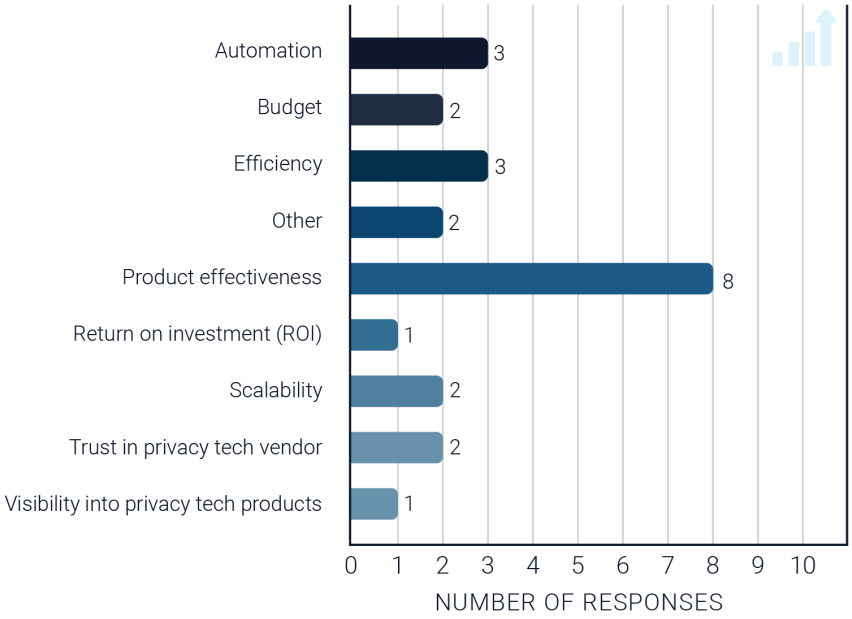


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Data retention	Retention
Data identification, vendor management	Vendor Management, De-Identification
Vendor assessment	Vendor Management
Algorithm/code governance tool	Shift Left Privacy by Design
Differential privacy tools	Data minimization, De-identification
Data deletion and retention policy enforcement	Retention
Third party privacy questionnaire/reviews	Vendor Management
De-identification, eyes-off model training	De-identification
Data minimization	Data minimization
Internal privacy rules repository	Accountability
Data deletion & retention	Retention
Code privacy governance	Shift Left Privacy by Design
1. Realtime data maps 2. Reliable data inventory 3. Privacy preserving data analytics	Accountability, Data Minimization
1) Cradle-to-the-grave data lifecycle data management tool 2) Data processing analytics tool, covering data analytics 3) Privacy audit tools. 4) Age verification. 5) Privacy trust marks.	Accountability, Data Minimization

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

Why are (or aren't) you interested in purchasing privacy tech right now?

