How Privacy Tech Is Bought and Deployed

iapp | TrustArc

How Privacy Tech Is Bought and Deployed

Executive Summary

For the second year running, the IAPP together with TrustArc surveyed 345 privacy professionals around the globe to gain an understanding of how privacy technology products are purchased and deployed within an organization. Since 2017, the IAPP has mapped out the privacy tech marketplace through the IAPP Privacy Tech Vendor Report, which identifies 10 categories of products. Like the 2018 survey, results this year shine a light on which products are in use and under whose budget privacy tech purchases are made, as well as other budgetary and purchase-decision-making insights.

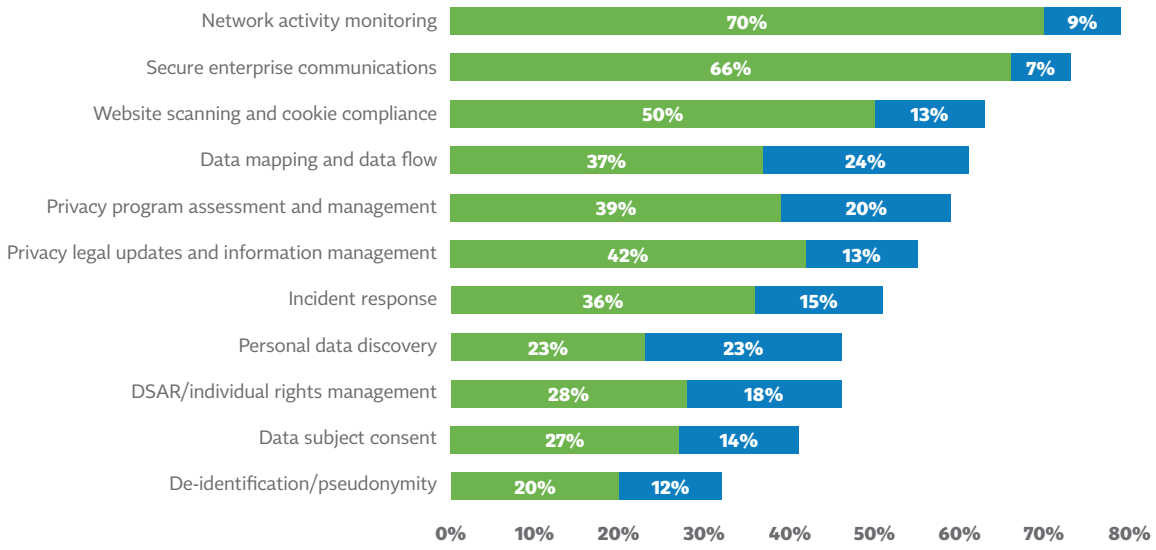
The increasing complexity of modern business in the digital world, coupled with a cacophony of global privacy frameworks, has increased the need for organizations to adopt solutions that demonstrate compliance and are scalable and efficient.

Similar to last year's survey, it is clear that certain technologies belong to the information technology and information security side of the organization, while others clearly fall under the privacy department's domain. Yet others may fall under the marketing department. As outlined in the IAPP Privacy Tech Vendor Report, however, the tools identified generally fit under two broad categories: enterprise privacy management and privacy program management solutions.

There is no shortage of data that comes out of this 2019 survey, but there are some worthy takeaways. For one, products that help enterprises discover and map data flows are poised for growth. Second, and perhaps even more noteworthy, privacy and data protection professionals increasingly have input into certain privacy technology purchases, though they often have less budgetary control.

Last year's survey served as a baseline for market adoption. The 2019 survey builds on that baseline and helps chart where privacy tech market adoption is likely heading in the next year. On the whole, the news is good for vendors and privacy pros alike.

Organizations that have purchased or are planning to purchase in the next 12 months



- **In line with last year's results, enterprise-wide technologies that** increase security or affect an organization's IT architecture have a more mature standing in the marketplace. A vast majority of respondents have purchased, tested and implemented network activity monitoring and secure enterprise communications and thus have no plans to purchase such tools in the near future.

- **Significantly, the most likely** products that respondents are planning to purchase in the next 12 months are data-mapping and data-flow tools, followed by personal data discovery products and privacy program assessment and management solutions. It's also worth noting that data subject access request/individual rights management tools — a new category in the survey this year — are also on the rise; nearly one in five respondents has plans to purchase DSAR tools in the next year. All these categories are in the privacy program management realm rather than the enterprise side, a positive trend for the privacy department.

- **Unsurprisingly, lack of budget and resources** is the number one barrier to privacy tech adoption, followed by getting approval and the immaturity of privacy tech solutions. Another notable reason privacy pros are not purchasing these tools from vendors is that they have already developed their own in-house solutions.

- **The biggest driver for privacy tech** adoption is the need to demonstrate compliance. With the arrival of the EU General Data Protection Regulation and other more recent privacy laws, including the California Consumer Privacy Act, this need to demonstrate compliance has grown in significance in the last year.

- **Increased privacy obligations** and proliferation of new privacy tech solutions have brought the privacy office into tech-purchasing decisions. Most notably, the privacy/data protection office is most frequently involved in the decision to purchase privacy program assessment and management solutions. These are closely followed by privacy legal updates and information management tools, DSAR/individual rights management, and data subject consent tools.

- **In 8 out of 11 product categories**, at least one-quarter of respondents said the privacy/data protection office is involved in the decision to acquire and use tools. This includes more enterprise-wide solutions or solutions that involve infosecurity or information technology, including website scanning and cookie compliance, incident response, and deidentification/pseudonymity.

- **Though the privacy/data protection** office is consistently involved in purchasing decisions, it is IT/infosec that most often controlled the budget for secure enterprise communications, network activity monitoring, incident response, deidentification/pseudonymity, website scanning and cookie compliance, and personal data discovery.

- **However, the privacy/data protection** office most commonly holds the budget for privacy program assessment and management, followed by privacy legal updates and information management, DSAR/individual rights management and data subject consent. The privacy/data protection office controls the budget for data mapping and data flow about just as often as IT does.

- **Of the categories outlined in this** survey, respondents said they are least likely to purchase deidentification/pseudonymity tools in the next 12 months. This is a change from last year, when data subject consent tools were the least likely to be purchased. Perhaps deidentification tools are simply too niche for widespread adoption.

- **For tech vendors, sales calls** should include not just the privacy team, but also members of the legal and IT teams when possible. Privacy and data protection teams are likely to be involved in privacy-tech-purchasing decisions when data mapping and program management tools are involved — two of the tools most poised for new growth according to our survey — while legal was often involved in personal data discovery decisions. Still, because these tools need to be integrated into existing IT systems, it's often IT that controls the budget, even for privacy tools.

- **Our results did not show any meaningful differences** in privacy-tech-purchasing habits between regulated (e.g., financial and health) and nonregulated industries or among companies by size.

- **Overall, the data demonstrates** there were few notable changes from when the survey was conducted last year. We did not see a significant shift from potential buyers to completed sales. The percentage of interested buyers stayed roughly the same over last year, with a few converting to actual purchasers, and some dropping out of the market. Because we didn't survey exactly the same people, of course, these trends are speculative.

- **In general, this year's survey seems** to show that the market for privacy tech is far from saturated given the number of respondents who said they will purchase some form of privacy tech in the next 12 months.

Introduction

The EU General Data Protection Regulation, which came into force last year, created a demand for in-house privacy professionals, increased pressure on and demand for outside privacy counseling and consulting, and required growth in headcount at regulators' offices.

It also pushed privacy technology solutions, which had been developing for a few years, into prime time.

