HOW PRIVACY TECH IS BOUGHT AND DEPLOYED

NEW RESEARCH FROM THE IAPP AND TRUSTARC PROVIDES A STATE OF PLAY FOR NEW SOLUTIONS ADDRESSING NEW PRIVACY AND DATA PROTECTION CHALLENGES

iapp | TrustArc

EXECUTIVE SUMMARY

In May 2018, IAPP and TrustArc surveyed 328 privacy professionals around the globe and asked them a series of questions about each of 10 categories of privacy technology, as identified in the IAPP's annual Privacy Tech Vendor Report. The results provide illuminating benchmarking data about what technology is truly in use vs. what technology is still far from mainstream. Further, it's clear that certain technologies are truly the domain of the privacy office, while other tech that might be vital to a contemporary privacy program is generally handled by and operated out of the infosec or IT departments.

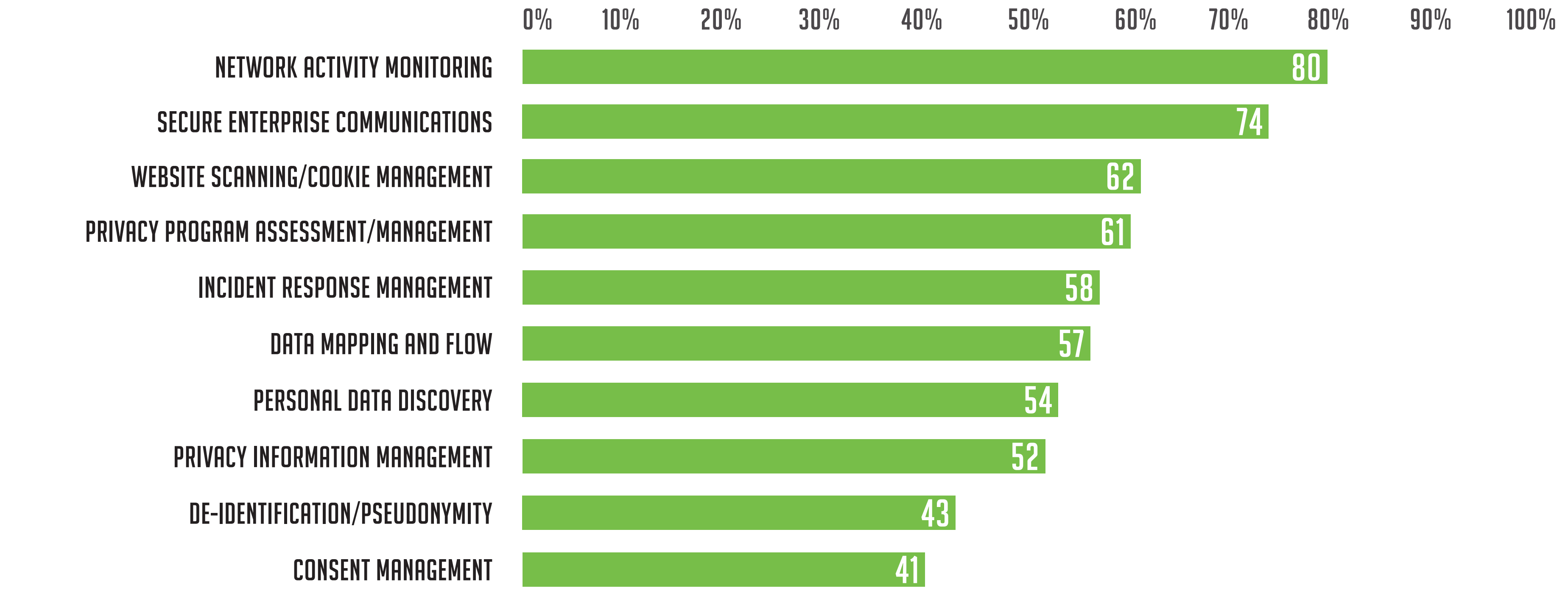
The survey produced a great deal of data, as disclosed in the full report, but the highlights include:

- Those technologies with security applications and general enterprise use are clearly more mature and in-use than newer, privacy-office-specific technologies, but the data shows a clear wave of uptake coming.

- The most likely new technologies to be adopted by privacy offices are Data Mapping and Flow, Personal Data Discovery, and Privacy Program Assessment/Management technologies, all of which are in the plans for future purchase by roughly a quarter of companies.

- Budget is the largest reported barrier to adoption, but larger firms, where budget is less of an issue, are not developing solutions in house, and are directionally less likely to say either lack of demonstrated need or immaturity of the technology are barriers. Essentially, if they've got budget, they're in the market. But the largest firms, those with 25,000 or more employees, are not the largest adopters of privacy technology. Rather, it is those with 5,000 to 25,000 employees.

ORGANIZATIONS THAT HAVE PURCHASED OR ARE PLANNING TO PURCHASE:



EXECUTIVE SUMMARY

- Of the 10 categories of technology, Consent Management tools are the least adopted by the market, and are not coming on strong. There is an indication that the market doesn’t find Consent Management as difficult or important as conventional wisdom would have you believe. Almost 60 percent of companies have no plans to invest in Consent Management tools.

> *“The most likely new technologies to be adopted by privacy offices are Data Mapping and Flow, Personal Data Discovery, and Privacy Program Assessment/ Management technologies [...]”*

- De-identification tools are also relatively niche, the second least likely to be adopted and not particularly on people’s radar. Only 42 percent of companies have purchased or plan to purchase this type of technology.

- U.S. firms are more likely to have already operationalized Enterprise Privacy Management solutions, which are more likely to have security and other enterprise applications. EU/U.K. firms are more likely to have already invested in Privacy Program Management technologies, which are designed more specifically for the “privacy team.”

- Larger companies are more likely to have privacy teams with budgets for technology, where smaller companies are more likely to have IT or infosec budgets that privacy must influence.

- While some technologies are clearly the province of the infosec or IT teams in terms of budget authority, privacy has influence over purchasing the majority of the time for eight of the 10 categories of technology, and is involved nearly 40 percent of the time for both Networking Activity Monitoring and Secure Communications Technology.

- While it may not be mainstream yet, there is clearly some momentum for consultants and law firms to use technology to help serve their clients and solid indication that this practice will grow in the near future.

IN THIS FIRST-EVER BENCHMARKING OF ADOPTION OF PRIVACY TECH, WE NOW HAVE A BASELINE FOR FUTURE CHARTING OF MARKET GROWTH.

iapp | TrustArc

INTRODUCTION

TECHNOLOGY IS CHANGING THE WAY WE MANAGE PRIVACY

Privacy and data protection have challenged organizations for decades. While, historically, most companies addressed these challenges primarily through a combination of legal and consulting services, many organizations' increasing reliance on data to drive business, the influx of new technologies into the workplace, and regulatory requirements to demonstrate ongoing compliance have necessitated technology solutions to efficiently manage and operationalize privacy.

While the market began to see some privacy-dedicated solutions for monitoring website trackers and managing cookie consent because of ePrivacy Directive mandates in the European Union in 2002, many companies have continued to rely on manual processes and ad hoc tools to manage their programs.