User or Buyer Survey
Answered: 14

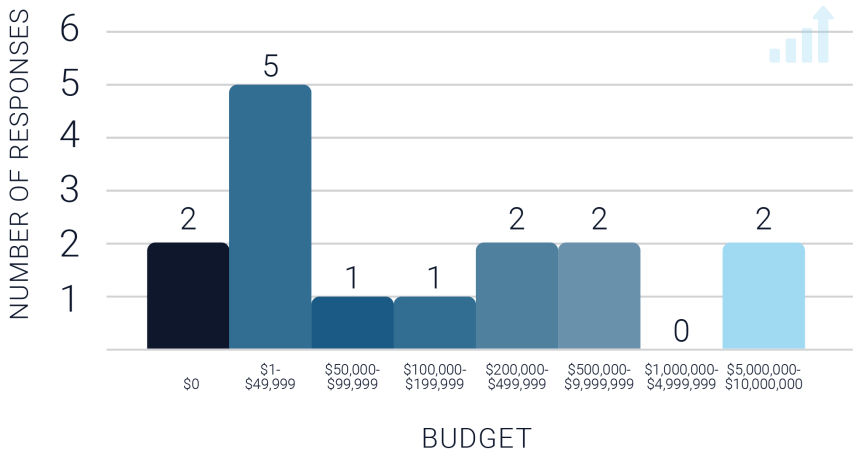


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Effective features	Product Effectiveness
Automation, scalability, documentation	Automation, Scalability,
Interest: manage vendors & other program pain points	Product Effectiveness
Maturity, ROI	Product Effectiveness, ROI
Availability and effectiveness of products	Product Effectiveness
Too many shady tools	Product Effectiveness
Not enough information about what's available	Visibility into Privacy Tech Products
Many organizations struggle with getting started with data science due to privacy concerns. Even before applying DP, FL it anything else, they would need to start looking at data but are blocked on PII/PHI limitations)	Other
Interest: availability of resources, budget. Disinterest: trust in vendor, efficacy of solutions,	Budget, Product Effectiveness, Trust in Privacy Tech Vendor
Interested: to free up headcount, manage privacy program, and become more efficient	Automation, Efficiency
Very interested in purchasing technical solutions to complex privacy tech problems	Product Effectiveness
Interested in deep privacy tech	Other
Building a privacy program from the ground up at a startup, looking for tech to jumpstart program development and increase program maturity year over year. Initial focus on compliance solutions.Budget and strategy yet to be defined.	Automation, Efficiency, Budget
Interest: efficiency and scalability, plug-and-play; disinterest: having to build products for the vendor, promising PbD without following through.	Efficiency, Scalability, Product Effectiveness, Trust in Privacy Tech Vendor

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What's your team's privacy tech tool budget?

User or Buyer Survey
Answered: 14



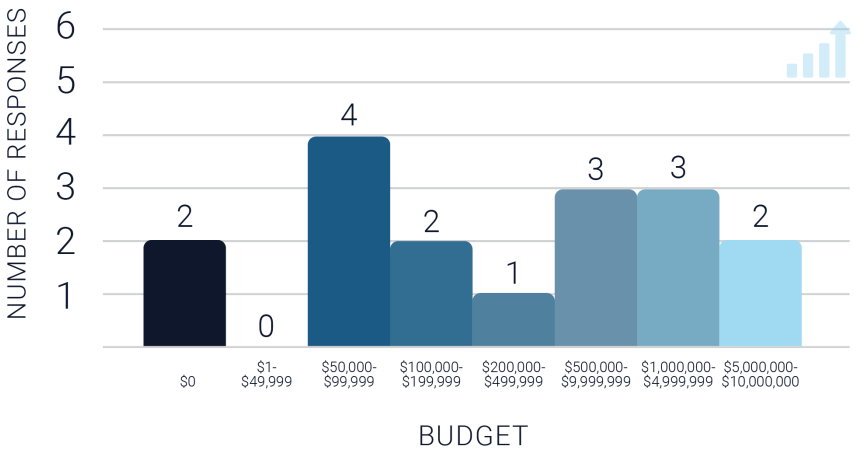
VERBATIM ANSWERS
$00.0
$00.0
$10,000.0
$15,000.0
$25,000.0
$30,000.0
$35,000.0
$55,000.0
$100,000.0
$200,000.0
$205,000.0
$500,000.0
$3,000,000.0
$5,000,000.0

Average team privacy tech tool budget: $655,357.14
Median team privacy tech tool budget: $45,000.00

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What's your company's total privacy tech tool budget?

User or Buyer Survey
Answered: 14



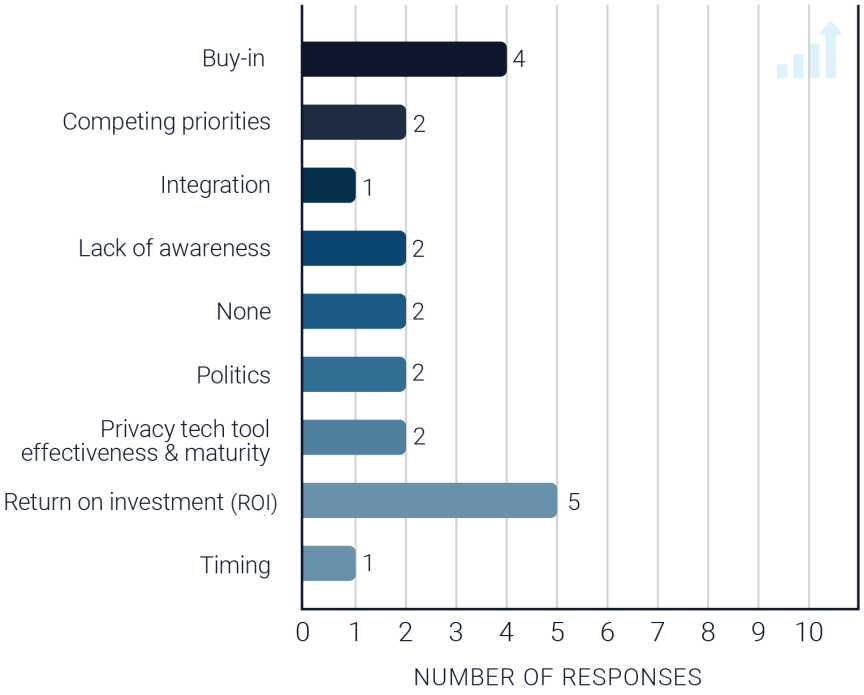
VERBATIM ANSWERS
$00.00
$00.00
$55,000.00
$65,000.00
$75,000.00
$90,000.00
$100,000.00
$155,000.00
$450,000.00
$500,000.00
$500,000.00
$750,000.00
$5,000,000.00
$10,000,000.00

Average company total privacy tech tool budget: $1,267,142.86
Median company total privacy tech tool budget: $127,500.00

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What are some of your challenges in securing a privacy tool budget?

