

2011

Privacy Professional's Role, Function and Salary Survey

International Association of Privacy Professionals



2011 Privacy Professional's Role, Function and Salary Survey

International Association of Privacy Professionals

|| *A Message from the Chairman*

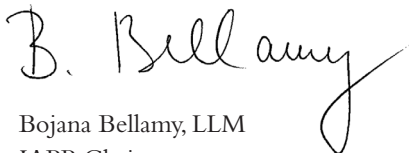
As the IAPP's new chairman, it is my great pleasure to bring you the 2011 IAPP Privacy Professional's Role, Function and Salary Survey.

This annual report is among the most valued member benefits that the IAPP provides. For the 2011 edition, we have significantly expanded both the breadth and depth of the survey questions. The result is a detailed profile of today's practitioner and the most comprehensive report on the profession ever published by the IAPP.

For the first time, we have divided the survey into sections that correspond to the major branches of our field. This allows us to provide you with new insights into the responsibilities, positioning, aspirations and earning power of your peers.

I trust that the information presented here will help you become an even more valued and productive member of the privacy community.

Sincerely,



Bojana Bellamy, LLM
IAPP Chairman
Director of Data Privacy
Accenture
London, UK

2011

Privacy Professional's

Role, Function and Salary Survey

|| Table of Contents

I. Executive Summary 4

II. Survey Findings 6

 Profile of the Privacy Profession 6

 Role 12

 Function 23

 Salary 35

 Privacy Specialties..... 42

 Privacy Concerns for 2011 58

III. Survey Methodology 60

 Objectives 60

 Questions 61

 Limitations 61

 Delivery and Sample 62

IV. Appendix: Survey Questions 63

I. Executive Summary

The International Association of Privacy Professionals (IAPP) administers an annual survey of its membership to understand the roles and functions of global privacy professionals. This study tracks compensation trends for individuals and the time allocation for their privacy tasks. It also explores how privacy professionals see their roles and responsibilities evolving in the near and distant future.

The 2011 Privacy Professional's Role, Function and Salary Survey was completed by the IAPP in coordination with Minnesota Privacy Consultants (MPC), a research and consulting firm that specializes in privacy operations and personal data governance for both corporate and governmental organizations. The IAPP developed and fielded the survey, and MPC provided analysis and reporting.

This is the most comprehensive and detailed study to date on the various segments of the privacy profession. Among the major findings of this year's report:

Role of the Privacy Professional

- Half of the responding privacy leaders report to the top executive or a direct report.
- Twenty-seven percent said their title was “chief privacy officer or official.”
- Roughly three-quarters of respondents are seeking convenient career-development opportunities in 2011, including Web conferences, local conferences and privacy-information services, while half are planning to travel for one privacy conference.

The Privacy Function

- The legal or compliance departments are home to 63 percent of privacy functions.
- Thirty-nine percent of privacy functions comprise two or fewer people, while 39 percent are teams of six or more.
- Forty percent of privacy functions have budgets of \$75,000 or less for outside privacy support, while 37 percent have \$250,000 or more.
- Ninety-seven percent said meeting regulatory compliance obligations was their privacy function's top business driver, followed by 80 percent who listed “avoiding having to make data breach notifications.”
- Almost two-thirds of respondents said their organization had not issued a security breach notice or suffered a privacy enforcement action in the past year, while three percent reported that either a breach or an enforcement action occurred to them more than 50 times last year.

Salaries

- The average privacy base salary has grown an impressive 12 percent since last year to \$123,971—the highest figure ever. With an average bonus just over \$18,000, the average total compensation for privacy pros topped out at \$142,117.
- The most highly compensating private-sector departments are those that typically employ attorneys and MBAs, with marketing (\$154,654), ethics and corporate responsibility (\$153,188), and legal (\$151,396) leading the pack.

- By department, the most highly compensated privacy pros work in government standalone privacy offices (\$105,630), IT (\$104,432) and risk management (\$103,600).
- By location of home office, those working for European-headquartered firms earned the most (\$133,026), followed by firms based in the U.S. (\$126,761) and Canada (\$94,698).
- By region, privacy pros based in the U.S. earned the top average salary (\$127,426), followed by those in Europe (\$114,947) and Canada (\$95,909).
- By sector, the highest-paying sectors for privacy pros are utilities (\$165,000), business services and supplies (\$160,777) and telecommunications (\$160,197).
- Two-thirds of respondents hold the Certified Information Privacy Professional (CIPP) credential, with an average base pay of \$120,029.

Specialties

- One-third of information technology (IT) privacy pros have the CIPP/IT credential, and their average salary of \$116,486 was roughly \$5,000 more than their non-CIPP/IT peers.
- IT privacy pros spend 57 percent of their time on privacy, and one-third of that time is dedicated to assisting with audits, assessments and gap remediation.
- The typical privacy advisor bills the equivalent of four days per week to clients, 55 percent of which is dedicated to privacy and billed at a rate of \$290 per hour.
- The top average bill rates of privacy advisors are in the business services & supplies (\$274) and banking (\$260) sectors, and the lowest rates are in the healthcare equipment and services (\$243) and government (\$224) sectors.
- Fourteen respondents classified themselves as vendors of privacy products. Compared to privacy advisors, privacy vendors were over 20 percentage points more prevalent in the education and academia and software and services sectors. They were less prevalent in the banking and telecommunications sectors.
- Seven respondents classified themselves as dedicated to researching, writing about or teaching privacy, and their top two areas of concern for 2011 are data disclosure to third parties and privacy and society.
- Of the eight survey respondents who classified themselves as privacy advocates, seven listed the security of personal data as their top agenda item for 2011.
- Fifteen respondents are responsible for enforcing privacy regulations in their jurisdictions, with the top priority for 2011 of limiting personal data uses and retention.
- The 40 respondents in the small-business category, in spite of their smaller size, shared the same top two concerns as their counterparts from larger organizations: complying with privacy regulations and avoiding data breaches.
- When asked about the state of privacy protection worldwide, there was broad consensus across all survey segments that there are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward more protection.

II. Survey Findings

This section presents the results of the survey. It is divided into five parts:

- Profile of the Privacy Profession
- Role
- Function
- Salary
- Specialties

Where possible, the findings are compared with identical elements from previous years' surveys.

Profile of the Privacy Profession

Industry Sector

Greater concentration of sectors. The largest number of respondents to the 2011 survey came from the financial services sector, which includes banking and insurance. This sector accounted for almost one-fourth of all responses. This continues the decade-long trend of financial services overtaking the healthcare sector as the top privacy employer. In last year's report, we noted that the decline of privacy practitioners in healthcare during the previous decade probably resulted from the initial HIPAA-compliance deadline in 2003, which may have generated a surge in U.S.-based health-care privacy professionals and respondents, and a subsequent fall-off among this cohort. The government sector continued its several-year trend of steady growth. It now accounts for one-fifth of survey respondents. The technology and software sector saw the most rapid growth since last year. It is the third most common employer of privacy professionals.

This year, we greatly expanded the number of sectors respondents could choose from, using the sector terminology found in the Forbes Magazine Global 1000 list. Our goal was twofold: to establish more detailed baselines in anticipation of a decade of growth in the privacy profession and to enable matching of survey data with outside datasets for richer future analyses.