Recently however, and largely thanks to the complexity of complying with the EU's brand-new General Data Protection Regulation, we have started to see the adoption of technology tools progress with the introduction of solutions that automate privacy assessments and data mapping. To help companies navigate the influx of solutions, the IAPP created the Privacy Tech Vendor Report in 2017. Since the initial release 18 months ago, the report has grown to encompass 10 product categories and more than 150 companies.

We were still left, though, with little insight into who was using these solutions.

To dig into this question, the IAPP and TrustArc joined forces to conduct in-depth research into the actual deployment of technology today, and the plans organizations have laid for the future. We surveyed more than 300 privacy professionals from around the globe and asked them a series of questions about what they've bought, who had the budget, and, perhaps more interestingly, who had influence over the decision-making. We continue to see privacy, IT, and infosec teams working hand-in-hand in trying to tackle the many difficult challenges presented by privacy, data protection, and security.

In addition to providing extensive information on current use and future plans to help companies benchmark versus the industry, the research also provides a baseline by which we can measure changes over time in order to monitor progress in the industry. Which of these technologies will come into maturity? Which may find themselves mired in obscurity?

We hope you will find the report informative and helpful.

Chris Babel, CEO, TrustArc

J. Trevor Hughes, CIPP, CEO, IAPP

HOW PRIVACY TECH IS BOUGHT AND DEPLOYED

NEW RESEARCH FROM THE IAPP AND TRUSTARC PROVIDES A STATE OF PLAY FOR NEW SOLUTIONS ADDRESSING NEW PRIVACY AND DATA PROTECTION CHALLENGES

Though privacy and data protection have been operational challenges for organizations going back to the late 1960s, a combination of legal reforms and technological advancement has made the task of operationalizing privacy and data protection greatly more complicated in recent years. Particularly, the app and gig economies, combined with the advent of the European Union's General Data Protection Regulation, has led to a reality for many organizations where they must account for how personal data is entering the organization, how it is being used, what permissions are attached to it, and who has responsibility for managing it.

Seeing this need, a flood of new technology vendors have created a new privacy technology marketplace, which the IAPP first documented in January 2017 with the inaugural Privacy Tech Vendor Report, identifying nine broad categories of vendors and populating those categories with fewer than 50 companies from around the globe. In just 18 months, the number of categories has grown to 10 and the IAPP has identified an additional 100-plus vendors, making clear the rapid growth of the burgeoning industry.

PRODUCT CATEGORY DESCRIPTIONS

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 AND FLOWS 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 AND COOKIE COMPLIANCE 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.

ENTERPRISE PRIVACY MANAGEMENT

SOLUTIONS DESIGNED TO SERVICE THE NEEDS OF THE PRIVACY OFFICE ALONGSIDE THE OVERALL BUSINESS NEEDS OF AN ORGANIZATION

NETWORK 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.

SECURE ENTERPRISE COMMUNICATIONS ARE SOLUTIONS THAT HELP ORGANIZATIONS COMMUNICATE INTERNALLY IN A SECURE WAY IN ORDER TO AVOID EMBARRASSING OR DANGEROUS LEAKS OF EMPLOYEE COMMUNICATIONS.

However, any number of questions remained unanswered: Which categories of technology are more mature and in use than others? Whose budget is being used to acquire these products? Who in the organization is actively using these solutions? Are traditional vendors to privacy offices, like consultants and external counsel, using these technologies on behalf of their clients?

To this end, the IAPP and TrustArc surveyed more than 300 privacy professionals around the globe and asked them a series of questions about each category of privacy technology. The results provide illuminating benchmarking data about what technology is truly in use vs. what technology is still far from mainstream. Further, it's clear that certain technologies are truly the domain of the privacy office, while other tech that might be vital to a contemporary privacy program is generally handled by and operated out of the infosec or IT departments.

For example, more than two-thirds of organizations are already employing Networking Activity Monitoring technologies to understand how personal data is traveling throughout the organization, yet just 1 percent of organizations use the privacy budget to purchase a solution.

On the other hand, fewer than one in five organizations have operationalized Consent Management solutions, but it was in privacy's budget 31 percent of the time, more than any other department.

It may not be surprising that privacy's budget is most often used for Privacy Program Assessment software and Privacy Information Management systems, bought by privacy 49 and 43 percent of the time, but perhaps it's not intuitive that privacy budget is only used for De-identification solutions 10 percent of the time, and only 9 percent of privacy teams use their budget for Website Scanning and Cookie Compliance solutions. Rather, 70 percent of organizations place the de-identification buy in either IT or infosec, and 66 percent of organizations use those teams' budgets to pay for cookie compliance.

This underscores the nature of privacy professionals as influencers in their organizations who must work efficiently to articulate their needs and requirements to the IT and infosec teams so as to acquire tools to better accomplish their goals. Privacy professionals must, then, work to understand the software-buying process, how to undertake requirements exercises, and how to communicate effectively in terms that technologists commonly use and understand.

> “ ***“[...] fewer than one in five organizations have operationalized Consent Management solutions, but it was in privacy's budget 31 percent of the time, more than any other department.”***

Indeed, while Network Monitoring might not be in privacy's budget, the privacy team is involved in the buying decision 37 percent of the time.

In the course of this report, we examine the data regarding which technologies organizations around the globe have taken on — and which they have no plans to take on — and explore the impacts of organization size and geographical location on their buying habits and technology use.

REPORT METHODOLOGY

The IAPP used, as it does with the majority of its surveys, the distribution list for the IAPP's Daily Dashboard newsletter, which covers the privacy industry daily and has roughly 37,000 subscribers hailing from around the globe. This list is opt-in, and is clearly read by those working in privacy and interested in privacy matters. The newsletter is free, and those who sign up for it in the IAPP Subscription Center are alerted that they will be sometimes asked to fill out a survey.

The survey was in the field from May 16 through June 4, 2018.

The survey first asked demographic questions to identify a respondent's basic geographic location in the world, the size of the organization for which they work, and the industry in which that organization is located. Then we asked them to identify the role they occupy in the industry:

- Attorney, working as outside counsel.
- Consultant, working as part of a consulting firm.
- In-house, in the private sector.
- In-house, in the public sector.

If they were outside counsel or consultant, we branched them to questions about how they use technology in their firms or to help clients.

If they were in-house, we asked them to identify themselves as:

- Privacy, legal department.
- Privacy, compliance department.
- Privacy, other department.
- Information technology.
- Information security.
- Other.

All of these we then branched into questions that asked how they would describe their organizations in terms of each of the 10 basic privacy technology categories identified in the most recent IAPP Privacy Tech Vendor Report:

- Not purchased.
- Planning to purchase in the future.
- Have purchased, but still testing.
- Purchased, tested, and implemented.

Then, if they selected one of the latter three options, we asked these people a series of further questions about that technology.

First, we asked who was involved in the decision to acquire the technology:

- The IT team.
- The Infosec team.
- The Privacy team.
- The in-house Legal team.
- External consultant.
- External counsel.

Then we asked whose budget was, or would be, used to acquire the technology:

- The IT team.
- The Infosec team.
- The Privacy team.
- The in-house Legal team.
- Some other business unit.
- Don't know.