User or Buyer Survey
Answered: 14

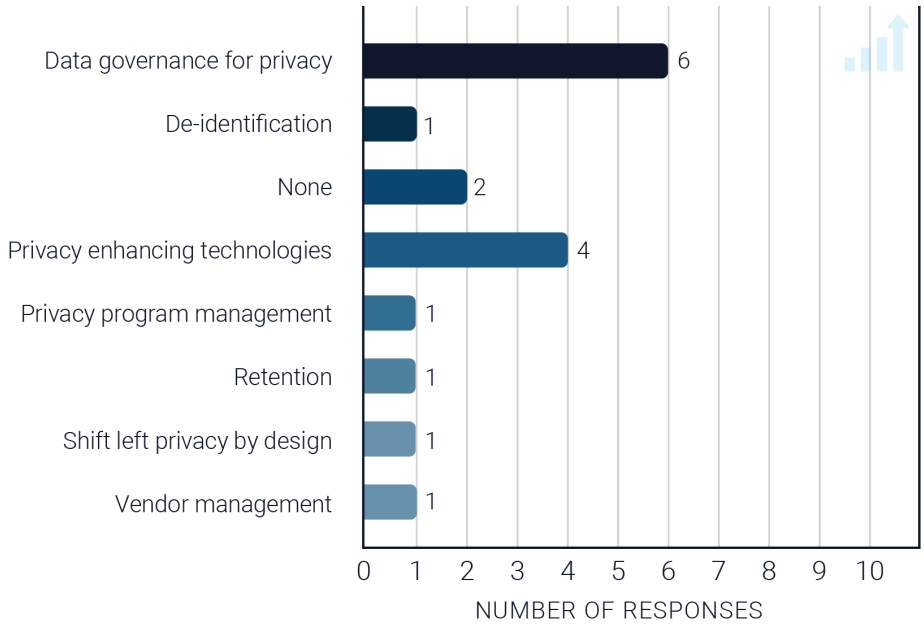


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Timing, team and leadership support, demonstrating value	Timing, Buy-In, ROI
Awareness of risk, other projects take priority	Lack of Awareness, Competing Priorities
Leadership buy in	Buy-In
Demonstrating ROI.	ROI
None	None
Recency bias - FB got away with it	ROI
Integration	Integration
Approval from various stakeholders that the tool covers their compliance needs	Buy-In
Immature products. No products are solving hard technical problems at scale.	Privacy TechTool Effectiveness & Maturity
No challenge. We're able to get budget when we demonstrate a product's value, such as saving on additional headcount.	None
Finding tools that work. Justifying a tool's ability to solve an important business pain point.	Privacy TechTool Effectiveness & Maturity
Internal politics	Politics
1. Initial focus is on compliance, getting budget for privacy tech that falls outside of compliance(GDPR, CCPA) scope is difficult to advocate for. 2. Shared ownership, privacy tools are used by various teams like data infra, analytics, adtech teams and aligning on 1 cost center is difficult. 3. Privacy is not a core business focus area	ROI, Buy-In, Politics, Competing Priorities
Lack of understanding by stakeholders/budget approvers, demonstrating value.	Lack of Awareness, ROI

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What privacy tech tools would you buy if you had the budget?