Table 1: Respondents' sectors

Sector	2003	2010	2011	Change since 2003	Change since last year
Financial services	21%	20%	23%	2%	3%
Insurance	na	na	10%	na	na
Banking	na	na	10%	na	na
Diversified financials	na	na	3%	na	na
Government	4%	17%	20%	16%	3%
Technology and software	6%	9%	13%	7%	4%
Software and services	na	na	10%	na	na
Technology hardware and equipment	na	na	3%	na	na
Healthcare equipment and services	56%	15%	9%	-47%	-6%
Business services and supplies	5%	11%	7%	2%	-4%
Education	na	3%	4%	na	1%
Drugs and biotechnology	na	3%	4%	na	1%
Manufacturing	2%	3%	2%	na	-1%
Conglomerates	na	na	3%	na	na
Telecommunication services	2%	4%	3%	1%	-1%
Nonprofits	na	na	3%	na	na
Media	na	na	2%	na	na
Retailing	1%	3%	3%	2%	0%
Hotels, restaurants and leisure	0%	2%	1%	1%	-1%
Oil and gas operations	na	na	1%	na	na
Aerospace and defense	na	na	1%	na	na
Utilities	na	na	1%	na	na
Transportation	na	na	1%	na	na

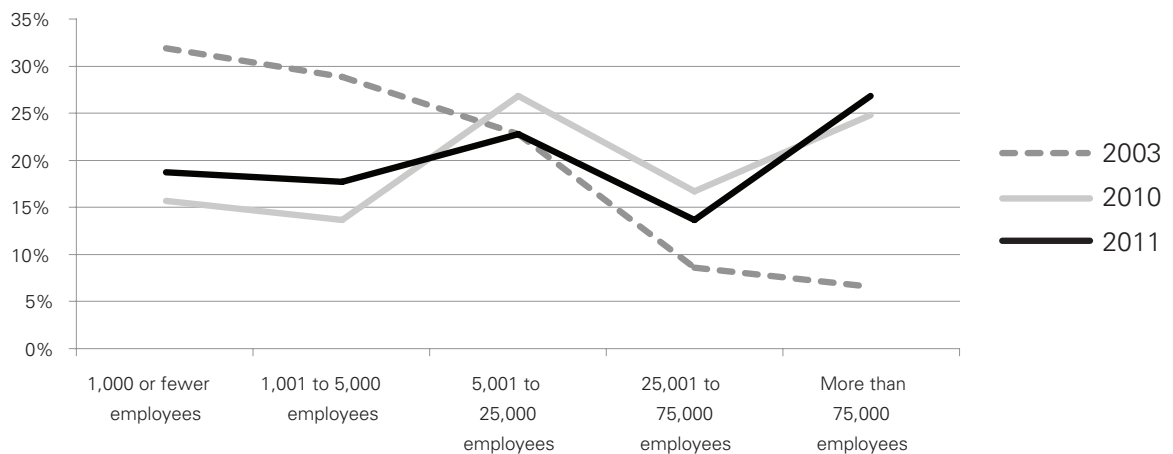
Organization Size

More large organizations represented. Most respondents to the 2011 survey came from those working for large-sized organizations. Responses from those working in the smallest firms—those with 1,000 or fewer employees—grew this year. Mid-sized firms declined in representation.

Table 2: Organization size

Organization Size	2003	2010	2011	Change, 2003 to 2011	Change, 2010 to 2011
1,000 or fewer employees	32%	16%	19%	-13%	+3%
Fewer than 250 employees	na	na	10%	na	na
250 to 1,000 employees	na	na	8%	na	na
1,001 to 5,000 employees	29%	14%	18%	-11%	+4%
5,001 to 25,000 employees	23%	27%	23%	0%	-4%
25,001 to 75,000 employees	9%	17%	14%	5%	-3%
More than 75,000 employees	7%	25%	27%	20%	+2%

Organization size



Geographic Location

Respondents still from North America, but their organizations are global. An overwhelming number of survey respondents—95 percent—are based in the United States and Canada, a finding consistent with last year's survey. The firms and organizations served by those privacy professionals, however, are much more global in scope. Thirty-three percent of all respondents reported having employees in Africa and the Middle East, for example, while 37 percent maintain personnel in Latin America and 45 percent in the Asia-Pacific region. Among private-sector firms, an even higher percentage have customers located in those regions.

Table 3: Region where survey respondents are based

Region	2010 Share	2011 Share
U.S.	85%	84%
Northeast	na	26%
South	na	15%
Upper Midwest	na	14%
West	na	14%
No response	na	14%
Canada	9%	11%
Europe	4%	3%
Asia-Pacific	1%	1%
Africa-Middle East	na	1%

Table 4: IAPP members' regions

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Total Members	99	698	916	886	1499	2170	2774	3863	5064	6137	6569	7899
U.S.						1968	2458	3383	4418	5219	5555	6505
Canada						81	152	268	376	535	551	649
Europe						93	116	147	178	271	337	512
Asia - Pacific						26	43	56	78	92	100	145
Latin America						2	3	4	8	13	19	32
Other Int'l						0	2	5	6	7	7	na

Table 5: Employees by region

Region	2010 #	2010%	2011 #	2011%	Change from 2010 to 2011
United States	798	90%	946	92%	2%
Canada	471	53%	519	50%	-3%
Europe	421	47%	495	48%	1%
Asia-Pacific	385	43%	459	45%	2%
Latin America	329	37%	379	37%	0%
Middle East & Africa	56	6%	344	33%*	27%

*This is the first year that the Middle East & Africa was included as its own region, which likely accounts for the sharp increase.

Table 6: Customers by region

Region	Respondents' existing markets
United States	94%
Canada	62%
Europe	60%
Asia-Pacific	53%
Latin America	50%
Middle East & Africa	42%

Regional presence of responding organizations

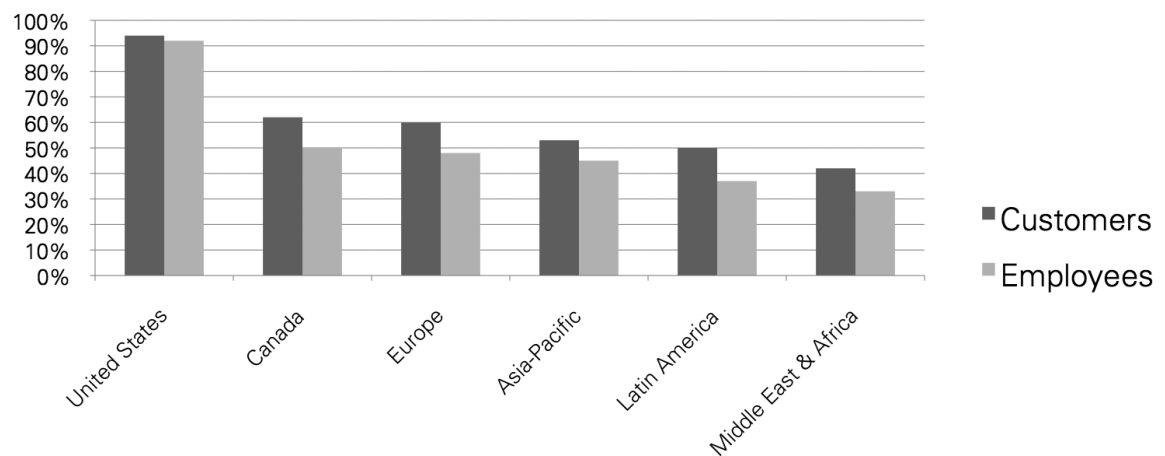


Table 7: Respondents' sectors by region

Sector	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
Aerospace & Defense	14					*
Banking	87	9	*			
Business Services & Supplies	53	11	5	*	*	*
Capital Goods	*					
Chemicals	*					
Conglomerates (multiple sectors)	25	*	*	*		
Construction						
Consumer Durables	*					
Diversified Financials	33	*				
Drugs & Biotechnology	26	*	6	*	*	
Education & Academia	30	10				*
Food, Drink & Tobacco	*					
Food Markets	*					
Government	180	27		*		
Healthcare Equipment & Services	66	20	*			
Hotels, Restaurants & Leisure	10	*				
Household & Personal Products	*					
Insurance	88	12	*			
Materials						
Media	24		*			
Nonprofit	24	5				
Oil & Gas Operations	*	*	*			
Retailing	25					*
Semiconductors	6		*			
Software & Services	95	*		*		
Technology Hardware & Equipment	24	*	5			
Telecommunication Services	31		5			
Trading Companies	*					
Transportation	5	*				
Utilities	9					