REPORT METHODOLOGY

Next we asked a similar question about who would, or does, actually use the technology:

- The core privacy team.
- Privacy champions outside the core team.
- Other teams such as HR, Marketing, etc.
- External consultants on behalf of the privacy team.
- External counsel on behalf of the privacy team.

Finally, we asked from whom the privacy technology was actually acquired:

- Direct from the manufacturer.
- Via a systems integrator.
- Via a distributor or channel partner.
- Don't know.

Once those questions were completed, we asked the degree to which a selection of factors WERE "barriers" to acquiring privacy technology in general, not within any specific category:

- Lack of budget.
- Lack of demonstrated need for such tools.
- Low degree of technical skills on the privacy team.
- Inadequate internal resources for implementation.
- The need for approval from IT.
- The need for approval from Infosec.
- Ignorance of technology acquisition process.
- Immaturity of the market for privacy tech solutions.
- We've developed our own privacy tech in-house.

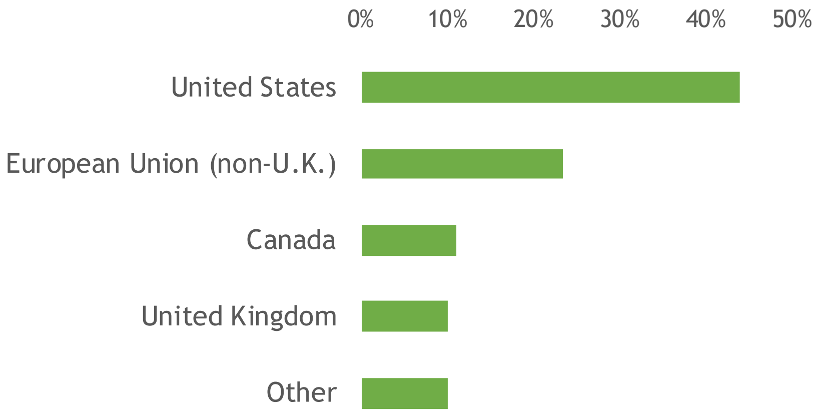
WE HAD A TOTAL OF 328 PEOPLE COMPLETE THE SURVEY, WHICH ASSURED ANONYMITY AND THAT NO ANSWERS WOULD BE ANALYZED OTHER THAN IN THE AGGREGATE. OF THOSE 328, A SUBSET OF 253 HAD INTERNAL ROLES AND COMPLETED THE MAJORITY OF THE SURVEY. ANOTHER 75 HAD EXTERNAL ROLES AND WERE ASKED WHICH OF THE TECHNOLOGIES THEY WERE USING ON BEHALF OF THEIR CLIENTS.

FROM THERE WE ANALYZED THE DATA FROM A VARIETY OF VIEWPOINTS, LOOKING FOR STATISTICALLY MEANINGFUL CORRELATIONS THAT MIGHT HELP ORGANIZATIONS WITH THEIR BENCHMARKING OPERATIONS.

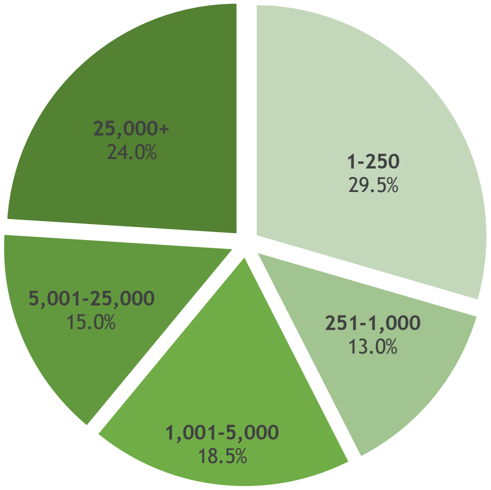
REPORT METHODOLOGY

RESPONDENT DEMOGRAPHICS

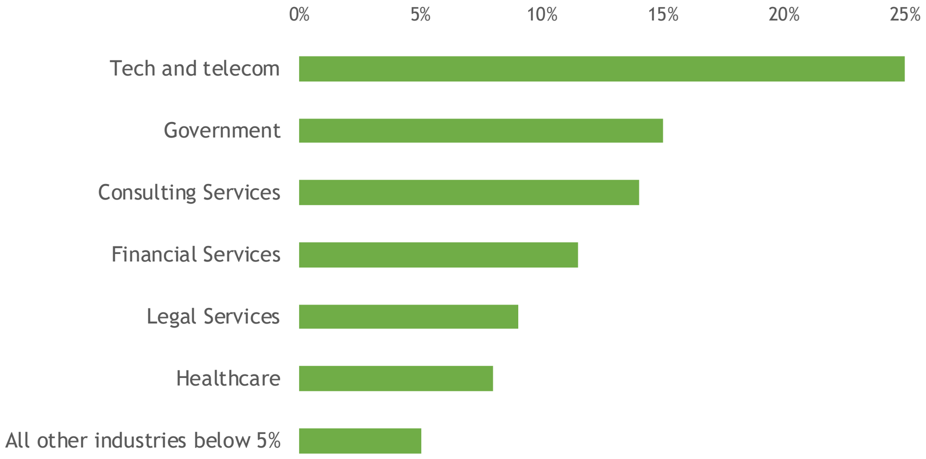
As is to be expected, the geographic constitution of the respondents largely mirrors the IAPP's membership:



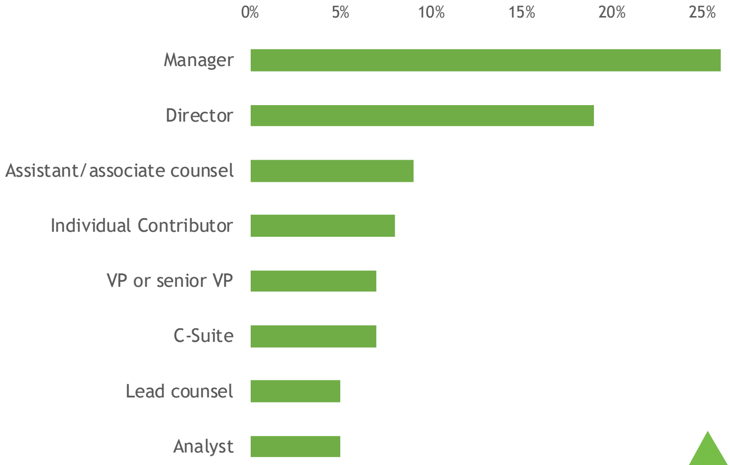
The respondents represent a relatively even distribution of company sizes, though with the largest percentage coming from the SMB sector:



And they come most prominently from the Technology, Government, Financial Services, and Consulting Services industries:



Finally, nearly half of respondents were at the manager or director (non-board) level in their organization, with a wide selection of other roles identified:



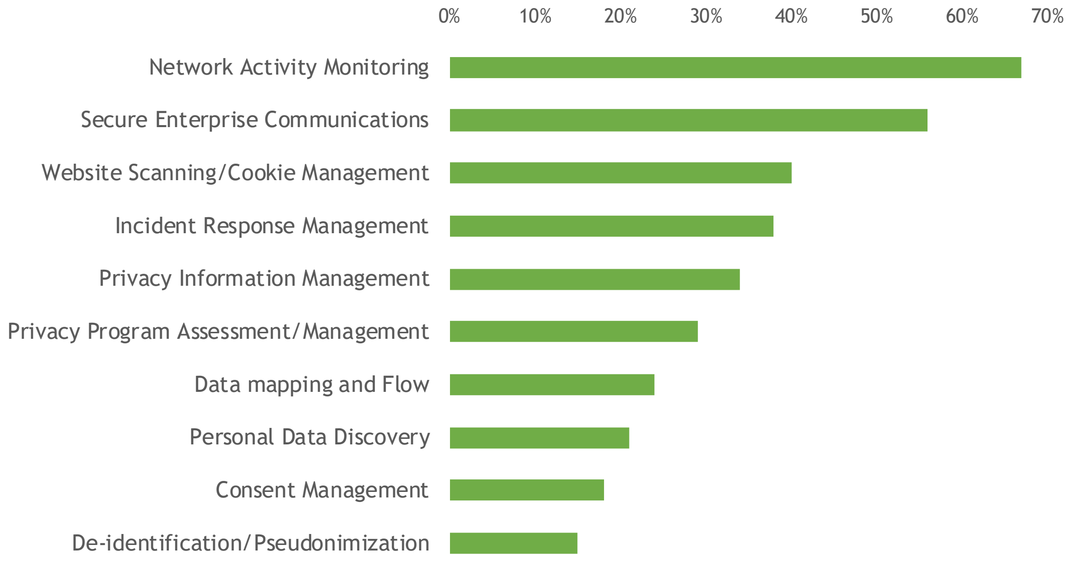
YOU'LL SEE IN FURTHER ANALYSIS HOW THESE FACTORS AFFECTED, OR DIDN'T, THE WAY TECHNOLOGY IS BOUGHT AND USED WITHIN ORGANIZATIONS.

JUST HOW MATURE ARE THESE MARKETS?

One way to assess the maturity of a marketplace is to judge how much of a market has been penetrated. While we don't have a way to assess whether these organizations truly need each of the 10 categories of identified privacy technology, we can at least show what percentage of organizations are actually already buying and implementing these various technologies. We also found some variation by geography and company size as factors in technology adoption.

First and foremost, of the 10 categories of privacy technology, Network Activity Monitoring technology is clearly the most in-use:

ORGANIZATIONS THAT HAVE PURCHASED AND IMPLEMENTED:



> *"Privacy Program Assessment and Management software has made significant headway, considering it was essentially unknown as a product as recently as five years ago."*

It's no secret that the infosecurity marketplace and its range of solutions is much more mature and robust than that for privacy technology. It should be no surprise then, that core security technologies that might also serve a privacy function are more frequently implemented, as is the case for many of what we call Enterprise Privacy Management solutions.

Network Activity Monitoring is something many security operations are likely to have on board, so they can understand traffic loads, watch out for DDoS attacks, and watch out for unauthorized access to certain organizational data.

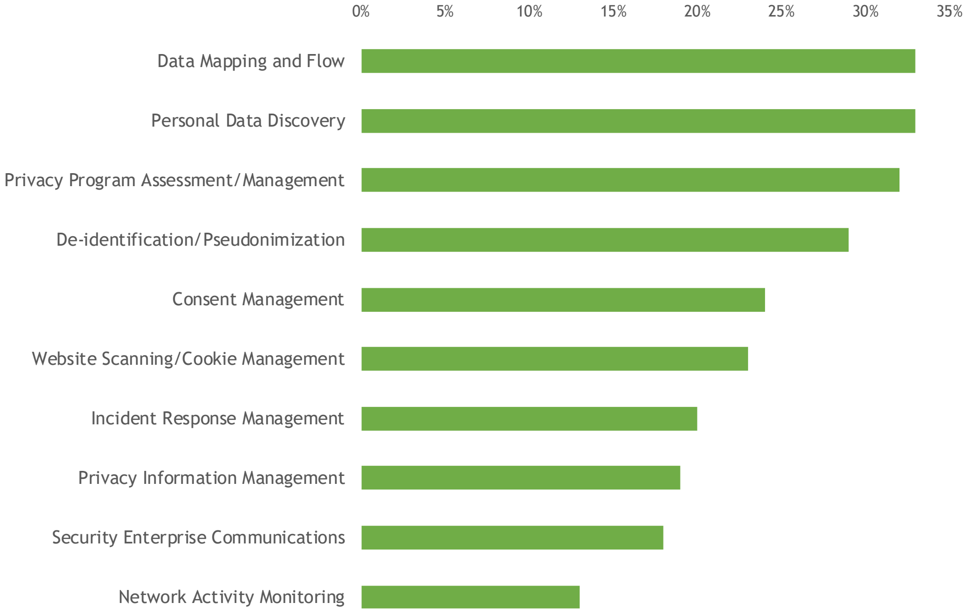
Similarly, it is now relatively standard practice for security teams to use some kind of Secure Enterprise Communications — such as enterprise solutions that are increasingly being developed to allow for encrypted business conversations, or even simple personal messaging apps — to correspond after a security incident that may have compromised the network, so as not to alert intruders that the team is aware of their presence.

What's perhaps more interesting to look at are those categories of technology that are relatively bespoke for the privacy team. Privacy Program Assessment and Management software has made significant headway, considering it was essentially unknown as a product as recently as five years ago. Even more indicative of Privacy Assessment/Management's nascent status is that yet another 32 percent of organizations are either planning to purchase this technology in the future or have already purchased it (11 percent) but have yet to implement.

JUST HOW MATURE ARE THESE MARKETS?

Similarly, both the Data Mapping and Flow and Personal Data Discovery categories have either already been purchased or are in the plans for another 33 percent of organizations, which shows how in-demand these solutions are as the GDPR and other laws require a deep knowledge of what personal information and organization holds, where it lives, and how it travels through an organization.

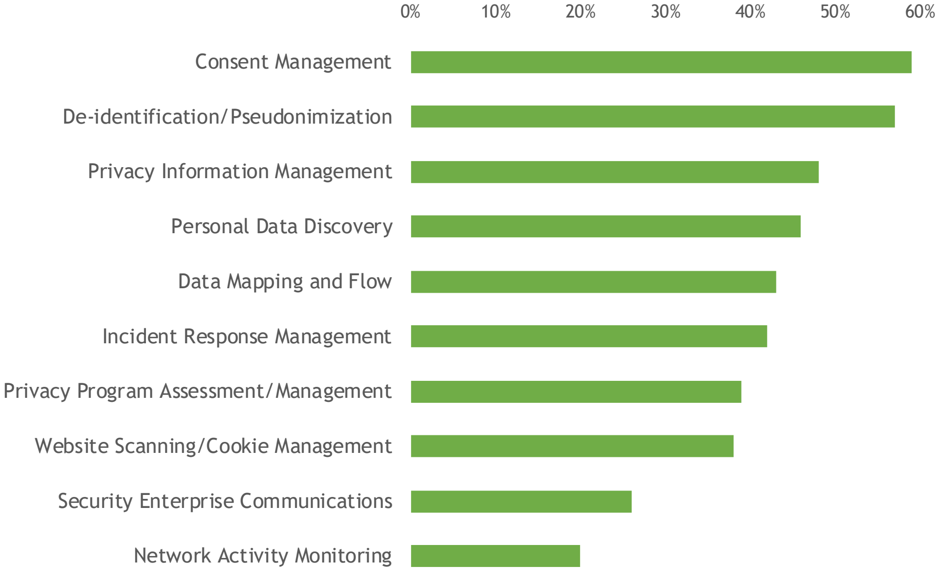
WHAT'S NEXT? ORGANIZATIONS THAT ARE PLANNING TO PURCHASE, OR HAVE PURCHASED BUT NOT IMPLEMENTED:



However, technology that manages what consent is attached to what data, Data Subject Consent Management, will likely not be purchased at all by 59 percent of companies. Is this evidence of the argument that way too much of the public discourse around privacy compliance is centered in consent, while organizations are instead relying on one of the other six bases for legal processing under the GDPR to process personal data? Is this proof that organizations feel their privacy statements are sufficient so that data subjects know what they're getting into when they provide personal information to organizations, and the granularity of consent tracking that some in the industry espouse is overkill?

We also see that 57 percent of organizations have no plans to invest in De-Identification/Pseudonymization solutions, which also speaks to the targeted nature of such solutions. It may be that only those organizations doing sophisticated research, or whose businesses rely heavily on data analytics, have any need for commercial solutions.

NICHE MARKETS? ORGANIZATIONS THAT HAVE NOT PURCHASED AND HAVE NO PLANS TO BUY:



MARKET MATURITY BY REGION

There are several areas where companies' level of engagement with privacy technologies appear to differ significantly between the U.S., Canada, and the EU/U.K. For example, more companies in the EU/U.K. have purchased technology for Data Subject Consent Management (32 percent) compared to companies in the U.S. (24 percent) and Canada (7 percent). This would indicate the GDPR has, indeed, put an emphasis on consent as a valid basis for processing personal data, while privacy law in Canada and the U.S. may be based on consent, but, without the GDPR's added requirement for consent to be easily revocable, there is less impetus for tracking consent metadata closely.

Similarly, EU companies also are slightly more engaged with Data Mapping and Flows tools (43 percent have purchased) than U.S. companies (35 percent) and Canadian companies (15 percent).

Meanwhile, companies in the U.S. report being more engaged with Network Activity Monitoring tools than companies in the EU, an indication that cybersecurity technology is more entrenched in the U.S., given the more longstanding breach notification and response culture that has been created by the patchwork of breach notification laws and HIPAA's established impact.

Amongst U.S. respondents, 76 percent have purchased these tools — and are either testing or have implemented them — versus only 62 percent of EU/U.K. respondents and 59 percent of Canadian respondents. Secure Enterprise Communications are another tool with which U.S. companies are more engaged (67 percent have purchased) than their EU/U.K. (58 percent) and Canadian (44 percent) counterparts. And U.S. companies are also more engaged with tools to handle Privacy Information Management (42 percent have purchased) than companies in Canada (33 percent) and the EU/U.K. (29 percent), which certainly makes sense given the U.S. sectorial approach to privacy and Canada's strong privacy laws at the province level.

This may also explain why U.S. companies seem more engaged with Personal Data Discovery technologies (35 percent have purchased) versus EU/U.K. companies (19 percent) and Canadian companies (11 percent). While these tools may seem bespoke for the privacy team, we see in our budget data that these are just as likely to be purchased by IT/Infosec as privacy, and they have clear security use.

Further, in the EU/U.K., 19 percent of respondents are planning to purchase Network Activity Monitoring technology, versus just 6 percent in the U.S., which paints a picture of an EU marketplace catching up with their U.S. counterparts, who have for longer been part of breach culture. Silicon Valley, after all, is a hotbed not just of consumer technology, but security technology as well.

However, we don't see statistical differences in the geographic purchase of Incident Response tools, which could be explained by the narrative that privacy offices have largely been using normal business tools for their operational work to this point and so the myriad breach laws in the U.S. haven't driven as much adoption. Just 38 percent of firms have invested in the first place and the privacy office has more budget here (28 percent) than with either Network Monitoring or Secure Communications, where privacy's involvement is minimal.

> *"Silicon Valley, after all, is a hotbed not just of consumer technology, but security technology as well."*

Regarding plans to purchase tool/technologies in the future, the biggest market appears to be technology for Personal Data Discovery, which 37 percent of EU/U.K. respondents indicated their company is planning to buy. There is also significant demand for Data Mapping and Flows tools in Canada and the EU/U.K, with about 33 percent of Canadian respondents and 29 percent of EU/U.K. respondents indicating that their company is planning to buy this technology in the future.

We otherwise don't see significant deviation in how organizations are planning to buy technology by geography.

HOW COMPANY SIZE AFFECTS TECHNOLOGY ACQUISITION AND USE

The big companies in our data set, those with more than 25,000 employees, are much more likely to be American: 56 percent of those largest firms are from the U.S., while only 35 percent of the smallest firms (under 250 employees) are American. U.S. firms were 44 percent of the sample overall.

Further, 15 percent of the smallest businesses were in the U.K., versus just 6 percent of the large firms, and 10 percent of the firms overall.

> *“There may be something to the idea that bigger companies are more complex, which complicates buy decisions.”*

In fact, it’s hard to separate the effects of size from the effects of geography. They correlate very closely.

For example: When we look at size and try to pull out how it impacts technology acquisition, one category, the 250-1000 employees bucket, is demonstrably the least likely to have purchased just about all of the technology types. Which is odd until you see that the companies in that bucket are disproportionately Canadian: 19 percent of them, versus just 11 percent overall. The Canadian responses are much more likely to say that budget is an impediment to purchasing and that they work for a government entity. These are more likely factors affecting purchasing behavior than company size.

As we tease out the effect of size, however, we do see some impact: Larger companies are more likely to have invested in enterprise communications, for example, with 76 and 65 percent of the top two bands having done so. It may be that larger and more complex organizations are more likely to see the value in a secure communications system in general, to help with Incident Response, but also to deal with other issues like protecting intellectual property and maintaining competitive advantages in the marketplace ahead of big releases.

We also see something interesting in the second to highest band, 5,000-25,000 employees, which is directionally more likely to have purchased both Consent Management tech (15 percent more likely) and Privacy Program Management software (11 percent more likely), while the even larger companies were not statistically more likely to do either.

This could simply be flukey, considering sample size. One theory might be that these biggest companies simply have the resources to build their own tech for the privacy office, but the numbers don’t bear that out: The numbers show no significant correlation with internal development as a barrier to acquisition by company size, though the smallest companies are the least likely to have built their own, directionally.

Further, the largest companies were significantly less likely to say they lacked internal resources, and significantly less likely to mention budget as an impediment, while small companies were definitely more budget conscious. So, it’s not a matter of privacy teams at the largest companies having a hard time being heard above the noise as they advocate for budget.

Another theory may be that the acquisition and approval process simply takes longer in the biggest organizations. However, we don’t see any difference in the numbers of different-sized companies planning to make buys in the future. However, there may be something to the idea that bigger companies are more complex, which complicates buy decisions.