User or Buyer Survey
Answered: 14

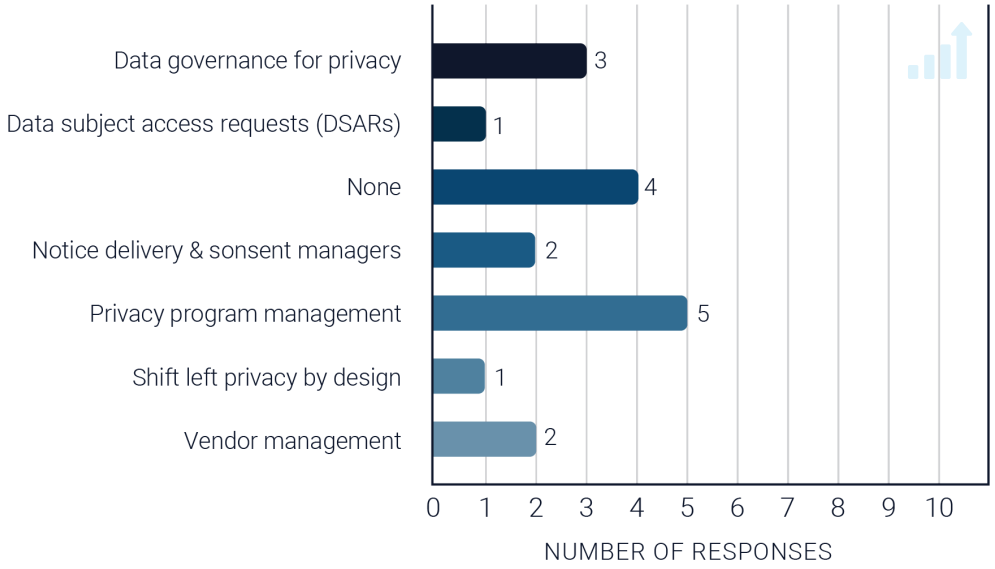


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Data sharing governance	Data Governance for Privacy
Data identification, vendor management	De-Identification, Vendor Management
Data catalogue tool	Data Governance for Privacy
Data discovery	Data Governance for Privacy
Privacy Enhancing Technologies for data analytics	Privacy Enhancing Technologies
Hmm, not sure yet	None
Data inventory	Data Governance for Privacy
N/A	None
Differential privacy tools.	Privacy Enhancing Technologies
Article 30 data inventory tool	Data Governance for Privacy
Data deletion and retention tools	Retention
All the mature Privacy Enhancing Technologies available	Privacy Enhancing Technologies
Privacy by design tools, differential privacy tools	Privacy Enhancing Technologies, Shift Left Privacy by Design
Digital asset management privacy tech tool, to demonstrate good data stewardship and transparency, like a privacy trust mark	Data Governance for Privacy, Privacy Program Management

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What privacy tech tool have you budgeted for?

User or Buyer Survey
Answered: 14

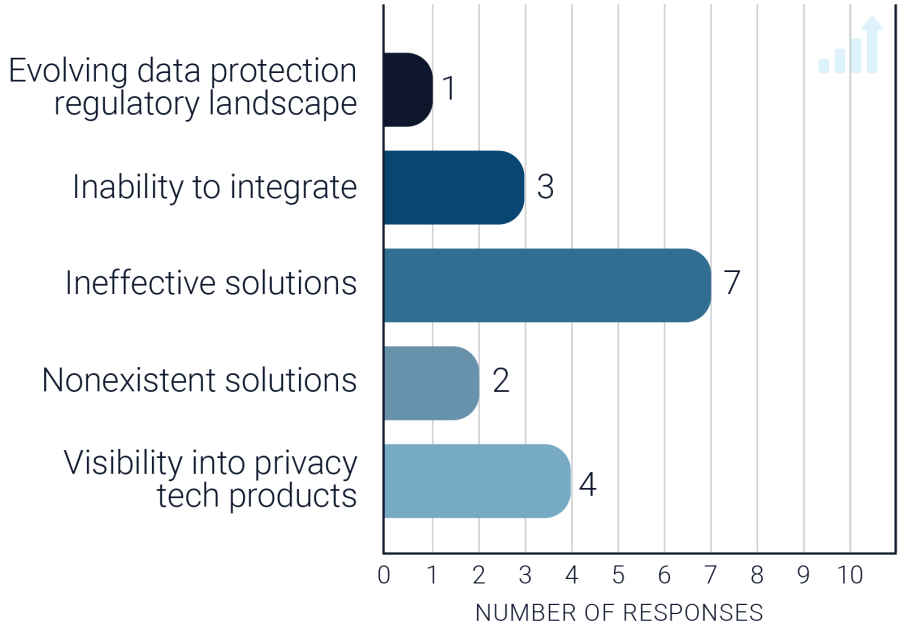


VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
DPIA	Privacy Program Management
None	None
Vendor review tool	Vendor Management
Consent management	Notice Delivery & Consent Managers
N/A	None
N/A	None
PIA	Privacy Program Management
N/A	None
Vendor management tools.	Vendor Management
Data inventory, privacy policy rules repository, PIA tools	Data Governance for Privacy, Privacy Program Management
Privacy engineering training tool	Shift Left Privacy by Design
Privacy training	Privacy Program Management
Data discovery tools (BigID), Cookie Management tools, Consent Management tools	Data Governance for Privacy, Notice Delivery & Consent Managers
PIAs, DSARs, data discovery.	Privacy Program Management, DSARs, Data Governance for Privacy

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

What are your biggest challenges in the privacy tech space?