*fewer than five respondents

Role

What is the nature of the privacy role? As we noted in *A Call for Agility: The Next-Generation Privacy Professional*, the privacy profession is in a period of transition, and it is maturing. This year's results continue to reflect this trend. Among the key findings:

- Privacy professionals are evenly distributed across all levels of their organizations, with 42 percent occupying middle-management positions.
- Privacy leaders are most often in senior positions, with 50 percent reporting to the top executive or a direct report.
- As in past years, respondents report similar allocations of time, but they are performing slightly more strategic tasks this year.
- One of the top sources of private-sector and government privacy jobs appears to be the IT department.
- The most common words in respondents' titles included "privacy," "security" and "compliance," while a full 27 percent said their title was "chief privacy officer or official."
- Privacy professionals report a high level of self-assessed privacy expertise, with the most common rating being "I have the knowledge, skills and experience to manage all aspects of our organization's privacy needs."
- Roughly three-quarters of respondents are seeking convenient career development opportunities in 2011, including Web conferences, local conferences and privacy information services, while half are planning to travel for one privacy conference.

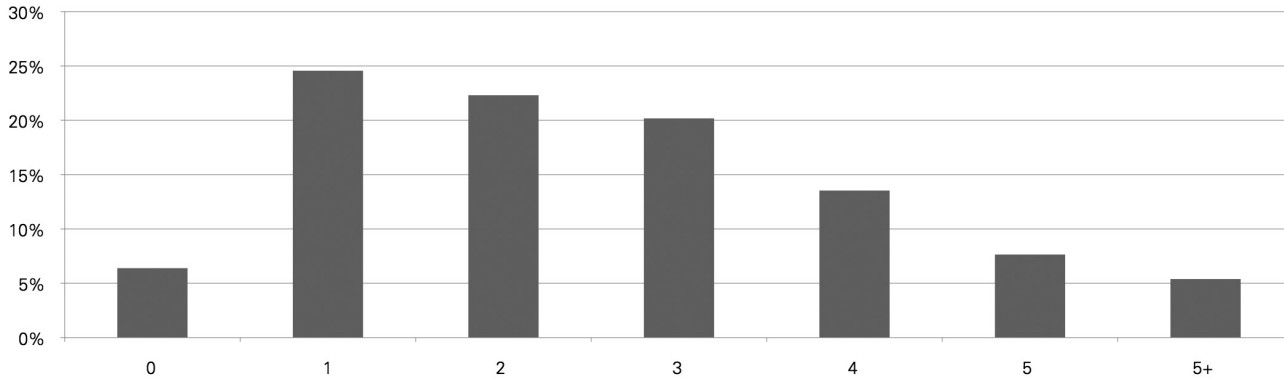
Level within the Organization

Privacy pros spread across all levels of organizations. We asked privacy pros to tell us about their reporting structure, finding that a startling 31 percent report directly to the top executive or are only one layer of management away from the top executive. Twenty-eight percent are four or more levels from the top executive, with the remaining 42 percent occupying mid-management positions. This bell-shaped distribution across organizational levels, indicative of a mature stage, tells the story of a privacy profession which has come of age.

Table 8: Levels of management between respondents and the chief executive
Private sector in-house and government professionals

Management Level	Number	Share
0 (You are a "C-level" executive who reports directly to the top executive)	51	6%
1 (Typically a Vice President who reports to someone who reports to the top executive)	196	25%
2 (Typically a Director or Vice President)	178	22%
3 (Typically a Manager or Director)	161	20%
4 (Typically a Senior Analyst or Manager)	108	14%
5 (Typically an Analyst or Senior Analyst)	61	8%
6 (You are a "C-level" executive who reports directly to the top executive)	51	6%

Management levels between respondents and top executives



Senior-level privacy leaders. We asked privacy pros about the reporting structure of their organization’s top privacy leader. Only five percent of respondents reported their organization had no privacy leader, while half said their privacy leader either reported to the top executive or was only one layer of management away. This suggests that not only has privacy “arrived,” but the privacy agenda also has access to the “C suite.” Respondents from Canada reported their privacy leaders had the highest average organizational level, followed by the United States and Europe.

Table 9: Levels of management between the organization’s top privacy leader and the chief executive

Private sector in-house and government professionals

Management Level	Number	Share
0 (Our top privacy leader is a “C-level” executive who reports directly to the top executive)	124	16%
1 (Typically a Vice President who reports to someone who reports to the top executive)	268	34%
2 (Typically a Director or Vice President)	195	24%
3 (Typically a Manager or Director)	115	14%
4 (Typically a Senior Analyst or Manager)	44	6%
5 (Typically an Analyst or Senior Analyst)	6	1%
5+	11	1%
Organization does not have a privacy leader	36	5%

Levels of management between the privacy leader and the top executive

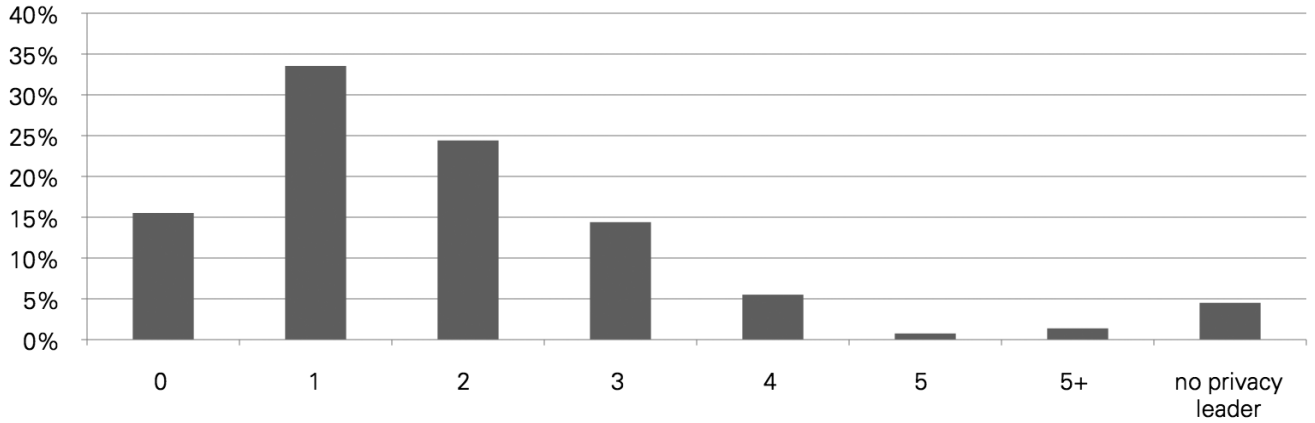
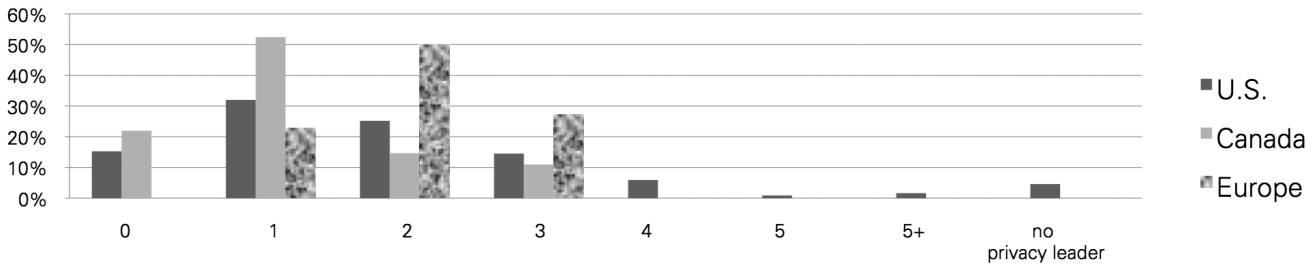