Not only do privacy professionals need tools to organize and record data mapping and inventory exercises, as well as systems for conducting privacy and data protection impact assessments, they also increasingly need technical assistance with consent management, cookie compliance, data subject access requests, and the like.

The impending implementation of the California Consumer Privacy Act — the first comprehensive privacy law of its kind in the United States — creates similar time-sensitive obligations for organizations, especially in data subject rights of access, rectification and deletion.

Information privacy's close and older cousin, information security, has helped to create a market for enterprise solutions for managing such tasks as network activity monitoring and incident response. These tools are often purchased and used by the information technology team and/or the information security team. As the IAPP has documented the growth of the privacy tech sector — including producing the annual Privacy Tech Vendor Report, now in its third year — we have started to ask: Who is buying and using privacy tech tools? How involved is the privacy team in acquiring technical solutions for their growing data governance responsibilities?

This report follows up on a similar one the IAPP and TrustArc conducted in 2018. This year, we surveyed 345 privacy professionals from around the globe about what tools they have purchased, what they plan to buy in the future, and what they have no plans to buy any time soon. We also asked about who owns the budget for these kinds of tools and who influences the decision to buy. The results can be used to help gauge the health and maturity of this important growing industry.

We hope you find the report informative and useful.

Chris Babel, CEO, TrustArc

J. Trevor Hughes, CIPP, CEO, IAPP

The privacy tech marketplace

Privacy and data protection compliance are not new. They go back decades, but a broader combination of legal obligations in recent years and rapid technological advancement across industry verticals have greatly increased enterprise risk and generated more complicated compliance obligations. Much of this is in the scope of the privacy department. More recently, the advent of the GDPR and CCPA means companies of virtually every stripe must know what personal information they have, where it's stored, how it's processed, and who it's shared with. Individuals, particularly in the EU, but soon in California and perhaps across the U.S., have more rights around their data. Organizations need to be nimble and accurate in responding to data subject access requests, consent changes, data portability and so on. To be agile, efficient and scalable, departments need technological solutions.

In recent years, the market responded to increased organizational needs around privacy compliance. The wealth of new privacy tech startups created an entirely new marketplace that wasn't a reality just five or so years ago. The IAPP first documented this marketplace in 2017 with its inaugural Privacy Tech Vendor Report. That first iteration included more than 50 vendors across nine product categories. By the fourth quarter of 2018, the Privacy Tech Vendor Report documented nearly 200 privacy tech vendors across 10 product categories. And the market has yet to slow down.

When the IAPP first launched the Privacy Tech Vendor Report, one challenge was defining the categories of tools vendors have created to solve myriad data protection problems. The following chart lists the product category descriptions defined in the Privacy Tech Vendor report and used in this survey to evaluate privacy tech engagement in the marketplace.

PRIVACY PROGRAM MANAGEMENT – solutions designed specifically for the privacy office

Assessment managers tend to automate different functions of a privacy program, such as operationalizing PIAs, locating risk gaps, demonstrating compliance, and helping privacy officers scale complex tasks requiring spreadsheets, data entry, and reporting.

Consent managers help organizations collect, track, demonstrate and manage users' consent.

Data mapping solutions can come in manual or automated form and help organizations determine data flows throughout the enterprise.

Incident response solutions help companies respond to a data breach incident by providing information to relevant stakeholders of what was compromised and what notification obligations must be met.

Privacy information managers provide organizations with extensive and often automated information on the latest privacy laws around the world.

Website scanning is a service that primarily checks a client's website in order to determine what cookies, beacons and other trackers are embedded in order to help ensure compliance with various cookie laws and other regulations.

DSAR/individual rights management tools help organizations manage and operationalize data subject access requests.

ENTERPRISE PRIVACY MANAGEMENT – solutions designed to service the needs of the privacy office alongside the overall business needs of an organization

Activity monitoring helps organizations determine who has access to personal data and when it is being accessed or processed. These solutions often come with controls to help manage activity.

Data discovery tends to be an automated technology that helps organizations determine and classify what kind of personal data they possess to help manage privacy risk and compliance.

De-identification/pseudonymity solutions help data scientists, researchers and other stakeholders derive value from datasets without compromising the privacy of the data subjects in a given dataset.

Enterprise communications are solutions that help organizations communicate internally in a secure way in order to avoid embarrassing or dangerous leaks of employee communications.

Though the Privacy Tech Vendor Report is a good road map of which vendors are in the space and what products they offer, this year's survey, like last year's, goes further to investigate deeper questions about adoption and budgetary control to help assess the state of the marketplace. Which categories of products are in higher demand than others? Who in the organization has budget for such tools, and who has input for purchasing decisions?

To drive this survey, the IAPP and TrustArc asked nearly 350 privacy professionals from around the world a series of questions about privacy tech vendor products and the purchasing decisions around them. Benchmarked against last year's survey, on the whole, there has not been a significant shift in the data, indicating that the market is still maturing.

The top four categories that respondents were planning to purchase in the next 12 months are products that primarily fit under the privacy program management sphere of influence. At the top of the pack is data mapping and data flow, at 24%. With obligations such as the GDPR in full effect, it's not surprising that this is a vendor solution at the top of a privacy department's wish list. Mapping data flows integrates naturally with personal data discovery, the second highest category for planned purchase, at 23%. Knowing what data an organization possesses, where it's located, how it flows, and who it's attached to are foundational aspects of creating a privacy-compliant framework within the enterprise and helping organizations get in line with regulations, like the GDPR.

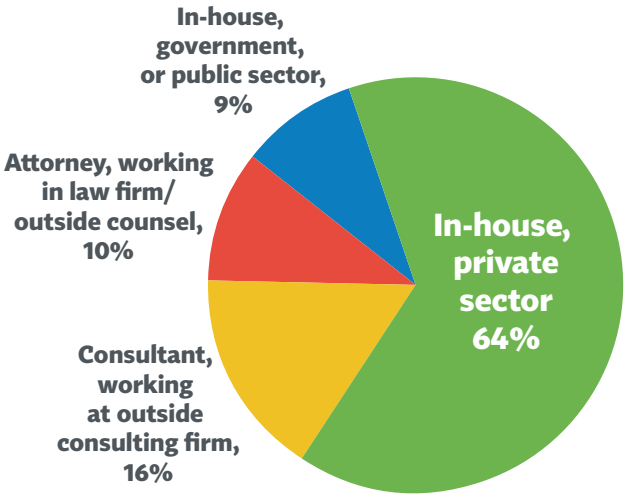
Also, unsurprisingly, privacy program assessment and management is near the top of planned purchases in the next 12 months. One in five respondents identified this category as a likely purchase in this year's survey. These solutions play a large role in operationalizing the privacy department through more streamlined dashboards for privacy impact assessments, for example, and communicating and managing the work of the privacy office. The old days of spreadsheets and Word documents are simply not up to the demands of the modern digital ecosystem.

New to the survey this year is the DSAR/individual rights management category. Nearly one in five respondents (18%) plans to purchase DSAR technology in the next year. This falls in line with the natural progression of enterprise privacy compliance. First, locate personal data, then map the flow of that data, create a framework to manage, and assess privacy compliance, then be prepared to respond to your users. Other global privacy regulations are beginning to adopt some of the GDPR's DSAR provisions, which perhaps places more future value on DSAR solutions. Like consent management, data subject access requests can be difficult to operationalize, but as more vendors jump into this space, perhaps increased adoption will continue.

The old days of spreadsheets and Word documents are simply not up to the demands of the modern digital ecosystem.