User or Buyer Survey
Answered: 14



VERBATIM ANSWERS	TRANSLATION FOR GRAPHIC
Not enough available privacy tech tools with good features	Nonexistent Solutions, Ineffective Solutions
Velocity of new laws and regulations and lack of interoperability of standards	Inability to Integrate, Evolving Data Protection Regulatory Landscape
Knowing which tools do what	Visibility into Privacy Tech Products
Product and feature maturity	Ineffective Solutions
Finding promising privacy tech tools	Visibility into Privacy Tech Products
Too many simplistic solutions	Ineffective Solutions
Integrating with existing tools and systems	Inability to Integrate
It's too theoretical and doesn't necessary align with blockers and issues in industry	Ineffective Solutions
Getting market research directly from users/buyers.	Ineffective Solutions
Cutting through the marketing noise and figuring out best in breed	Visibility into Privacy Tech Products
Maturity of products	Ineffective Solutions
Not enough available privacy tech products for technical pain points	Nonexistent Solutions, Ineffective Solutions
Lack of awareness about the tools that exist outside of the big players like [redacted]	Visibility into Privacy Tech Products
Silo'd solutions. Ch integrations.	Inability to Integrate

Source: The Rise of Privacy Tech (TROPT) Defining the Privacy Tech Landscape 2021

ENDNOTES

[1]CrunchBase, Privacy Companies: Summary, https://www.crunchbase.com/hub/privacy-companies (Last Accessed October 28, 2021).
[2]TROPT Privacy Tech Database, https://airtable.com/shrNEnZFaT4q12ezs .
[3]Chandy Gopalakrishnan, "Who's Funding Privacy Tach?" April 20. 2021 for Tech Crunch, https://techcrunch.com/2021/04/20/whos-funding-privacy-tech/ (Last Accessed October 28, 2021).
[4]CrunchBase, Privacy Companies: Summary, https://www.crunchbase.com/hub/privacy-companies (Last Accessed October 28, 2021).
[5]Lourdes Turrecha, "Defining Privacy Tech," May 23, 2021, https://medium.com/privacy-technology/defining-privacy-tech-ae7b022888ec (Last Accessed October 28, 2021).
[6][See, for example NIST, "NIST Develops Privacy-Preserving Encounter Metrics That Could Help Slow Down Future Pandemics," March 29, 2021, https://www.nist.gov/news-events/news/2021/03/nist-develops-privacy-preserving-encounter-metrics-could-help-slow-down (Last Accessed October 28, 2021), or UCSF, "UCSF Launches Pilot of Privacy-Preserving Smartphone Tool to Help Slow Spread of COVID-19," September 30, 2020, https://www.ucsf.edu/news/2020/09/418646/ucsf-launches-pilot-privacy-preserving-smartphone-tool-help-slow-spread-covid (Last Accessed October 28, 2021).
[7]Apple and Google, "Privacy-Preserving Contact Tracing," https://covid19.apple.com/contacttracing (Last Accessed October 28, 2021).
[8]Emily Ashley & Lourdes Turrecha, "Apple's iOS 14 privacy labels are rolling out today – and other notable iOS 14 privacy features," December 8, 2020, https://medium.com/privacy-technology/ios14s-privacy-labels-are-being-rolled-out-today-plus-its-other-notable-privacy-features-3e528db63901 (Last Accessed October 28, 2021).
[9]Apple Newsroom, "Apple advances its privacy leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8," June 7, 2021, https://www.apple.com/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/ (Last Accessed October 28, 2021).
[10]Jason Aten, "How Signal Became the Most Popular App in the World Overnight," January 16, 2021 for Inc.com, https://www.inc.com/jason-aten/how-signal-became-most-popular-app-in-world-overnight-why-it-matters.html (Last Accessed October 28, 2021).
[11]Rae Hodge, "What is Signal? Everything you need to know about Elon Musk's app recommendation," January 28, 2021 for Cnet Tech, https://www.cnet.com/tech/services-and-software/what-is-signal-everything-you-need-to-know-about-elon-musks-app-recommendation/ (Last Accessed October 28, 2021).
[12]Brave, "Brave Passes 36 Million Monthly Active Users," September 2, 2021, https://brave.com/36m-mau/ (Last Accessed October 28, 2021).
[13]Gilad Edelman, "DuckDuckGo's Quest to Prove Online Privacy is Possible," June 16, 2021 for Wired, https://www.wired.com/story/duckduckgo-quest-prove-online-privacy-possible/ (Last Accessed October 28, 2021).
[14]Nick Lucchesi, "Protonmail hits 5 Million Accounts and Wants Users to Ditch Google by 2021," September 17, 2018 for Inverse, https://www.inverse.com/article/49041-protonmail-ceo-andy-yen-interview (Last Accessed October 28, 2021).
[15]Natasha Lomas, "Proton, the Privacy Startup Behind E2E Encrypted ProtonMail, Confirms Passing 50M Users," May 19, 2021 for TechCrunch, https://techcrunch.com/2021/05/19/__trashed-13/ (Last Accessed October 28, 2021).
[16]See Alan F. Westin, "Privacy and Freedom," March 1, 1968 https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr&ref=hackernoon.com (Last Accessed October 28, 2021).
[17]See Carissa Veliz, "Privacy is Power: Why and how you should take back control of your data," https://www.penguinrandomhouse.com/books/673341/privacy-is-power-by-carissa-veliz/.
[18]See Neil M. Richards and Woodrow Hartzog, "Privacy's Trust Gap," January 17, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899760 (Last Accessed: October 29, 2021) and Ari Ezra Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World," August 14, 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309632 (Last Accessed: October 29, 2021).
[19]See Daniel J. Solove, "Understanding Privacy," May 5, 2008, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888 (Last Accessed October 28, 2021).
[20]For example, purpose and use limitation are hotly debated as out-of-date in today's data-driven world.
[21]OECD: Privacy Principles, http://oecdprivacy.org; Information Commissioner's Office, Guide to the GDPR: Principles, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/princi-