Table 10: Levels between the top privacy leader and the top executive, by region
Private sector in-house and government professionals

Management Level	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
0 (Our top privacy leader is a “C-level” executive who reports directly to the top executive)	103	18	*	*	*	*
1 (Typically a Vice President who reports to someone who reports to the top executive)	216	43	5	*	*	6
2 (Typically a Director or Vice President)	170	12	11	*	*	*
3 (Typically a Manager or Director)	98	9	6	*	*	*
4 (Typically a Senior Analyst or Manager)	40	*	*	*	*	*
5 (Typically an Analyst or Senior Analyst)	6	*	*	*	*	*
5+	11	*	*	*	*	*
Organization doesn’t have a privacy leader	31	*	*	*	*	*

*fewer than five respondents

Levels between CPO and CEO, by region



Responsibilities

Balanced allocation of time. Survey respondents have reported a consistent, relatively unchanging mix of time allocation over the years. This year marked a slight increase in the portion of time spent on strategic issues. Indeed, the most time-consuming single task identified was of a strategic nature—advising the organization on privacy issues. Not only did this task account for 15 percent of respondents’ weekly hours on average, but also that line item increased the most of any since last year—4 points. This is further evidence that the privacy agenda is gaining access to the strategic decision makers of organizations.

Table 11: Allocation of time for various tasks
Private sector in-house and government professionals

Time Allocation	2010	2011	Change from 2010 to 2011
STRATEGIC	30%	32%	+2%
Developing privacy strategy	9%	8%	-1%
Analyzing privacy regulations	10%	8%	-2%
Advising and consulting the organization on privacy	11%	15%	4%
PROCESS	33%	32%	-1%
Developing and performing privacy training and communications	9%	8%	-1%
Monitoring and measuring privacy compliance and enforcement	8%	9%	1%
Responding to data incidents	9%	7%	-2%
Reporting to management and privacy stakeholders	8%	7%	-1%
FOUNDATIONAL	23%	22%	-1%
Performing privacy risk assessments and data inventories	8%	8%	0%
Developing and implementing privacy policies and guidance	11%	10%	-1%
Administration of privacy personnel and budget	4%	4%	0%
ACTIVITIES NOT RELATED TO PRIVACY	-	14%	14%

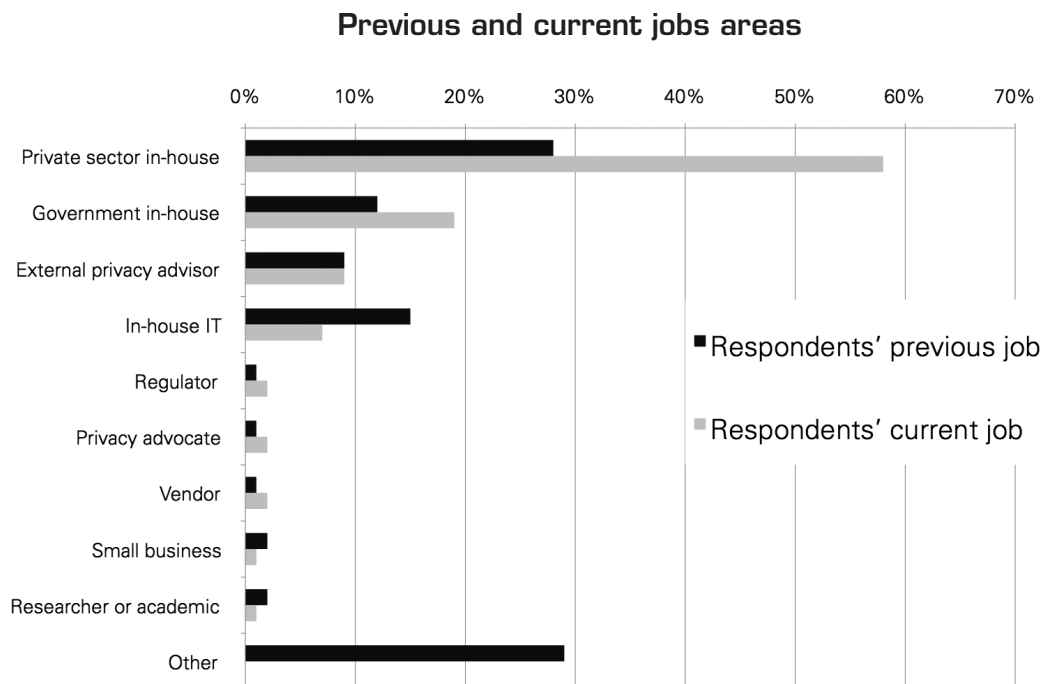
Note: We made some statistical adjustments to last year's data to compare it with this year's results, including the assumption that the category "activities not related to privacy" would have received about the same share of respondents last year had that option been listed in last year's survey.

Career Development

Most privacy professionals found in corporate positions. By far, the largest share of respondents—58 percent—work as in-house privacy professionals in private corporations. This is followed by government-sector privacy jobs. These two employment opportunities were also the highest net gainers on respondents’ career paths. Among those surveyed, more individuals are moving to jobs in government and the private sector than are leaving these positions. For the first time this year, we asked about other niches in the privacy profession, IT and small business. The most common previous job was “other.” The in-house IT role may be a key provider of new private-sector and government privacy positions—that role was the largest net loser in the survey.

Table 12: Career path of most recent job change

Privacy Role	Respondents’ previous jobs	Respondents’ current jobs	Change
Private sector in-house	28%	58%	30%
Government in-house	12%	19%	7%
External privacy advisor	9%	9%	0%
In-house IT	15%	7%	-8%
Regulator	1%	2%	1%
Privacy advocate	1%	2%	1%
Vendor	1%	2%	1%
Small business	2%	1%	-1%
Researcher or academic	2%	1%	1%
Other	29%	na	na



“Privacy,” “compliance” and “security” most frequent in job titles. We asked respondents to choose from a list of keywords which ones appeared in their job title. Not surprisingly, “privacy” appears in just over half of responses. Remarkably, more than a quarter of respondents say they have the “CPO” moniker. In the future, this baseline will tell us whether the use of this C-suite title is growing or waning in popularity. Interestingly, the second-most-occurring keyword among respondents was not “security,” but “compliance.” This tracks with earlier results showing privacy being placed more often in the compliance department than in the information security department. The European equivalent of privacy—“data protection”—appeared in three percent of responses, which corresponds with the smaller EU sample size.