One significant thing we notice in regard to size is that the two largest bands of companies are directionally more likely to have a privacy team with its own budget making the Privacy Program Assessment/Management buy, for example. In addition, while smaller companies generally make almost all privacy tech buys with either IT/infosec budget or privacy budget, these larger companies begin to bring in yet more budgets, including legal and other departments like HR and marketing.

Looking closer at the case of Privacy Program Assessment/Management, for example, the privacy team is the leading owner of budget for all company sizes. In the largest companies, however, the Legal department is much more likely to make the buy than in any other size grouping.

Similarly, for Consent Management software acquisition, which is an IT buy in the smaller companies, the privacy team emerges as most likely to have budget for the two largest size bands, and the largest companies even move the budget to marketing and other departments 29 percent of time. This is backed up by these largest organizations reporting that Consent Management is most likely to be used by non-privacy departments like marketing, by a margin of 11 percent over the sample as a whole.

Finally, it’s worth noting two things here specifically: First, for all categories of technology, about 10-15 percent of respondents were unsure whose budget was used. Second, while we can pull out a few of these interesting tidbits, it remains the case that size of company is not often a significant indicator of how privacy technology is bought and used.

WHO PAYS THE BILLS?

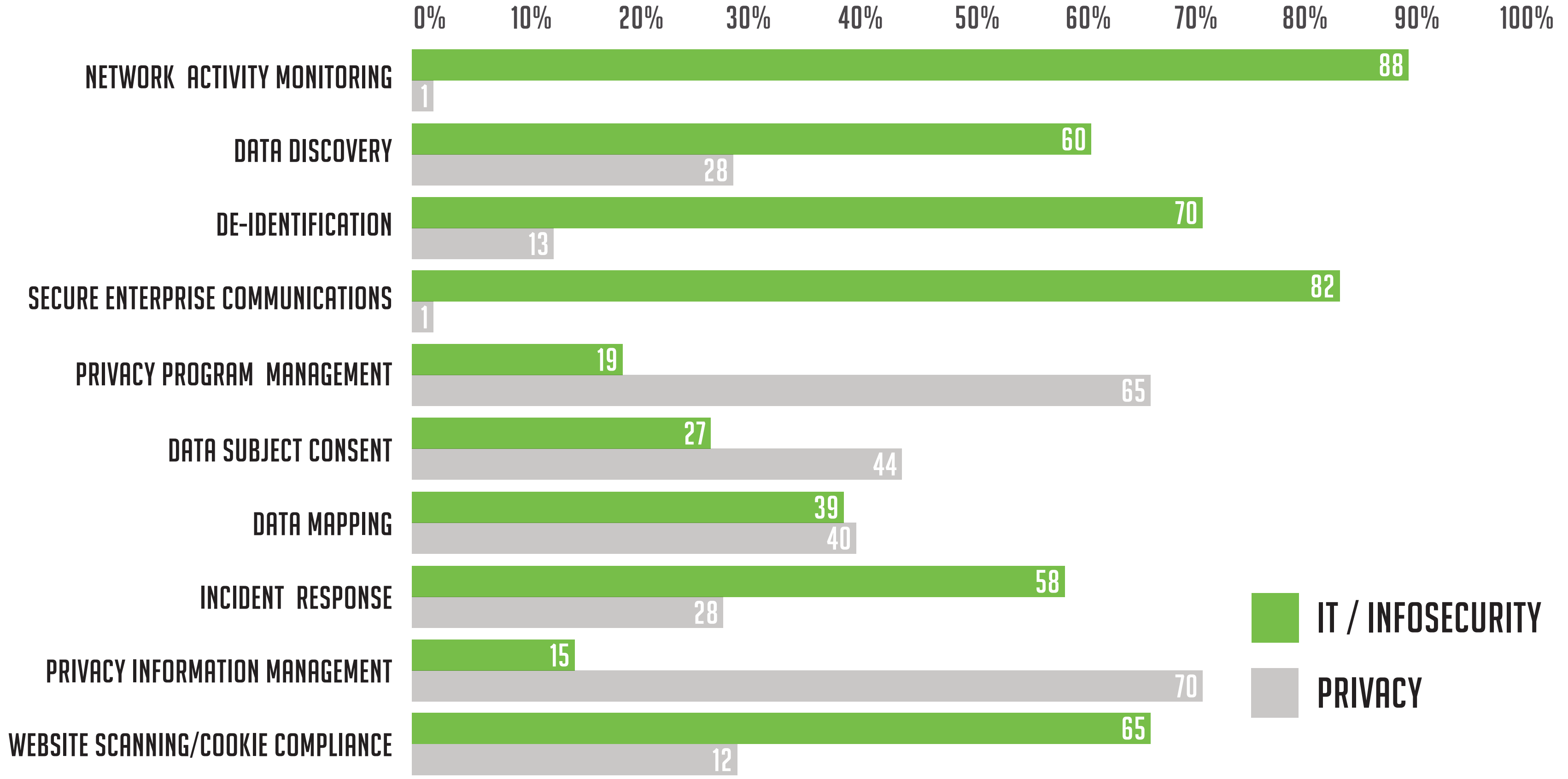
As you'll recall, in our Privacy Tech Vendor Report, the IAPP has posited that there are two big buckets in which you can put these technologies that are useful to the privacy team:

Privacy Program Management (or PPM): Solutions that are designed specifically for the privacy office. This includes Assessment Managers, Consent Managers, Data Mapping, Incident Response, Privacy Information Managers, and Website Scanners.

Enterprise Privacy Management (or EPM): Solutions designed to serve the needs of the organization as a whole, but which are also useful for privacy operations. This includes Network Activity Monitoring, Data Discovery, De-Identification Solutions, and Enterprise Communications. The theory, developed through significant interviews, was that the PPM category is largely researched and acquired by the privacy team itself. While the EPM category is generally the domain of IT or infosec.

Now, with this data, we have the first hard evidence to determine the legitimacy of those suppositions. The verdict: Not bad.

WHERE BUDGET FOR PURCHASE RESIDES:



WHO PAYS THE BILLS?

Where we really miscalculated in our initial bucketing is with the Incident Response and Website Scanning and Cookie Compliance solutions, which our data clearly says is in the IT and infosec budgets and not with privacy or legal.

While the Website Scanning results might make sense, where understanding what's happening on the website is inextricably linked to performance of the site in general and goes well beyond privacy, the Incident Response findings might run counter to some industry conventional wisdom.

The narrative in this case often runs that security is in charge of making sure breaches and other incidents don't happen, while privacy and legal are in charge of cleaning up the mess. Well, at least in terms of buying the software that helps manage the process of evaluating the nature of the incident and responding appropriately, our data would say IT and infosec still hold the purse strings, which means they also likely control the process, though the data is not as stark as in other categories.

However, for the rest, we largely nailed it, though Data Mapping can really go either way and will be something that's interesting to watch over time.

If there is any trend to be seen, it's largely that as the size of the company grows, the budget moves from IT and infosec into legal and privacy, and even beyond into places like marketing and HR.

We do not see significant regional differences in where budget resides, nor significant differences by industry.

WHERE THE BUDGET ISNT: THE U.S. GOVERNMENT

Clearly, lack of budget is a significant barrier to acquiring technology to help run a privacy program. If you don't have money, it's awful hard to buy things.