ples/; Department of Homeland Security: The Fair Information Practice Principles, https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles; IAPP: Fair Information Practice Principles, https://iapp.org/resources/article/fair-information-practices/; PIPEDA Fair Information Principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/; FTC: Privacy Online (A Report to Congress), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (All links last Accessed October 28, 2021).

[22]Oxford Learner's Dictionaries, "Technology," https://www.oxfordlearnersdictionaries.com/us/definition/english/technology (Last Accessed October 28, 2021).

[23]Merriam-Webster, "Technology," https://www.merriam-webster.com/dictionary/technology (Last Accessed October 28, 2021).

[24]Lourdes Turrecha, "Defining Privacy Tech," May 23, 2021, https://medium.com/privacy-technology/defining-privacy-tech-ae7b022888ec (Last Accessed October 28, 2021).

[25]See Alan F. Westin, "Privacy and Freedom," March 1, 1968 https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr&ref=hackernoon.com (Last Accessed October 28, 2021).

[26]See Carissa Veliz, "Privacy is Power: Why and how you should take back control of your data," https://www.penguinrandomhouse.com/books/673341/privacy-is-power-by-carissa-veliz/ .

[27]See Neil M. Richards and Woodrow Hartzog, "Privacy's Trust Gap," January 17, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899760 (Last Accessed: October 29, 2021) and Ari Ezra Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World," August 14, 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309632 (Last Accessed: October 29, 2021).

[28]European Commission's Charter of Fundamental Rights, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en (Last Accessed October 28, 2021).

[29]Office of the Privacy Commissioner of Canada, "Privacy Enhancing Technologies -- A Review of Tools and Techniques," November 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#fn9 (Last Accessed October 28, 2021).

[30]OECD Working Party on Information Security and Privacy, "Inventory of Privacy-Enhancing Technologies (PETs)," January 7, 2002, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final (Last Accessed October 28, 2021).

[31]John J. Borking and Charles Raab. Laws, PETs and Other Technologies for Privacy Protection. Journal of Information, Law and Technology, 1:1–14, 2001.

[32]Lourdes Turrecha, "Defining Privacy Tech," May 23, 2021, https://medium.com/privacy-technology/defining-privacy-tech-ae7b022888ec (Last Accessed October 28, 2021).

[33]S.224 Promoting Digital Privacy Technologies Act, Introduced February 4, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/224/text (Last Accessed October 28, 2021).

[34]Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," January 2011 for Information & Privacy Commissioner of Ontario, Canada, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (Last Accessed October 28, 2021).

[35]Lourdes Turrecha, "Defining Privacy Tech," May 23, 2021, https://medium.com/privacy-technology/defining-privacy-tech-ae7b022888ec (Last Accessed October 28, 2021).

[36]Michelle Finneran Dennedy, Jonathan Fox, and Thomas R. Finneran, "The Privacy Engineer's Manifesto," https://link.springer.com/book/10.1007/978-1-4302-6356-2 (Last Accessed October 28, 2021).