Table 13: Key words in respondent job titles

Key Word	Number	Share
Privacy	509	53%
Privacy officer or official	370	39%
Chief privacy	283	30%
Chief privacy officer or official	258	27%
Compliance	123	13%
Compliance officer or official	88	9%
Chief compliance	54	6%
Chief compliance officer or official	52	5%
Security	75	8%
Security officer or official	44	5%
Chief Security	35	4%
Chief security officer or official	30	3%
Data protection	30	3%
Data protection officer or official	14	1%
Chief data protection	8	1%
Chief data protection officer or official	7	1%
Risk	29	3%
Risk officer	15	2%
Chief risk	13	1%
Chief risk officer or official	9	1%
Governance	18	2%
Chief governance	10	1%
Chief governance officer or official	9	1%

Self-assessment of privacy expertise. We asked respondents to rate their level of expertise on a five-point scale that included detailed definitions at each level. The results show that privacy practitioners are comfortable and confident in their abilities. Almost three-quarters of respondents said that they possessed the competence at least sufficient to manage all aspects of their organizations' privacy needs. Indeed, one in seven respondents said that they were sufficiently competent to manage the privacy function of a multinational firm in any industry or to manage any large practice advisory firm. Interestingly, the relatively high distribution of this curve somewhat matches the distribution of the seniority level of privacy leaders. It may be that many survey respondents who are not themselves the privacy leader or practice leader are confident that they could do their superiors' jobs.

Table 14: Level of privacy expertise of respondents

Self-Assessed Privacy Expertise	Number	Share
I am new to privacy.	40	4%
I can fulfill some of the privacy needs of our organization very well.	249	24%
I have the knowledge, skills and experience to manage all aspects of our organization's privacy needs.	318	30%
I have the knowledge, skills and experience to lead a privacy function or privacy practice in a regulated industry (such as healthcare, finance, government or telecom) and regulated jurisdiction (such as Europe, Canada, U.S., Australia or Japan).	300	29%
I have the knowledge, skills and experience to lead a privacy function of a large multinational in any type of industry or the privacy practice of a large advisory firm.	145	14%

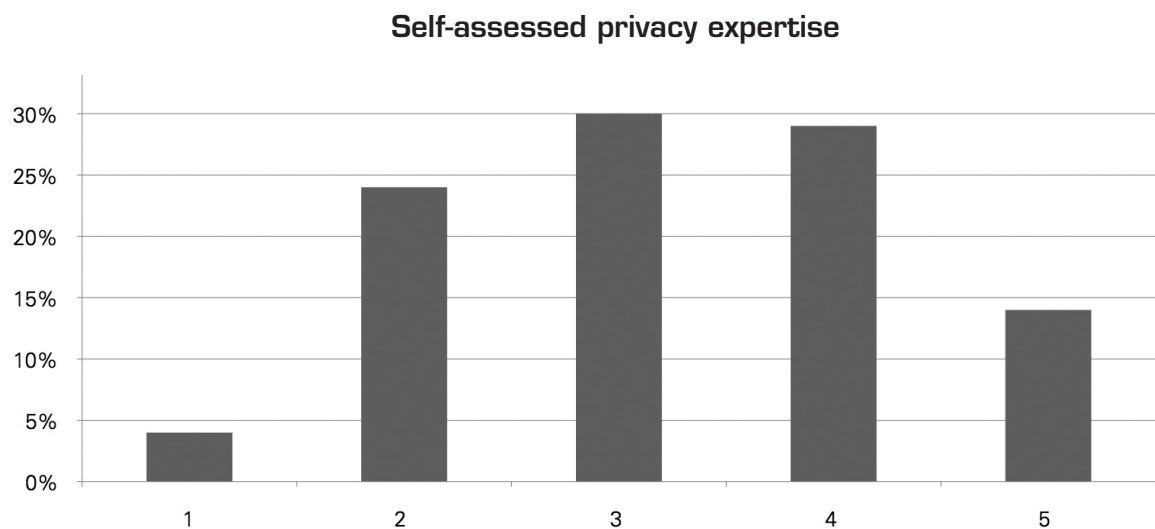


Table 15: Privacy expertise by sector and region

Industry Sector	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
Aerospace & Defense	4					2
Banking	3	3	4			
Business Services & Supplies	3	4	4	3	5	2
Capital Goods	3					
Chemicals	3					
Conglomerates (multiple sectors)	3	4	5	4		
Construction						
Consumer Durables	4					
Diversified Financials	3	3				
Drugs & Biotechnology	3	4	2	2	3	
Education & Academia	3	3				4
Food, Drink & Tobacco	3					
Food Markets	2					
Government	3	3		4		
Healthcare Equipment & Services	3	4	4			
Hotels, Restaurants & Leisure	4	3				
Household & Personal Products	4					
Insurance	3	3	3			
Materials						
Media	3		2			
Nonprofit	3	3				
Oil & Gas Operations	3	2	4			
Retailing	3					2
Semiconductors	3		3			
Software & Services	3	4		4		
Technology Hardware & Equipment	3	3	3			
Telecommunication Services	3		4			
Trading Companies	4					
Transportation	3	4				
Utilities	4					

Privacy professionals seek convenient career development opportunities. We asked privacy professionals how they would develop their skills and expertise in 2011. Respondents reported that they intend and are authorized to pursue low-cost and local career development opportunities. Respondents' indicated that local conferences, Web conferences and privacy news service subscriptions are the top choices for staying on top of new developments in their profession and acquiring new skills in 2011.