Research methodology

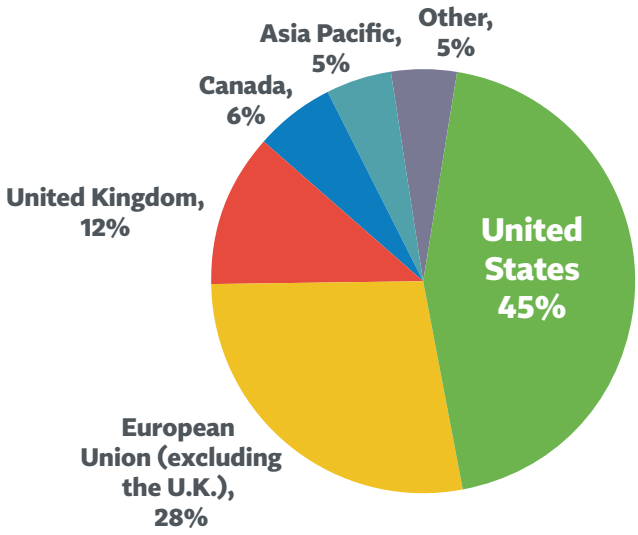
In March 2019, the IAPP fielded a 16-question survey to subscribers of the IAPP Daily Dashboard newsletter. The survey, which was in the field for approximately three weeks, took six minutes on average to complete. We receive complete responses from 345 privacy professionals. Although the survey primarily targeted in-house privacy, tech and legal professionals, we invited outside counsel and consultants to weigh in on whether they assist in privacy-tech-purchasing decisions on their clients' behalf.



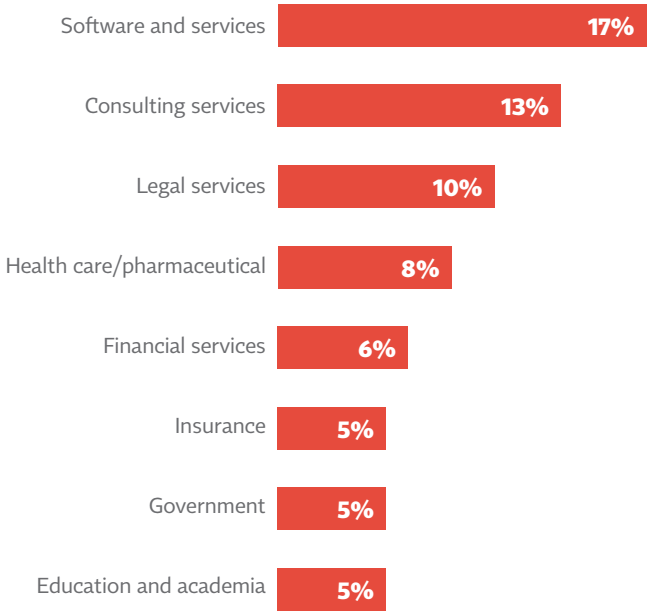
Respondent demographics

The IAPP Daily Dashboard subscribers hail from all over the globe. It's not surprising then that our survey reflects the global nature of IAPP membership. Among all respondents (i.e., in-house counsel, outside counsel, and consultants), 45% works for an organization headquartered in the United States, 28% for an EU organization, and about 12% in the U.K. The other regions were represented by Canada (6%), the Asia-Pacific region (5%), non-EU Europe (2%), Latin America (2%), and Africa and the Middle East (about 1%).

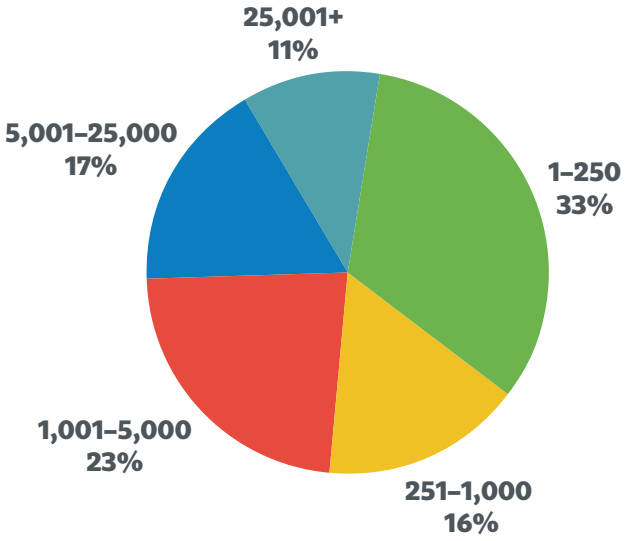
The software and services industry yielded the most responses at 17%, followed by consulting services (13%) and legal services (10%). Health care and pharmaceutical (8%) and financial services (6%) rounded out the top five. Thus, more than half of survey respondents worked within one of these five industries. Insurance (5%), government (5%), and education and academia (5%) were the next most common industries that respondents worked in.



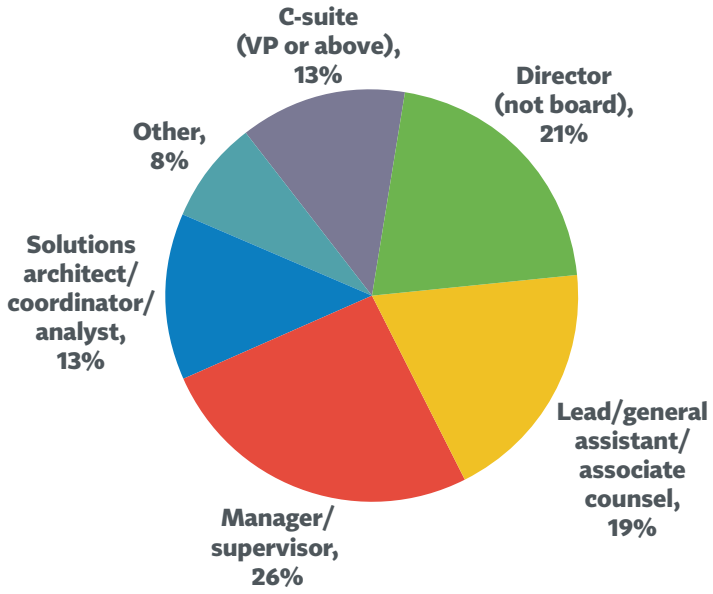
Regarding the size of their organization, the largest group of respondents (33%) is employed by very small organizations, or those with somewhere between 1 and 250 people.



The next largest group of respondents (23%) works for medium-sized organizations with anywhere between 1,001 and 5,000 employees globally. Roughly equal numbers of respondents work for small organizations (16%) and large organizations (17%), or those that employ between 251and 1,000 people and 5,001 and 25,000 people, respectively. Lastly, 11% of the sample works for very large organizations, which employ more than 25,000 people.