[37]Lourdes M. Turrecha, "Defining Privacy Tech," May 23, 2021, https://medium.com/privacy-technology/defining-privacy-tech-ae7b022888ec (Last Accessed October 28, 2021).

[38]Id.

[39]Jake Frankenfield, "Tor," August 4, 2021 for Investopedia, https://www.investopedia.com/terms/t/tor.asp (Last Accessed October 28, 2021).

[40]Techopedia Dictionary, "Identity Management (ID Management)," https://www.techopedia.com/definition/13636/identity-management-id-management (Last Accessed October 28, 2021).

[41]Gartner Glossary, "Identity Management," https://www.gartner.com/en/information-technology/glossary/identity-management (Last Accessed October 28, 2021).

[42]Techopedia Dictionary, "Data Infrastructure," https://www.techopedia.com/definition/31682/data-infrastructure (Last Accessed October 28, 2021).

[43]Gartner Glossary, "Marketing Technology." https://www.gartner.com/en/marketing/glossary/marketing-technology (Last Accessed October 28, 2021).

[44]Gartner Glossary, "Ad tech," https://www.gartner.com/en/information-technology/glossary/ad-tech (Last Accessed October 28, 2021).

[45]Chris Metinko, "Legal Tech Makes Its Case With Venture Capitalists, Tops $1B In Funding This Year," September 23, 2021

for Crunchbase News, https://news.crunchbase.com/news/legal-tech-venture-investment/ (Last Accessed October 28, 2021).
[46]The Data Governance Institute, "Defining Data Governance." https://datagovernance.com/defining-data-governance/ (Last Accessed October 28, 2021).
[47]Web3 Foundation, "About" page https://web3.foundation/about/ (Last Accessed October 28, 2021).
[48]Geoffrey A. Fowler, "87 percent of websites are tracking you. This new tool will let you run a creepiness check," September 25, 2020 for The Washington Post, https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight/ (Last Accessed October 28, 2021).
[49]The Markup: Blacklight, https://themarkup.org/series/blacklight (Last Accessed October 28, 2021).
[50]At a high level, differential privacy provides a mathematically rigorous definition of privacy that quantifies risk. It introduces carefully calibrated "noise," or random and meaningless data, to mask personal data. See Harvard University Privacy Tools Project: Differential Privacy, https://privacytools.seas.harvard.edu/differential-privacy
Secure multi-party computation (SMPC) allows multiple parties to "jointly compute an arbitrary functionality without revealing their own private inputs and outputs." See Zhao et al;, "Secure Multi-Party Computation: Theory, Practice, and Applications," https://www.sciencedirect.com/science/article/abs/pii/S0020025518308338.
Zero Knowledge Proofs (ZKPs) are a cryptographic method that allows one party to prove (the prover) to another (the verifier) that they know a statement to be true without sharing additional information. See Massachusetts Institute of Technology Theory of Computation: Zero-knowledge Proofs, https://toc.csail.mit.edu/node/218.
[51]Transmute, "Encrypted Data Vaults for Trusted Data Access," January 14, 2020, https://medium.com/transmute-techtalk/encrypted-data-vaults-c794055b170e (Last Accessed October 28, 2021).
[52]Data Protection Commission, "The Right of Access," https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information (Last Accessed October 28, 2021); Stinson LLP, "Preparing for the CRPA," January 22, 2021 for JD Supra, https://www.jdsupra.com/legalnews/privacy-2021-preparing-for-the-cpra-7038388/ (Last Accessed October 28, 2021); The Colorado Privacy Act (Bill Text), https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (Last Accessed October 28, 2021); and Virginia Consumer Data Protection Act (Bill Text), https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+SB1392 (Last Accessed October 28, 2021).
[53]Shawn Keve, "Privacy Must Be Central to Identity and Access Management," May 7, 2020 for Forbes, https://www.forbes.com/sites/forbestechcouncil/2020/05/07/privacy-must-be-central-to-identity-and-access-management/?sh=82ed578696ea (Last Accessed October 28, 2021).
[54]CPO Magazine, "Working Together for Privacy Protection: Identity Management Best Practices for Companies and Consumers," June 29, 2021, https://www.cpomagazine.com/cyber-security/working-together-for-privacy-protection-identity-management-best-practices-for-companies-and-consumers/ (Last Accessed October 28, 2021).
[55]Mark Settle, "Privacy Debt: The Achilles Heel of Every IT Organization," September 10, 2020 for Forbes, https://www.forbes.com/sites/marksettle/2020/09/10/privacy-debt-every-it-organization/?sh=3eb5ead87a3d (Last Accessed October 28, 2021).
[56]Thor Olavsrud, "Data Governance: A best practices framework for managing data assets," March 18, 2021 for CIO Magazine, https://www.cio.com/article/3521011/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html (Last Accessed October 28, 2021).
[57]PwC, "Five steps to meeting the CPRA's new data retention requirements," https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/cpra-data-retention-preparation.html (Last Accessed October 28, 2021).
[58]EY, "How to Minimize Risk through Data Disposition," February 19, 2021, https://www.ey.com/en_us/consulting/how-to-minimize-risk-through-data-disposition (Last Accessed October 28, 2021).
[59]NIST Computer Security Resource Center Glossary, "De-identification" https://csrc.nist.gov/glossary/term/de_identification (Last Accessed October 28, 2021).
[60]Bryan Cave Leighton Paisner, "What is 'pseudonymized' data?," January 17, 2020, https://www.bclplaw.com/en-US/insights/what-is-pseudonymized-data.html (Last Accessed October 28, 2021).
[61]NIST Privacy Engineering Program, "De-identification Tools," https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/de-id/tools (Last Accessed October 28, 2021).
[62]Richard Seiersen, "A Modern Shift-Left Security Approach," January 4, 2021 for Forbes, https://www.forbes.com/sites/forbestechcouncil/2021/01/04/a-modern-shift-left-security-approach/?sh=19fab35a7729 (Last Accessed October 28, 2021).
[63]Steve O'Hear, "Digi.me and Personal merge to put you in control of the nascent 'personal data ecosystem," August 17, 2017 for TechCrunch, https://techcrunch.com/2017/08/17/digi-me-and-personal-merge/ (Last Accessed October 28, 2021).
[64]GDPR, CCPA, HIPAA, amongst many other data protection laws require organization to pass down privacy and security