Table 16: Planned career development activities in the coming year

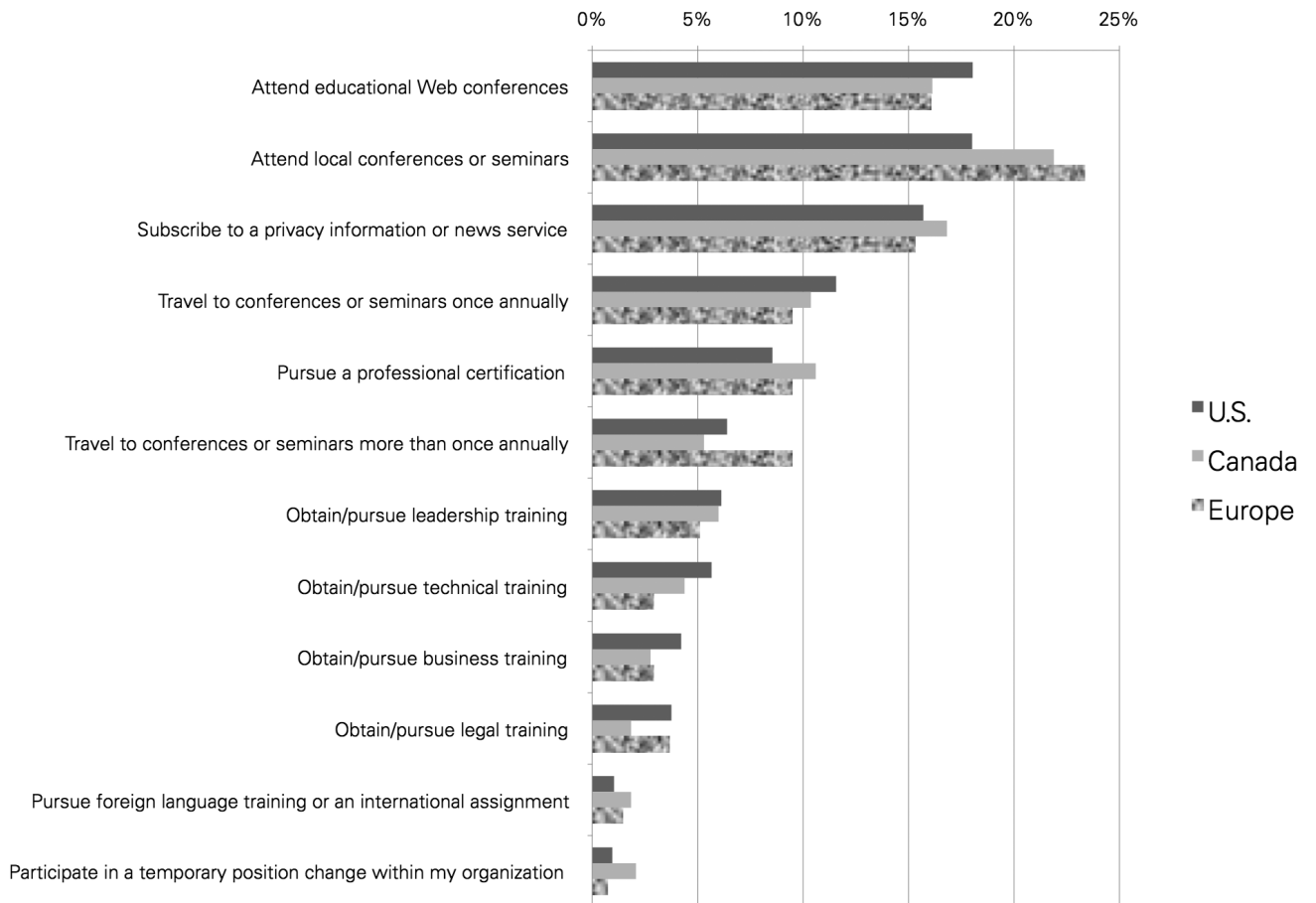
Career Development Activity	Number	Share
Attend educational Web conferences	763	80%
Attend local conferences or seminars	796	83%
Subscribe to a privacy information or news service	678	71%
Travel to conferences or seminars once annually	488	51%
Pursue a professional certification	382	40%
Travel to conferences or seminars more than once annually	273	29%
Obtain/pursue leadership training	266	28%
Obtain/pursue technical training	236	25%
Obtain/pursue business training	176	18%
Obtain/pursue legal training	154	16%
Pursue foreign language training or an international assignment	52	5%
Participate in a temporary position change within my organization	51	5%

Table 17: Planned career development activities by region

*How privacy professionals in each region plan to obtain new skills and expertise in 2011
(number of respondents).*

Career Development Activity	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
Attend educational Web conferences	663	70	22	4	2	2
Attend local conferences or seminars	662	95	32	4	1	2
Subscribe to a privacy information or news service	577	73	21	3	1	3
Travel to conferences or seminars once annually	425	45	13	4	0	1
Pursue a professional certification	314	46	13	5	3	1
Travel to conferences or seminars more than once annually	235	23	13	0	1	1
Obtain/pursue leadership training	225	26	7	5	2	1
Obtain/pursue technical training	208	19	4	3	0	2
Obtain/pursue business training	155	12	4	2	1	2
Obtain/pursue legal training	138	8	5	2	0	1
Pursue foreign language training or an international assignment	38	8	2	2	1	1
Participate in a temporary position change within my organization	35	9	1	3	1	2

Planned career development activities in 2011, by region



Function

What is the nature of the privacy function? Where is it organizationally situated? What level of resources does it have access to, and what are its business drivers? There is no consensus for these questions according to this year's responses. In many cases, however, two distinct answers top all others, suggesting the state of transition of the privacy profession is beginning to yield some time-tested alternatives. Among the key findings:

- There are two common locations for the privacy function: the legal or compliance departments, which were cited by 63 percent of corporate and government in-house respondents.
- Privacy functions are either very small—39 percent reported two or fewer people in their privacy office—or relatively large; 39 percent reported teams of six or more.
- Similarly, budgets for outside privacy support are either very limited or quite substantial. Forty percent said they had very little budget with which to make an impact—\$75,000 or less. Meanwhile, 37 percent said they had enough to fund a significant project over \$250,000.
- Eighty-two percent of corporate and government in-house respondents use a privacy attorney, while half as many use a privacy consultant.
- Respondents were unanimous on the top two business drivers for the privacy function: 97 percent said meeting regulatory compliance obligations, and 80 percent said avoiding having to make data breach notifications. Increasing the value of data, providing a competitive differentiator and enabling more effective marketing were seen as important for less than one-third of respondents' executives.
- Almost two-thirds of respondents said their organization had not issued a security breach notice or suffered a privacy enforcement action in the past year, while three percent reported either a breach or an enforcement action occurred to them more than 50 times last year.
- Privacy professionals rate their privacy maturity highly, with 46 percent self-assessing their organization at the Level 4 “managed” or Level 5 “optimized” categories on a five-point scale.