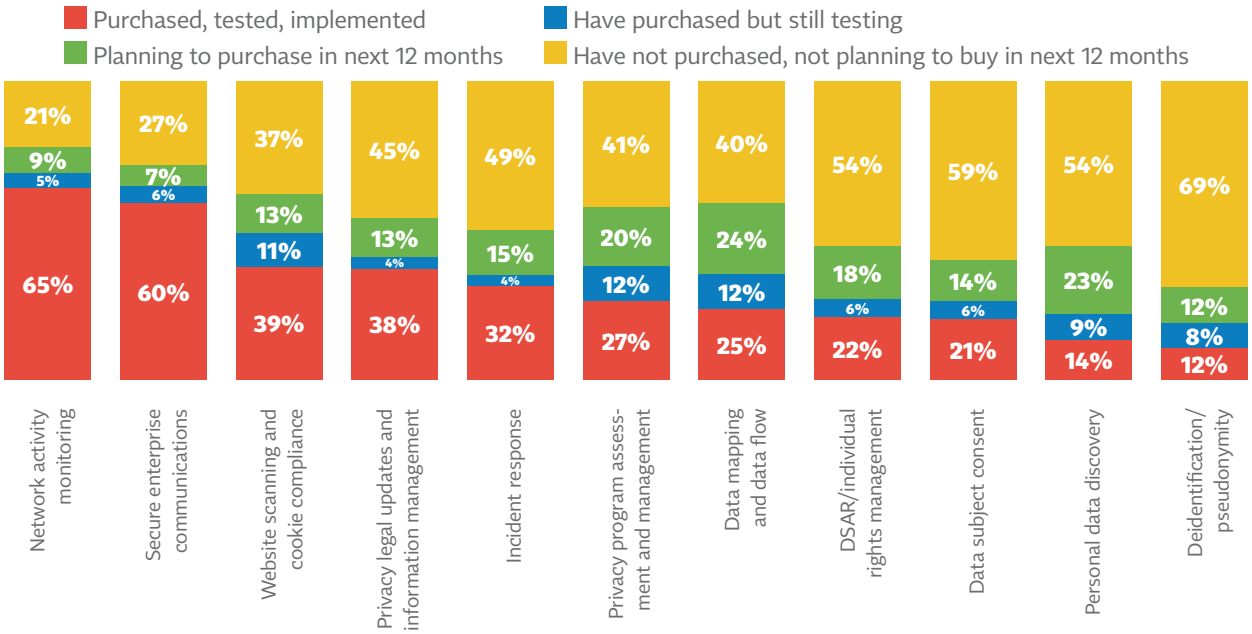


Finally, we asked respondents about their position within the organization they work for. Managers and supervisors represent the largest group (26%), while directors make up the second largest (21%). About one in five (19%) works as counsel, ranging from lead to assistant, while 13% holds a C-suite position at the vice president–level or above. The remaining 21% works either as a solutions architect, coordinator, analyst or in some other position.



Is the marketplace maturing?

This survey indicates that, yes, the marketplace continues to mature. It's clear that technology geared for the IT/infosec side is already established and integrated within



many organizations. However, it's also clear that technology for the privacy department continues to grow in demand. Compared to last year's survey, demand for privacy legal updates and information management solutions has grown by 5%, moving into fourth place.

Growing demand for privacy legal updates and information management tools reflects frantic pace of new privacy laws and proposed legislation

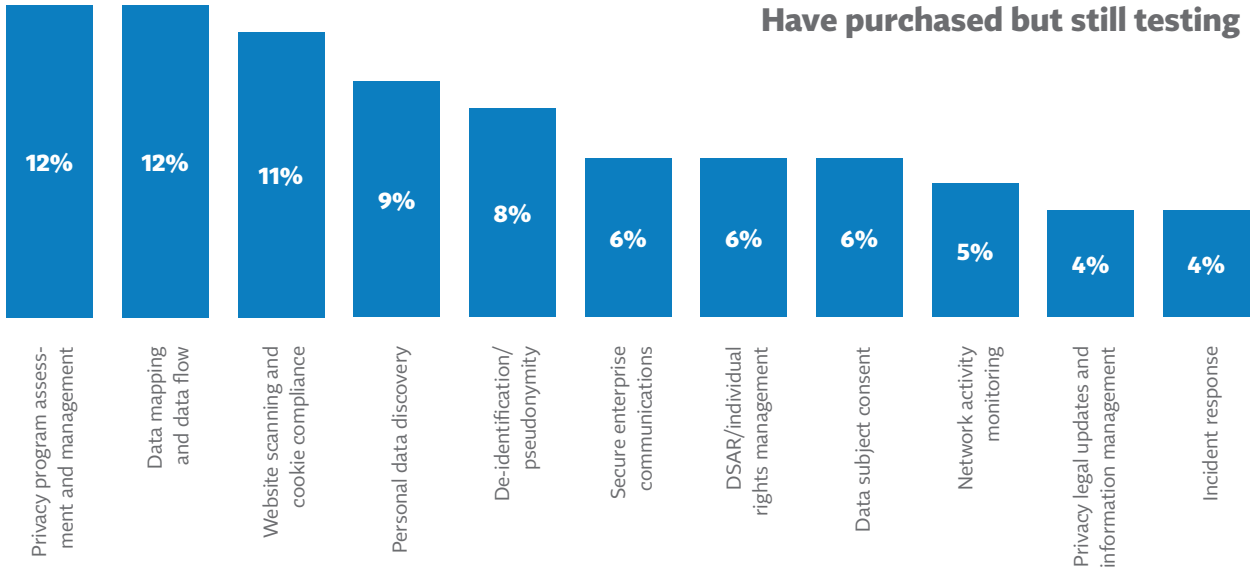
It makes sense that demand for privacy legal updates and information management tools has increased in the last year. During the course of the past 12 months, new privacy frameworks have popped up around the world, most notably in California with the CCPA. The advent of the CCPA has prompted other U.S. states to consider privacy laws, including a serious run from Washington state. Even the U.S. Congress is considering a federal privacy legislation. India has also drafted a comprehensive privacy bill, and Brazil has passed a national privacy law, just to name a few. Keeping track of all these new laws in order to benchmark regulatory compliance is a challenge this kind of technology can address.

It's also instructive to see which tools organizations have purchased but are still testing. For one, this suggests actionable insight into privacy tech priorities. At the top of the list reside privacy program assessment and management tools, as well as data-mapping and -flow technology. These are also top contenders for tools that respondents are planning to purchase in the next 12 months.

There is a clear need among privacy pros to assess and manage their privacy programs through technological solutions while also mapping data flows. It is no surprise then that it is the privacy/data protection department that is the most common decision maker for acquiring these tools. Perhaps even more importantly, it is the privacy/data protection department that is most often in control of the budget for such acquisitions.

Another common product that has been purchased in the last 12 months is website-scanning and cookie-compliance tools. Though the privacy and IT departments are tied for the most common decision makers for acquiring this tool, it's also worth noting that the marketing and legal departments often have a say here, as well. The only other category that marketing appeared to have

Have purchased but still testing



notable decision-making control over is data subject consent tools, which makes sense since website user tracking and consent are tied so closely to marketing initiatives.

Year over year, there is a slight downward trend in the purchasing of three privacy tech tools. This year, 7% fewer respondents said they have purchased or have plans to purchase incident response tools compared to last year, 8% fewer have purchased or have plans to purchase personal data discovery tools, and 11% fewer respondents have purchased or are planning to purchase deidentification/pseudonymity tools this year compared to last year.