We know from both anecdotal evidence and our annual IAPP-EY Privacy Governance Report (where 67 percent of all respondents report insufficient budget for privacy operations) that most privacy offices report inadequate budget on some level, which is unsurprising in a field that remains relatively nascent, but it's interesting to create a profile of those organizations least likely to have budget for technology.

Are there any commonalities? Yes. While some organizations from every industry and geography report significant budget barriers, this phenomenon is particularly the domain of the public sector. Specifically, in the United States and Canada.

To answer this question, we looked at just those organizations that rated lack of budget 7 or higher when we asked them to rank the degree to which one of nine factors was a barrier to purchasing tech. Of the 88 organizations in that sample, we saw some clear patterns.

First, this is more likely to be an American phenomenon. While just 44 percent of our overall sample or respondents was based in the United States, 52 percent of firms with budget concerns were U.S. based, and most of that difference was made up by European firms. Just 23 percent of organizations ranking a lack of budget highly were EU/U.K. based, versus 34 percent overall.

The rest of the difference was made up by Canada, which repeatedly through the survey expressed less likelihood to be using technology and clearly is the least likely geographic sample of respondents to have sufficient budget.

Similarly, privacy professionals working in government make up 25 percent of the sample of those expressing budget woes, 10 percent higher than the base sample. Consulting firms, law firms, and financial services organizations are less likely than the base sample to cite budget concerns.

With the GDPR coming into force in the European Union, where every public agency must have a data protection officer and where privacy is a fundamental human right, it would seem that European officials have put their money behind their rhetoric: The EU and U.K. government entities in our sample are not crying poor.

Their counterparts in the U.S. and Canada, however, are having a harder time of it.

WHAT KIND OF INFLUENCE DOES PRIVACY HAVE?

Even where budget may not be available for privacy pros, they do have influence over the decision-making. Only a few categories of technology are relatively purely the domain of privacy, but many of the categories where we saw budgets in the hands of IT and infosec show that privacy has valuable input in which technology to acquire or whether to acquire it at all.

Remember how we said Incident Response and Website Scanning are largely the budget domains of IT and infosec? That belies the large input that privacy has in those buying decisions.

For Incident Response, 69 percent of respondents said privacy had input into the decision-making, even more so than the IT team, despite only 28 percent of privacy teams actually having budget authority. Similarly, 57 percent of privacy teams had influence over the Website Scanning and Cookie Management tools, though only 12 percent had the purchase made from their budget.

As we might expect, legal had the most say in the Information Management category, as laws are their domain, but second was Consent Management, which may be the least adopted because it is the nexus where there are the most cooks in the kitchen, with four different teams over 40 percent. Is that a sign consent is an area where there is confusion regarding who should manage the operational lift? Personal Data Discovery, another area where many have decried the lack of an off-the-shelf solution, is also an area where many teams are likely to be involved, with three separate teams over 60 percent.

Finally, it’s good to note that privacy teams do, indeed, have the most say over purchasing Privacy Program Assessment/ Management tech. However, with IT and infosec having little say there, is it possible the solutions won’t be well integrated with other enterprise infrastructure?

WHO HAD INPUT IN ACQUISITION

DEPARTMENT	PRIVACY CATEGORY									
	NETWORK MONITORING	PERSONAL DATA DISCOVERY	DE-ID	SECURE COMMS	PRIVACY PROGRAM ASSESSMENT	CONSENT MANAGEMENT	DATA MAPPING	INCIDENT RESPONSE	INFORMATION MANAGEMENT	COOKIE TOOLS
INFORMATION TECHNOLOGY	82%	63%	71%	82%	33%	44%	49%	54%	23%	76%
INFORMATION SECURITY	78%	62%	53%	76%	38%	43%	49%	75%	36%	64%
PRIVACY	37%	72%	71%	37%	86%	81%	78%	69%	81%	57%
LEGAL	19%	36%	27%	16%	39%	47%	20%	33%	57%	21%
CONSULTANT	11%	10%	11%	7%	9%	7%	9%	7%	8%	4%
OUTSIDE LEGAL	2%	8%	3%	0%	6%	5%	4%	6%	7%	1%

WHO'S USING THE TOOLS IN THE ENTERPRISE?

Regardless of whose budget is being used, or who has influence over the buy, an organization is clearly more likely to be happy with a purchase if it sees use throughout the enterprise. The more teams who get value out of the technology, the more likely those teams are to support its adoption.

All of these technologies reportedly offer at least some value outside of the core privacy team, and a few are used as much or more by privacy champions throughout the organization and other teams like marketing, HR, IT and others.

> *"All of these technologies reportedly offer at least some value outside of the core privacy team."*

While De-identification tools, for example, may be something of a niche product, more than half of respondents said the technology would be used outside of those with privacy functions. Similarly, Network Activity Monitoring, Website Scanning and Secure Enterprise Communications would all be used more outside of the core privacy team than within.

On the flip side, as you might expect, Data Mapping, Data Discovery, Incident Response, and Consent Management are all most likely to be used by the core privacy team, but with clear value for privacy champions and other teams as well.

Privacy Program Assessment and Privacy Information Management tools are really the domain of the privacy team, with less than 40 percent reporting anyone outside the core privacy team would use those pieces of technology.

WHO WILL USE THE TOOLS ONCE PURCHASED?

DEPARTMENT	PRIVACY CATEGORY									
	NETWORK MONITORING	PERSONAL DATA DISCOVERY	DE-ID	SECURE COMMS	PRIVACY PROGRAM ASSESSMENT	CONSENT MANAGEMENT	DATA MAPPING	INCIDENT RESPONSE	INFORMATION MANAGEMENT	COOKIE TOOLS
CORE PRIVACY TEAM	44%	74%	64%	44%	91%	71%	79%	77%	86%	58%
PRIVACY CHAMPIONS OUTSIDE CORE TEAM	28%	34%	51%	38%	34%	47%	47%	45%	38%	30%
OTHER INTERNAL TEAMS (E.G. MARKETING, HR, ETC.)	59%	41%	52%	68%	18%	41%	46%	47%	24%	60%
OUTSIDE CONSULTANTS ON OUR BEHALF	6%	3%	5%	5%	5%	3%	4%	3%	2%	1%
OUTSIDE LEGAL ON OUR BEHALF	0%	0%	0%	1%	3%	3%	1%	5%	1%	0%

WHO'S USING THE TOOLS IN THE ENTERPRISE?

BUT OUTSIDE COUNSEL AND CONSULTANTS MIGHT BE BUYERS THEMSELVES

We also in this survey looked at the hypothesis that organizations are buying technology and then granting operational access to outside counsel or consultants, so they can use the technology on behalf of their clients. The early returns say this really doesn't happen often.

No tool is used by even 10 percent of respondents' outside counsel or consultants.

However, we did find some evidence that consultants and law firms are buying these technologies themselves, in order to help with client service. We asked those who self-identified as outside counsel or consultants to identify their engagement with each of the 10 categories of tools in the same way we asked internal voices to do so. While no technology is owned and operated by a majority of firms, and most tools are not even being considered by a majority of firms, some tools are more popular than others.