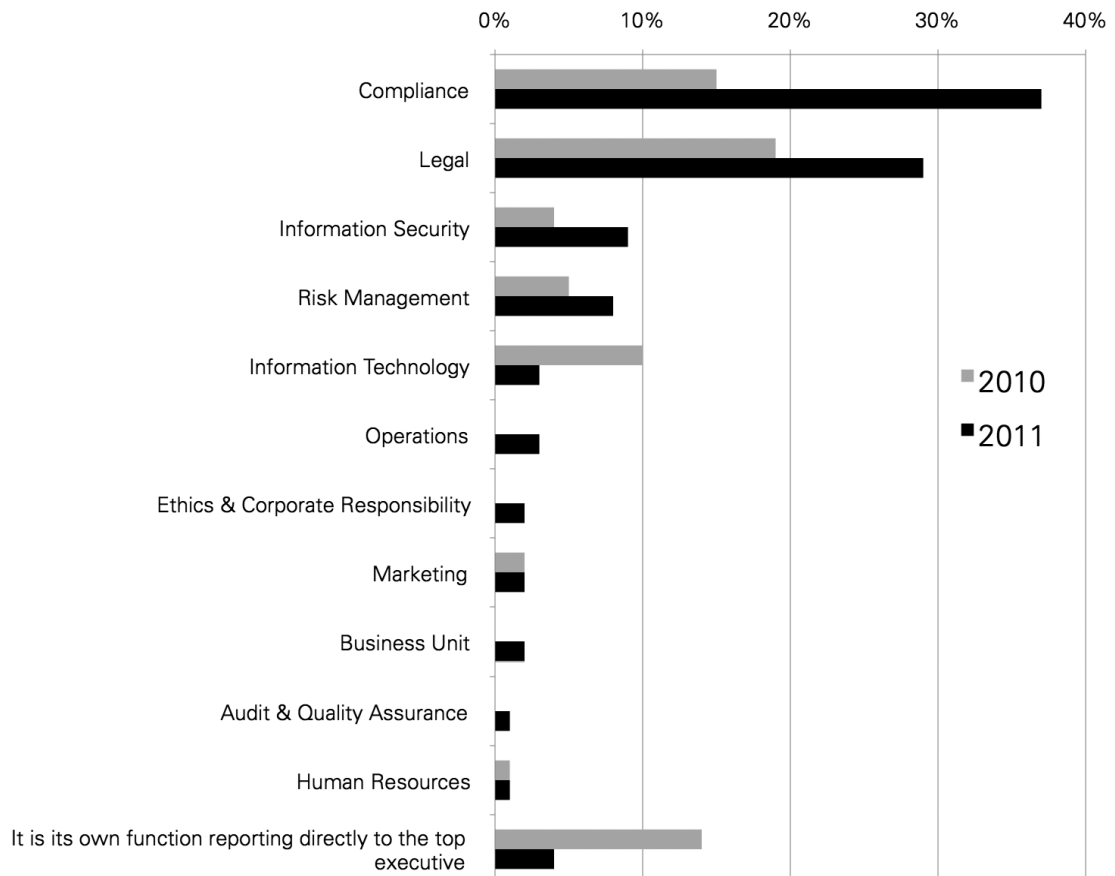
Location of the Privacy Function

Surge of placing privacy in legal and compliance departments. Privacy departments in private corporations and government agencies have turned up in myriad departments. Last year, the top two locations for the privacy office were legal and compliance. A sharp increase toward these two departments appears to have occurred in 2010, further solidifying them as the most common destination for the privacy function.

Table 18: Reporting structure of corporate and government privacy offices

Department	2010	2011	Change
Compliance	15%	37%	+22
Legal	19%	29%	+10
Information Security	4%	9%	+5
Risk Management	5%	8%	+3
Information Technology	10%	3%	-7
Operations	-	3%	-
Ethics & Corporate Responsibility	-	2%	-
Marketing	2%	2%	-
Business Unit	-	2%	-
Audit & Quality Assurance	-	1%	-
Human Resources	1%	1%	-
It is its own function reporting directly to the top executive	14%	4%	-10

Location of privacy office



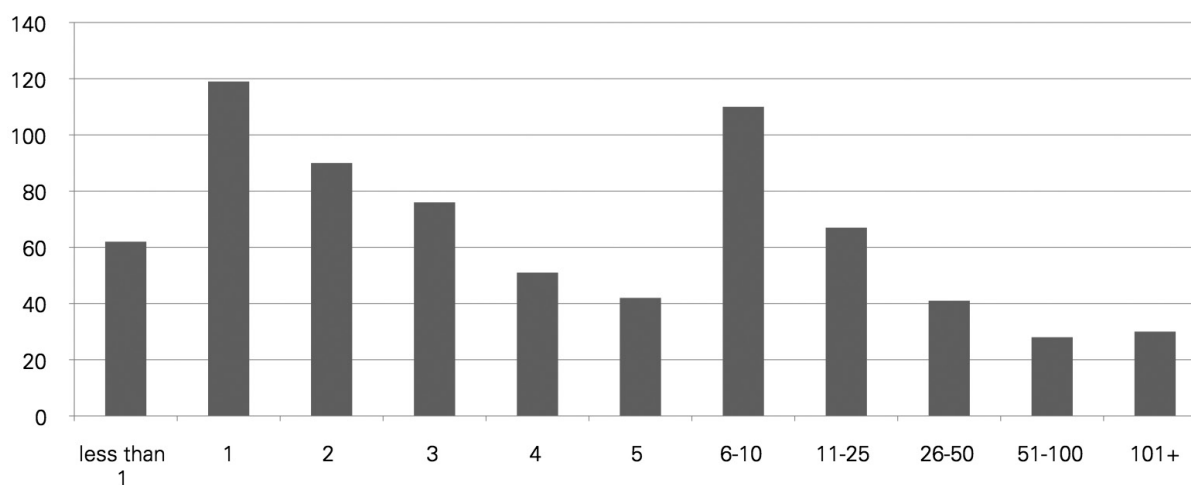
Resources of the Privacy Function

One-person privacy office still the norm. The privacy person is a lone wolf in organizations. Just over a quarter of respondents indicated that there are one or fewer full-time privacy staff at their organization. Overall, 61 percent say they have fewer than six people on their privacy team. Remarkably, this means that a full 39 percent employ six or more privacy professionals, with a significant eight percent maintaining more than 50. This suggests there may be a “tale of two cities” in the privacy profession—the privacy “jack of all trades” experience and the “lost in the crowd” experience.

Table 19: Number of privacy staff
Private sector in-house and government respondents

Size of privacy staff	Number of firms and agencies with this size staff	Share responding to this question
less than 1	62	9%
1	119	17%
2	90	13%
3	76	11%
4	51	7%
5	42	6%
6-10	110	15%
11-25	67	9%
26-50	41	6%
51-100	28	4%
101+	30	4%

Number of privacy staff



Feast or famine budgets for outside support. We asked in-house corporate and government respondents how much budget their privacy function has for non-personnel items. The answers reflected the same “tale of two cities” as the staffing question. Forty percent said they have very little to make an impact—\$75,000 or less. Meanwhile, a full 37 percent indicated having enough to fund a significant project over \$250,000, with five percent reporting a budget of more than \$5 million. American respondents’ budgets were higher than their Canadian counterparts, 65 percent had \$75,000 or less to work with. Interestingly, the most common European budget was higher than the midpoint of both, at \$250,001 to \$1 million.

Table 20: Non-personnel privacy budgets
Private sector in-house and government respondents

Budget	2011 Number	2011 Share
\$0	44	7%
Under \$25,000	131	20%
\$25,000–75,000	86	13%
\$75,001–150,000	86	13%
\$150,001–250,000	75	11%
\$250,001–1million	141	21%
\$1,000,001–5 million	71	11%
Over \$5 million	36	5%

Privacy budgets

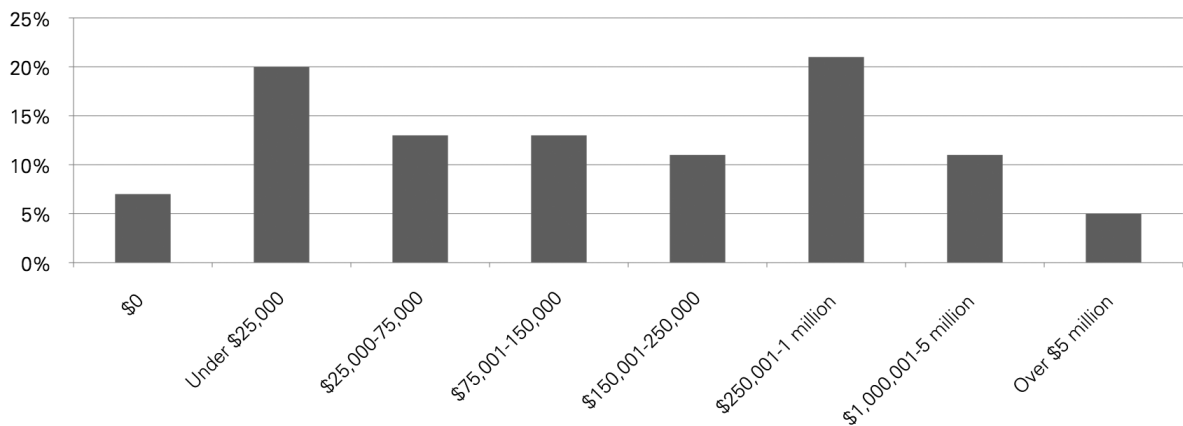


Table 21: Non-personnel privacy budgets, by region

Budget	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
\$0	36	7	*	*	*	*
Under \$25,000	94	33	*	*	*	*
\$25,001-75,000	69	12	*	*	*	*
\$75,001-150,000	73	9	*	*	*	*
\$150,001-250,000	67	5	*	*	*	*
\$250,001-1 million	124	9	7	*	*	*
\$1,000,001-5 million	63	5	*	*	*	*
Over \$5 million	36	0	*	*	*	*

*fewer than five respondents

Outside support important. Where are the budgets for outside support being allocated? The top line item is outside legal advice, followed in a distant second place by outside consulting. These proportions varied by region, however. Canadians, with relatively lower budgets, used consultants more often, while Europeans, with relatively higher budgets, used attorneys more often.