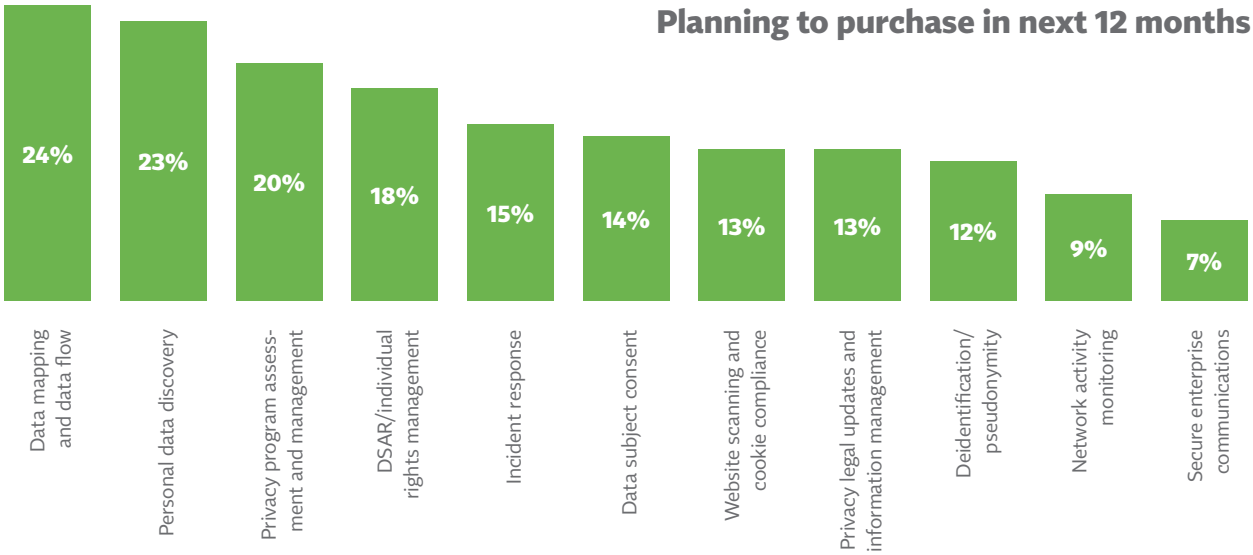
It's not readily apparent why there is a downward trend here other than perhaps other tools are being prioritized over these tools. Though, deidentification/pseudonymity tools appear to be the most niche and specific technological solution out of the 11 categories. That said, personal data discovery and deidentificaiton/pseudonymity tools are the fourth and fifth most-purchased tools in the past year, respectively.

The tools least likely to be in the testing stage, according to this survey, are incident response (4%), privacy legal updates and information management (4%) and network activity monitoring (5%). The latter is not surprising since it has already been established that such tools are part of a more mature IT/infosec marketplace that pre-dates the privacy tech marketplace. Privacy legal update and information management tools were newly introduced in the IAPP Privacy Tech Vendor Report in 2018, so perhaps we can chalk this up to lack of privacy need or awareness of product availability in the marketplace. As more vendors step into this space, and as market awareness grows, there could be an uptick in this product category.

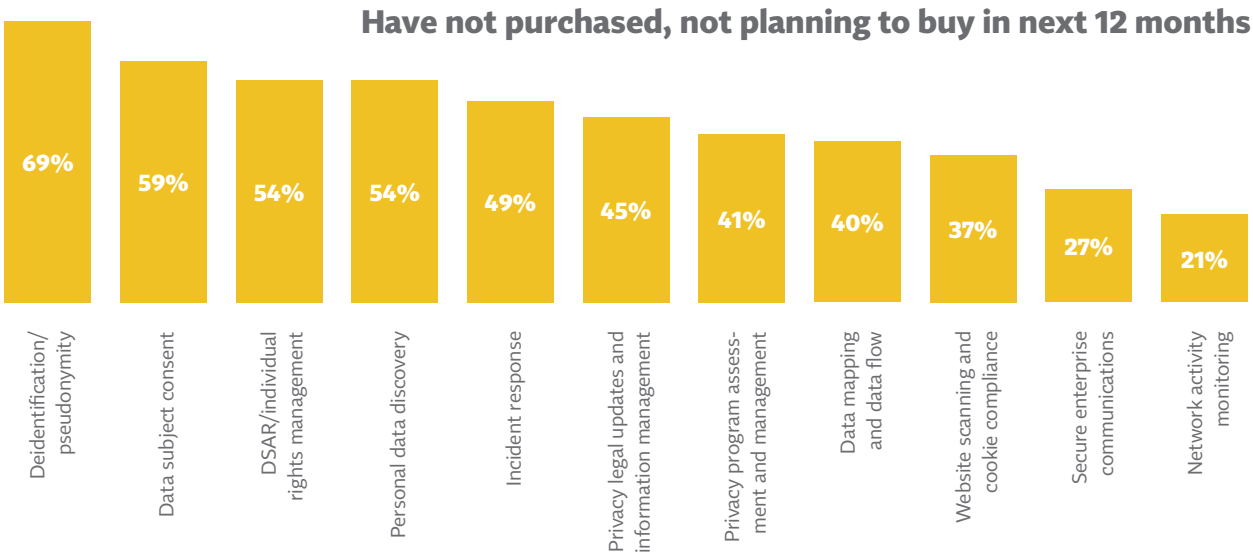
True, while only 4% of organizations have purchased and are testing incident response tools, according to this year's survey, it's not all doom and gloom for this product category, since 15% of respondents said they plan to purchase this technology in the next 12 months, placing it fifth among product categories in this question domain. Data breach response and notification obligations are an area this is not going away. In the U.S. alone, there are 50 different state data breach laws, not to mention the GDPR's 72-hour notification obligation.

At the top of the list for products respondents will least likely purchase in the next 12 months is deidentification/pseudonymity tools. As mentioned above, it may well be the case that

Planning to purchase in next 12 months



so far this product is too niche for the broader marketplace. Next in line is data subject consent tools. Nearly 60% of respondents have no plans to purchase this technology in the next year. As we suspected last year, it may still be easier to handle consent requests in-house, either through custom tools or by more traditional means.



Assessing market maturity by region

Unsurprisingly, respondents to this survey largely reflect IAPP membership in terms of regional location.

We found some directional trends in terms of purchasing and privacy tool adoption among regions. Notably, this survey found that while 75% of U.S.-based organizations have purchased Secure enterprise communications tools, only 56% of EU/U.K.-based organizations have made a similar purchase. Interestingly, there appears to be more hunger in the EU for planned purchases of this category than in the U.S. To wit, 6% of U.S.-based companies plan to purchase secure enterprise communications tools, while 9% of EU/U.K.-based organizations plan to do the same. Does this indicate that there was less market penetration in the EU until last year? Did U.S.-centric events, like the Sony Pictures Entertainment leaks of corporate emails, lead to greater awareness of this need by region?

Another interesting nugget worth digesting is planned purchase of data-mapping and data-flow tools. Desire for these solutions appears to be higher in the U.S., with 29% planning to purchase in the next 12 months, while only 16% of EU/U.K.-based organizations said they would purchase in the next year. Could this be an indicator that GDPR preparations have leveled out in the EU, while the CCPA is leading to a higher adoption rate?

The same could be interpreted on planned purchases of personal data discovery tools. According to this year's data, 29% of U.S.-based organizations plan to make the purchase, while 22% plan to do the same in the EU/U.K.

Finally, network activity monitoring tools appear to be in higher demand in the EU/U.K. than in the U.S. Though overall the planned adoption rate is low, 11% of EU/U.K. organizations and 7% of U.S. organizations plan to purchase these enterprise-wide, security-based tools. As was mentioned in last year's report, this may indicate that cybersecurity technology may be a bit more

Percentage that have purchased the tool, by region

	U.S.	EU/U.K.	Other
Network activity monitoring	75%	63%	68%
Secure enterprise communications	**74%**	**56%**	68%
Website scanning and cookie compliance	55%	46%	46%
Privacy legal updates and information management	44%	40%	43%
Incident response	38%	31%	46%
Privacy program assessment and management	29%	38%	39%
Data mapping and data flow	36%	37%	36%
DSAR/individual rights management	25%	27%	39%
Data subject consent	24%	27%	32%
Personal data discovery	24%	17%	36%
Deidentification/pseudonymity	16%	25%	18%

entrenched in the U.S. than in the EU due to longstanding breach notification laws and health care regulations in America.