requirements to their vendors and other third parties processing personal information.
[65]See, for example: TROPT Data Privacy Day 2021, The Marketplace Demand for Privacy https://www.youtube.com/watch?v=rR7npMhyp_w (Last Accessed October 25, 2021); Andrew Perrin, "Half of Americans have decided not to use a product or service because of privacy concerns," April 14, 2020 for Pew Research Center, https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/ (Last Accessed: October 29. 2021); and Consumer Reports, "Consumer Reports Study Finds Marketplace Demand for Privacy and Security," October 21, 2020, https://www.consumerreports.org/media-room/press-releases/2020/10/consumer-reports-study-finds-marketplace-demand-for-privacy-and-security/ (Last Accessed: October 29, 2021)
[66]TROPT Data Privacy Day 2021, "The Marketplace Demand for Privacy," https://www.youtube.com/watch?v=rR7npMhyp_w (Last Accessed: October 25, 2021).
[67]Figures pulled from: The Forum for Sustainable and Responsible Investment (US SIF), "Sustainable and Impact Investing Overview," https://www.ussif.org/files/2018%20Infographic%20overview%20%281%29%281%29.pdf (Last Accessed: October 29, 2021); US SIF, "2020 Report on US Sustainable and Impact Investing Trends," https://www.ussif.org/files/US%20SIF%20Trends%20Report%202020%20Executive%20Summary.pdf (Last Accessed: October 29, 2021); and Anne Field, "With $715B in AUM, Impact Investors Stay the Course, Despite the Pandemic, Says the GIIN," June 16, 2020 for Forbes, https://www.forbes.com/sites/annefield/2020/06/16/with-715b-in-aum-impact-investors-stay-the-course-despite-the-pandemic-says-the-giin/?sh=377bde166d3c (Last Accessed: October 29, 2021).
[68]CrunchBase, Privacy Companies: Summary, https://www.crunchbase.com/hub/privacy-companies (Last Accessed October 28, 2021).
[69]TROPT Privacy Tech Deal Flow Tool. For startups: https://www.riseofprivacytech.com/founders/. For investors: https://www.riseofprivacytech.com/investors/.

ABOUT THE RISE OF PRIVACY TECH

The Rise of Privacy Tech's (TROPT) mission is to fuel privacy innovation. We do this by bringing together privacy tech founders, investors, experts, and user-buyers to bridge the tech-capital-expertise gaps in privacy tech.

TROPT was founded by Lourdes M. Turrecha. TROPT's inaugural advisors include Michelle Dennedy, Melanie Ensign, Debra Farber, Gilbert Hill, and Fatima Khan.

THE RISE OF PRIVACY TECH

Contact information for The Rise of Privacy Tech (TROPT) can be found at www.riseofprivacytech.com.

Published November 2021.