The most popular technology, which makes sense, is Secure Communications, purchased and implemented already by 33 percent of the outside lawyers and consultants. Law firms, especially, need ways to communicate securely with clients. Another 23 percent are planning to make the purchase.
We also see some uptake in Network Activity Monitoring (28 percent) and Website Scanning (27 percent).

> *"While it may not be mainstream yet, there is clearly some momentum for consultants and law firms to use technology to help serve their clients"*

Those most on the planning board, however, include Privacy Information Management, which 29 percent of firms are planning to invest in, and Data Mapping and Flows, which is being eyed by 28 percent of firm respondents.

Least likely to be considered? Sixty-five percent said De-identification tools aren't in the plans, with only 5 percent investing so far, and 59 percent said they would not buy Personal Data Discovery tools, with only 15 percent having invested so far.

For all other tech, roughly a fifth to a quarter have purchased and another fifth to a quarter are planning on buying in the future. While it may not be mainstream yet, there is clearly some momentum for consultants and law firms to use technology to help serve their clients and solid indication that this practice will grow in the near future.

IF THEY'RE NOT USING IT AT ALL, WHY NOT?

In an attempt to understand what might be limiting the growth of the privacy technology sector, we asked respondents to evaluate various factors, on a scale of 1 to 10, that might act as barriers to adoption, as outlined in our methodology.

The primary answer, Lack of Budget, is hardly surprising. We've demonstrated that the Privacy Governance Report shows privacy teams often report a lack of adequate budget for the task presented to them. Further, the second most-common barrier, a lack of internal resources for implementation, is but another side of the same coin. Privacy teams don't have money and they're known to be generally new and small within organizations.

It's therefore also unlikely they have a deep well of IT resources, or project management resources, dedicated to them as of yet. Truly, the IT resources they do have were likely, at the moment of the survey, invested in tightening up compliance efforts and installing stop-gap measures to meet various GDPR obligation as the May 25, 2018, deadline for enforcement approached.

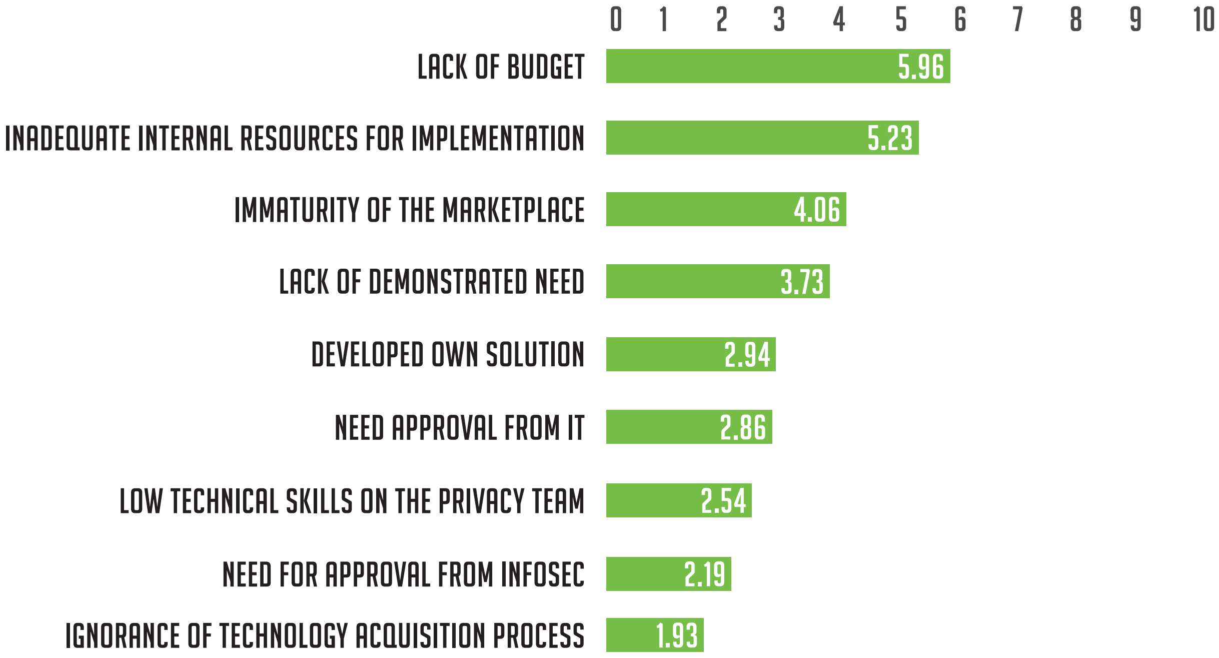
However, there is also clearly something of a wait-and-see attitude prevalent amongst privacy professionals. The third most common "barrier" to bringing privacy technology on board is a view that the market is still immature, which is followed directly by a lack of demonstrated need. It may very well be that many organizations without complicated data processing operations don't see a reason to go beyond successful operations that have been operated with common business tools like spreadsheets and word processing.

Further, the very next barrier is the fact that the organization has created its own internal solution using existing IT resources. As many of these technologies are similar to survey tools or technology used in security arenas, it may be that sophisticated IT teams with dedicated developers have simply created their own solution, or adapted something like Governance-Risk-Compliance software that's already owned by the organization to handle privacy compliance tasks as well.

The one thing we can say with some assurance is that privacy teams are unconcerned about the buying process. Maybe they have help from IT; maybe they're confident the vendors will educate them along the way.

It's also clear that they do, indeed, need that IT team's support, though that's not a significant barrier considering the overall scale.

WHAT FACTORS LIMIT GROWTH OF PRIVACY TECH?



WHO'S SELLING THESE SOLUTIONS?

One method for evaluating the maturity of a marketplace is to look at the path to market for products and the general sales channel. As a rule of thumb, as a market matures and commodifies, the consumer gets farther and farther away from the actual manufacturer of the product.

> *"[...] for every category of tech, about half of respondents purchased their technology directly from the manufacturer, about one third didn't know who sold them their tech [...]"*

In the enterprise software marketplace, this generally results in situations where the end user buys software through what are known as "value-added resellers" or "systems integrators." These companies re-sell software from major manufacturers, offering the added services of installation, maintenance, and general support to the enterprise with which they're working.

It is also sometimes the case that software gets resold by tech distributors that sell technology by many vendors, as a sort of central hub, but don't do any of the installation or maintenance and support.

Thus, we looked at the privacy technology marketplace to see where organizations were acquiring their tech to see just how far along some of these products are. The answer: Not all that far along.

In large part, for every category of tech, about half of respondents purchased their technology directly from the manufacturer, about one third didn't know who sold them their tech, and the small remaining portion purchased from a VAR or distributor.

Directionally, we saw that those more mature IT technologies like Network Activity Monitoring or Website Scanning, leaned slightly more toward a VAR/distributor, and the newer privacy-specific technologies leaned more toward the manufacturer itself.

In fact, Privacy Program Management software was the most likely to be purchased directly from the vendor, at 62 percent of all buys, speaking to its recent appearance on the marketplace.

However, it's fair to say that none of this technology is close to commodification or consolidation and there remains quite a bit of development to happen in this marketplace.

IAPP.ORG

TRUSTARC.COM