Barriers and motivators to privacy technology adoption

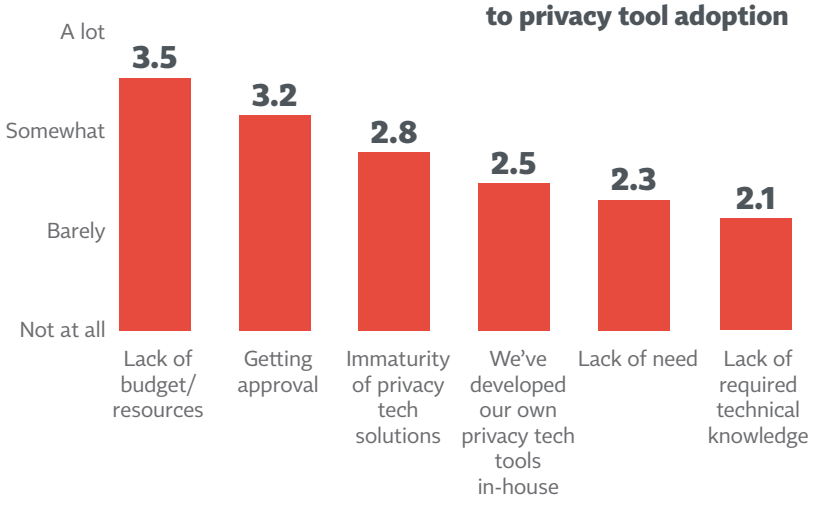
A longstanding issue for privacy departments around the world has always been the lack of budget and resources. Over the years, privacy pros have had to make do with the little they have. Though major regulations, like the GDPR, have certainly gained the attention of CEOs and executive leadership, respondents indicate that lack of budget and resources is the number-one barrier to privacy tech adoption.

Interestingly, however, there is no one major barrier to adoption. In this survey, respondents were asked to rate the question on a five-point semantic scale, ranging from "not at all," "barely," "somewhat," "a lot," to "major" barrier and motivator.

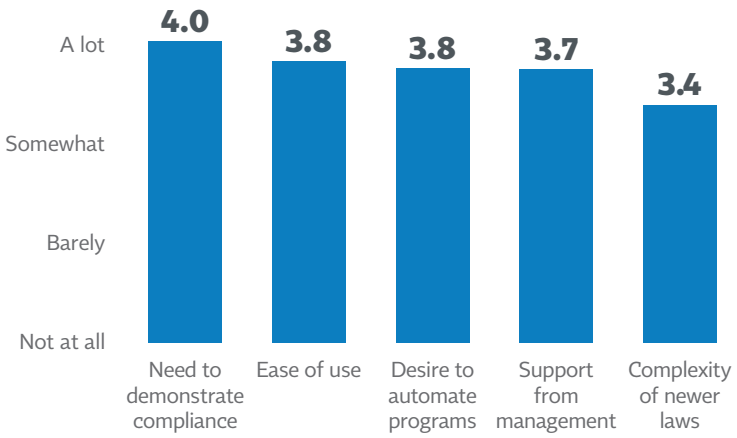
Lack of budget leads the way, but that is at a 3.5 rating, placing it equally between "somewhat" and "a lot." True, "a lot" is nothing to scoff at when considering barriers to tech adoption, especially when a privacy pro is trying to implement solutions, but it may be seen as a good sign that there is no "major" level barriers to adoption overall.

That said, lack of budget remains the single most common barrier to adoption. According to the data, 85% of respondents report this is at least "somewhat" of a barrier. Privacy pros and vendors alike will have to continue to come up with creative ways of convincing the purse holders that tech adoption is a necessary investment.

Lack of budget/resources and getting approval were rated as the largest barriers to privacy tool adoption



The need to demonstrate compliance was rated as the biggest motivator to acquiring privacy tools



Tied to lack of budget and resources is getting approval to make purchasing decisions. This is the second highest barrier at 3.2, closer to the "somewhat" semantic point. For a majority of the product categories included in this survey, it is the privacy/data protection department that is most frequently involved in the decision-making process, although there are also other teams (including legal, compliance, IT, marketing and infosec). Approximately 73% of respondents said getting approval is a barrier to adoption.

It may be noted that one year removed from the GDPR, there have yet to be many significant enforcement actions for noncompliance. If enforcement activity in the EU ramps up, this may help get the ear of the C-suite to increase budgetary spend for privacy tech adoption.

Another barrier for adoption directly involves the vendors. A majority of respondents indicate that the immaturity of privacy tech solutions and the in-house development of privacy tools indeed are obstacles. A total of 63% of those surveyed said this is at least somewhat of a barrier, while 52% said the same thing about their own in-house solutions.

These two data points suggest just how nascent the privacy tech marketplace remains. Many of these solutions were simply not around or needed just five or ten years ago. The growth of vendors captured in the first two versions of the IAPP Privacy Tech Vendor Report alone demonstrates the sheer number of new tech startups in the space. When the initial report came out in the first quarter of 2017, there were approximately 50 vendors. By the fourth quarter of 2018, the report catalogued nearly 200 vendors overall. And that does not include many of the big security companies; governance, risk and compliance organizations; and auditing firms that have been in the security, risk and compliance space for some time.

The number of companies in the IAPP's Privacy Tech Vendor Report grew from 50 to 200 in under two years.

That means there are a lot of new and fresh companies out there rapidly building tech solutions. But privacy and data protection are not easy tasks to automate or solve through technology. As tech vendors update, tweak and improve their products and services, this number will likely go down.

Similarly, with a lack of budget, privacy departments have had to be creative with their solutions. In a 2018 IAPP report with TrustArc, for example, we found 45% of respondents still used manual/informal processes for data inventory and mapping, while only 20% used commercially available mapping tools. It appears in-house technology is still a barrier to third-party tech adoption, which could be tied to lack of budget overall.

On the flip side, 92% of those surveyed said a motivator for tech adoption stems from the need to demonstrate compliance. Without a doubt, companies doing business in the EU need to demonstrate compliance via records of processing and other means. The CCPA will also help motivate more companies to demonstrate compliance, particularly in the U.S.

Another takeaway for privacy tech vendors is ease of use. That is the second highest motivator for tech adoption. Approximately 90% said this is at least somewhat of a motivator. Companies have different business models and often have a varying degree of legacy systems. Implementing new technology can often be difficult. Plus, if a technology is difficult to use, it will be less likely employees will use the technology successfully.

Third among the biggest motivators is the desire to automate programs within a company. At least 87% of respondents identified this as at least somewhat of a motivator. Automation often helps with scalability, which leads to efficiency and perhaps increased budget.

It is worth noting that the complexity of newer privacy laws is not the biggest motivator for tech adoption. Only 75% reports this as somewhat of a motivator.

Who is deciding to make the purchases?

This year's survey also asked respondents to identify the teams within their organization that are involved in the decision to acquire and use third-party privacy tech tools. Notably, the privacy and data protection teams are most frequently involved in the decision-making process. This is closely followed by the IT and infosec teams, not surprising since many privacy tech tools affect the IT architecture of a company, and it's often the case that these teams have a bigger budget from which to work.

As we suspected last year, and which continues through this new survey, the IT team is the most frequently involved player in the purchase of enterprise-wide tools, like secure enterprise communications tools, network activity monitoring tools, and website-monitoring and cookie-compliance

Who has input in purchasing privacy technology?

	IT	Infosec	Privacy/ Data protection	Legal	Compliance	Marketing	Other	Don't know
Network monitoring	32%	31%	16%	8%	9%	1%	2%	1%
Secure communications	34%	29%	16%	7%	8%	1%	3%	1%
Cookie tools	26%	16%	26%	10%	9%	9%	3%	2%
Privacy legal updates	7%	9%	36%	26%	16%	1%	3%	1%
Incident response	20%	23%	24%	14%	13%	1%	3%	1%
Privacy program assessment	11%	13%	37%	19%	14%	1%	4%	1%
Data mapping	18%	17%	31%	13%	13%	2%	5%	1%
DSARs	14%	13%	31%	18%	13%	3%	6%	1%
Data subject consent	14%	11%	27%	18%	14%	10%	5%	1%
Personal data discovery	23%	21%	28%	12%	12%	0%	2%	1%
De-identification	25%	18%	26%	9%	13%	1%	4%	3%

tools. It had already been established that these third-party offerings that have a hand in security are part of a more mature market that directly affects the IT team.

Interestingly, the legal team most often gets involved when it comes to the acquisition of privacy legal updates and information management tools, privacy program assessment and management tools, and DSAR/individual rights management tools. This is consistent with other research that many privacy departments report up through the legal department.

In parallel, the compliance team also has a hand in purchasing decisions involving privacy legal updates and information management tools, as well as privacy program assessment and management solutions. However, compliance is also involved in the acquisition of data subject consent tools.

This year's survey also asked respondents to identify the teams within their organization that are involved in the decision to acquire and use third-party privacy tech tools. Notably, the privacy and data protection teams are most frequently involved in the decision-making process.

Privacy and data protection teams are most likely to be involved in the purchasing of privacy program assessment and management tools, privacy legal updates and information management tools, as well as data-mapping and data-flow tools. All three categories are deeply tied to the day-to-day functions of the privacy office. The former tool above is literally designed for the functioning of the privacy department. This list also indicates the need for privacy departments to be abreast of changing privacy law and to have a comprehensive view of how personal data is collected, stored and shared throughout the organization.

The marketing team also has a role to play in the privacy tech ecosystem. They most often get involved when it comes to the purchase of data subject consent tools, website-scanning and cookie-compliance tools, as well as DSAR/individual rights management tools. All three categories are deeply intertwined with marketing initiatives, especially since consent and cookie compliance directly affect marketing initiatives and tracking for targeted advertising and personalization.

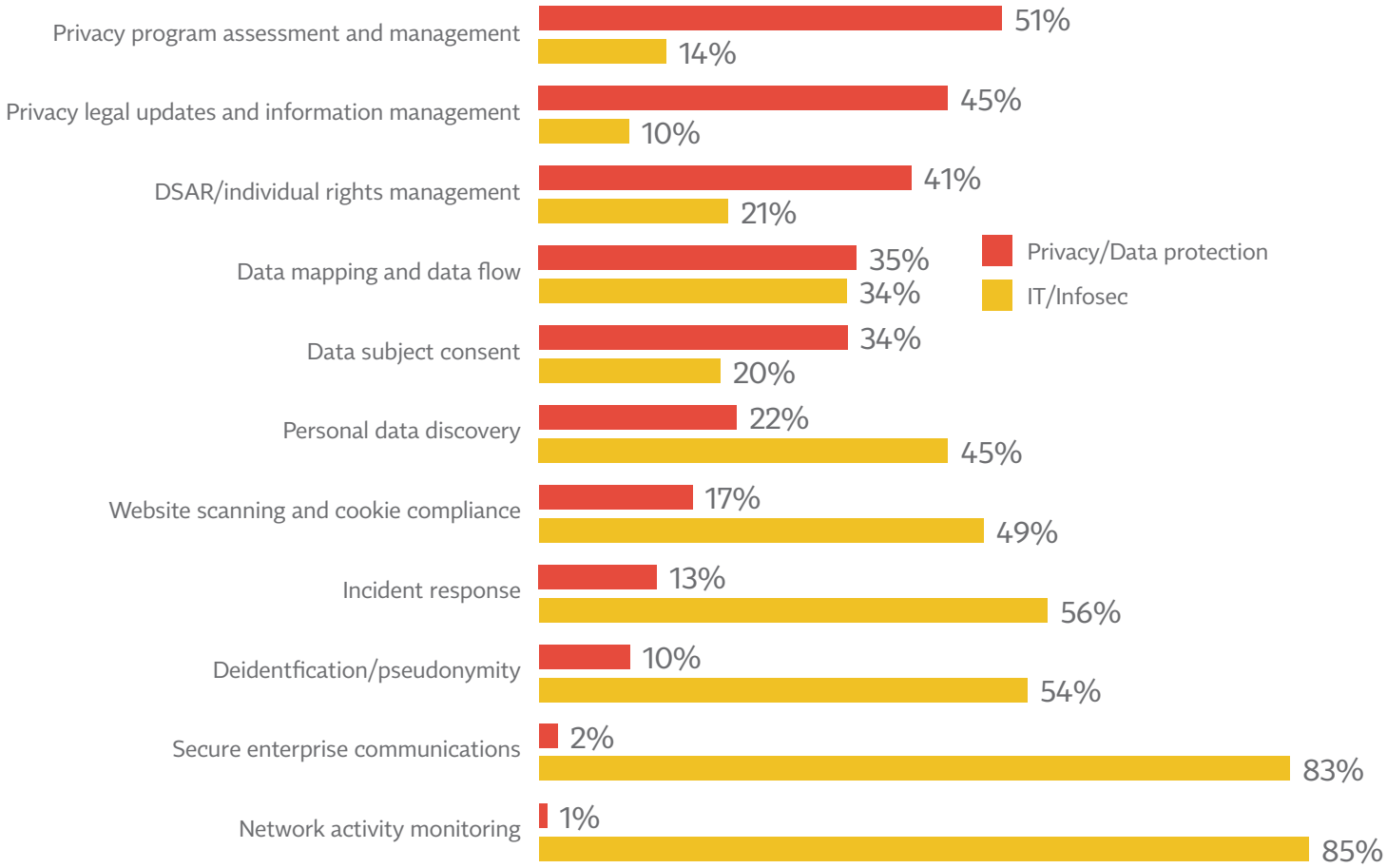
Who has the budget?

Though it is the privacy and data protection department that is most involved in a decision to purchase a third-party solution, it is the IT team's budget that tends to be used most often. This is most readily apparent for the purchase of secure enterprise communications, network activity monitoring, and, interestingly, deidentification/pseudonymity tools. The first two tools obviously affect the overall IT ecosystem and enterprise architecture, but the latter tool, though most heavily a privacy-protective tool, clearly requires an IT lift. Perhaps this is why it is least likely to be purchased in the next year.

The information security teams generally have the budget for purchasing incident response, network activity monitoring, and personal data discovery tools. These are in line with the IAPP Privacy Tech Vendor Report's observation in 2017 that such solutions fall on the enterprise privacy management side of things, which ultimately requires buy-in from the infosec team. Though personal data discovery tools can help the privacy department immensely, the technology often involves a form of artificial intelligence that goes through a companies' databases, a clear information security concern.

Similar to purchase decisions, it's the budget of the legal team that often pays for purchases of privacy legal updates and information management tools, privacy program assessment and management tools, data-

Where budget for purchase resides



Who will use the tools once purchased?

	IT	Infosec	Privacy/ Data protection	Legal	Compliance	Marketing	Other	Don't know
Network monitoring	38%	36%	11%	3%	6%	2%	3%	2%
Secure communications	26%	23%	14%	9%	11%	7%	10%	1%
Cookie tools	25%	15%	25%	5%	7%	17%	5%	1%
Privacy legal updates	7%	7%	36%	26%	16%	2%	4%	2%
Incident response	18%	22%	23%	14%	13%	2%	6%	2%
Privacy program assessment	8%	11%	37%	17%	16%	3%	6%	2%
Data mapping	18%	17%	31%	9%	12%	3%	8%	1%
DSARs	13%	7%	34%	16%	16%	4%	9%	2%
Data subject consent	10%	8%	29%	15%	13%	17%	7%	2%
Personal data discovery	21%	19%	31%	10%	11%	2%	5%	2%
De-identification	24%	17%	26%	4%	7%	3%	15%	3%

mapping and data-flow tools, as well as data subject consent tools. These are all solutions deeply engrained with privacy needs. This also indicates that many privacy departments likely report up through the legal department.

The compliance team most often uses its budget for privacy legal updates and information management, privacy program assessment and management, and incident response or data-mapping and data-flow tools. Since these are all primarily concerns related to the privacy department, this may also indicate some privacy teams report up through compliance.

The privacy and data protection teams, however, are most frequently drawn upon to purchase privacy program assessment and management tools, DSAR/individual rights management tools, and privacy legal updates and information management tools. The GDPR is obviously a big driver in the need for DSAR solutions, and clearly the privacy teams are actively getting budget for this growing solution.

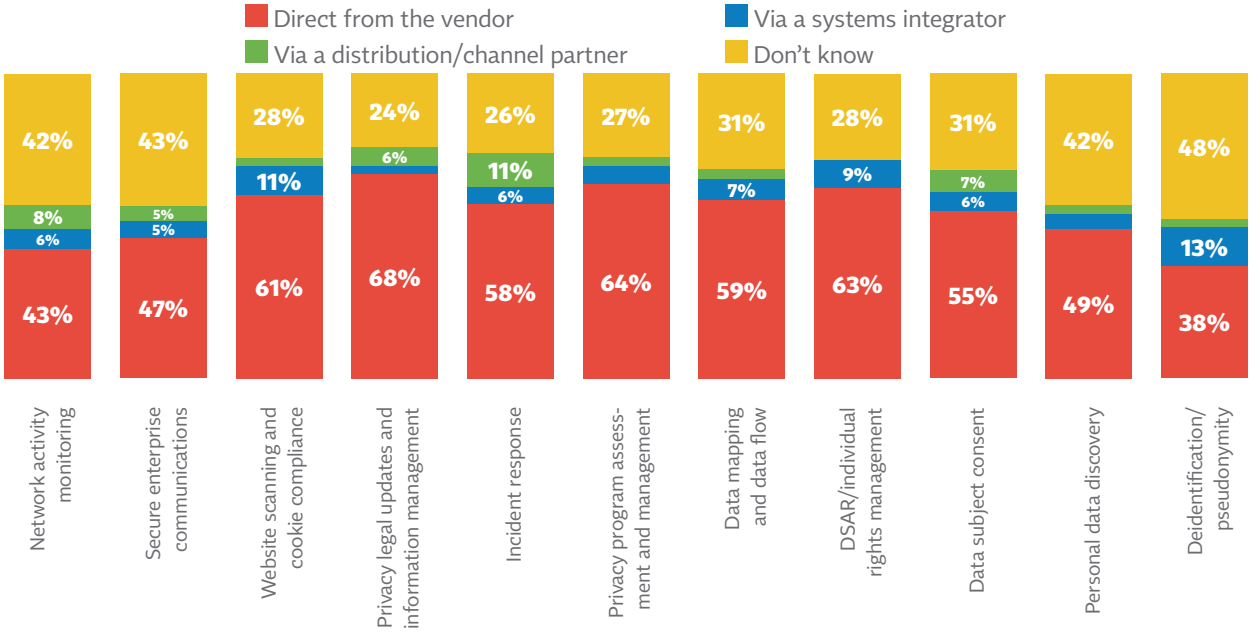
Predictably, the marketing team often has budget for website scanning and cookie compliance, as well as data subject consent tools. As stated above, these are tied to marketing initiatives. It is worth noting, however, that marketing also indicates it has the budget for deidentification/pseudonymity tools. There appears to be hunger for solutions that allow marketing to extract useful business intelligence while minimizing risk to data subjects.

From whom are organizations buying these tools?

As was outlined in last year's report, one way of assessing the maturity of a given market is to trace the path to market that products take. As a general rule, the more a market matures, the further away a consumer gets from the manufacturer.

For enterprise software, the path to market can take different forms, the most obvious of which is for the vendor to directly sell to the consumer. However, another path often results in the establishment of "value-added resellers" "channel partners" or "systems integrators." These companies resell the software from the manufacturers but offer added services for installation, maintenance, perhaps customization and other support. There are also tech distributors that resell

From whom will/did your company acquire this tool?



software from a variety of vendors, like a one-stop-shop of sorts.

To help assess potential market maturity, we asked respondents from whom they acquire their technology. Like last year, on the whole, the answer is "directly from the vendors," suggesting the market still has a way to go before reaching maturity. At the top of the list are tools for privacy legal updates and information management, privacy program assessment and management, and DSAR/individual rights management.

One interesting nugget to note, however, is that a large group of respondents does not know from whom they bought or will buy products, in particular when it comes to deidentification tools, secure enterprise management tools, and network activity monitoring tools. At first glance, this is unsurprising since it is likely these were purchased by the IT or infosec team, perhaps even before a privacy department was established.

Outside counsel and consultants slim but relevant market

Our survey asked outside counsel and consultants a single question about privacy tech purchases. Data breach remains a major motivation for engaging outside counsel and consultants. In terms of using technology to support these services — for themselves and their clients — outside counsel and consultants are mostly likely to be involved with secure enterprise communications, network activity monitoring, and incident response.

Also high on the list, however, are privacy legal updates and information management programs, which 43% has already purchased (either implemented or still testing), and which 11% plans to purchase in the next year. These is also a growing potential market for privacy program assessment and management — 16% of outside counsel and consultants surveyed are planning to purchase these tools in the next year.

	Have not purchased, not planning to buy in next 12 months	Purchased, tested, implemented	Have purchased but still testing	Planning to purchase in next 12 months
Secure enterprise communications	45%	48%	3%	4%
Incident response	47%	32%	15%	7%
Privacy legal updates and information management	47%	32%	11%	11%
Website scanning and cookie compliance	53%	31%	9%	8%
Data mapping and data flow	55%	31%	8%	7%
Privacy program assessment and management	48%	28%	8%	16%
Network activity monitoring	57%	33%	3%	7%
Data subject consent	53%	27%	9%	11%
DSAR/individual rights management	65%	20%	9%	5%
Personal data discovery	69%	20%	5%	5%
Deidentification/pseudonymity	72%	15%	5%	8%

What does it all mean?

Like last year, this survey demonstrates that enterprise-wide tools, like secure network monitoring or secure enterprise communications, for example, are well entrenched in many organizations. Products that respondents said they were most likely to purchase in the next 12 months are data mapping and data flow, personal data discovery, and privacy program assessment and management, indicating that privacy management tools are growing in demand. These top-three categories are deeply engrained with the privacy and data protection departments, though, it's often IT or legal that is making the purchases. It's also worth noting that DSAR/individual rights management, though a new category, came in fourth in this list.

With enforcement activity likely to ramp up in the EU and with laws like the CCPA set to go into effect at the beginning of 2020, the need for such solutions will continue to grow.