Table 22: Sources of external privacy support*

Source	Number	Share
Privacy attorney	431	81%
Privacy consultant	225	42%
Privacy services firms	142	27%

* Respondents could select more than one answer.

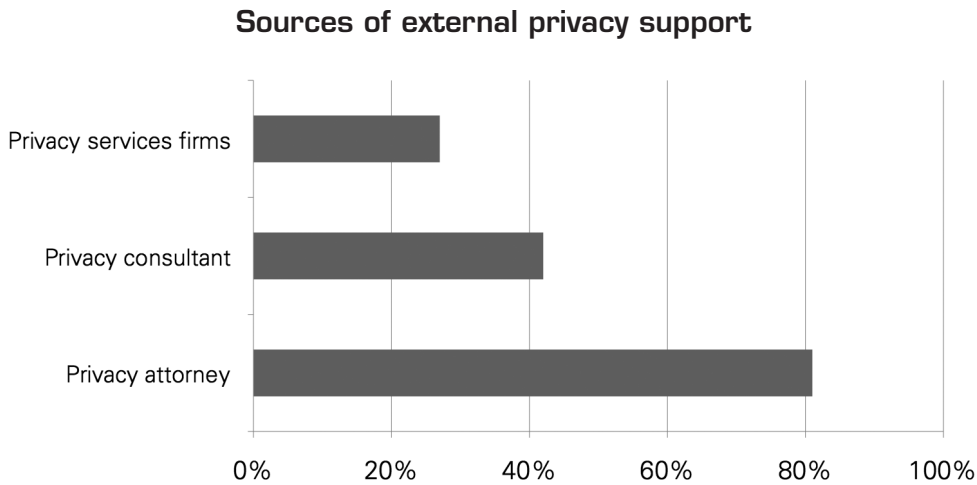


Table 23: Sources of external privacy support, by region

Source	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
Privacy attorney	372	37	20	★	★	★
Privacy consultant	184	35	5	★	★	★
Privacy services firms	122	14	★	★	★	★

★fewer than five respondents

Privacy Function Catalysts

Compliance compels firms to act. Risk reduction, not revenue generation, is by far the main reason in-house corporate and government respondents believe their top executives fund the privacy function. Survey results show that virtually all firms undertake actions on the privacy front with the primary objective of satisfying regulatory compliance obligations. Avoiding the need to make data breach notifications and the accompanying bad publicity was important for eight out of 10 respondents. Increasing the value of data, providing a competitive differentiator and enabling more effective marketing was seen as important for fewer than one-third of respondents. These results held true regardless of region. Even in Canada and Europe, for example, where data breach notification is not mandated to the degree of the U.S., this ranked as the number two reason that executives fund their privacy programs.

Table 24: Corporate and government executive reasons for funding the privacy function*

Reason for funding privacy	Number	Share
To meet regulatory compliance obligations	612	97%
To reduce the risk of data breach notification and publicized data breaches	516	81%
To enhance the organization's brand and public trust	402	63%
To meet the expectations of business clients and partners	385	61%
To reduce the risk of employee and consumer lawsuits	344	54%
To enable global operations and entry into new markets	216	34%
To increase the value and quality of data	191	30%
To provide a competitive differentiator	168	26%
To increase revenues from cross-selling and direct marketing	151	24%
To reduce the cost of storing data	77	12%

★ Respondents could select more than one answer.

Executive reasons for funding privacy

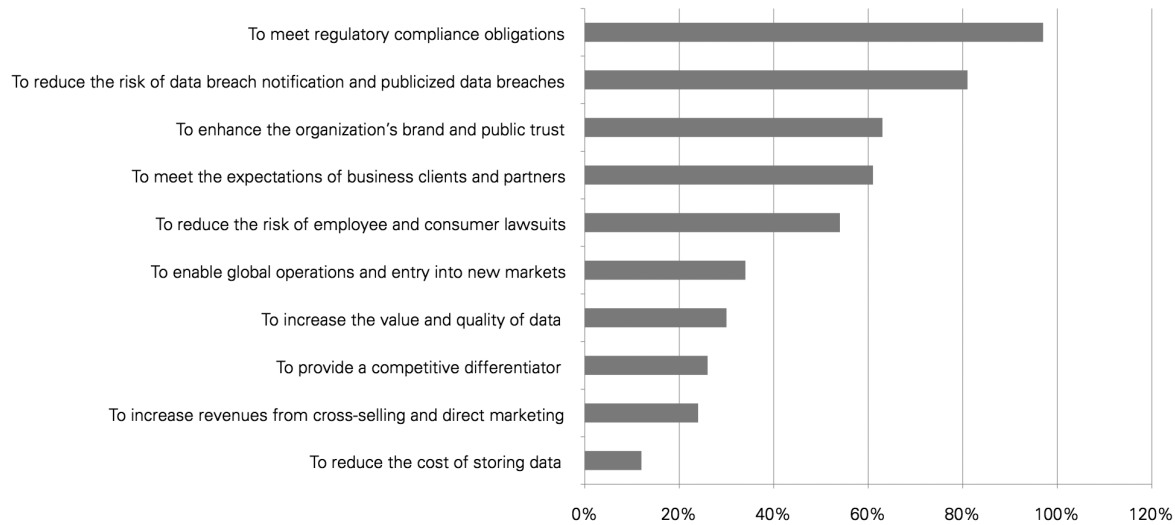


Table 25: Corporate and government executive reasons for funding the privacy function, by region *

Reason for funding privacy	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
To meet regulatory compliance obligations	528	48	29	*	*	*
To reduce the risk of data breach notification and publicized data breaches	441	44	23	*	*	*
To enhance the organization's brand and public trust	345	33	19	*	*	*
To meet the expectations of business clients and partners	333	33	16	*	*	*
To reduce the risk of employee and consumer lawsuits	298	22	17	*	*	*
To enable global operations and entry into new markets	198	7	6	*	*	*
To increase the value and quality of data	169	10	8	*	*	*
To provide a competitive differentiator	149	8	8	*	*	*
To increase revenues from cross-selling and direct marketing	132	9	6	*	*	*
To reduce the cost of storing data	70	*	*	*	*	*

*fewer than five respondents

Turning a corner on data breach notifications? Security breach notification has garnered more attention in the past several years—in the United States in particular—than perhaps any other privacy topic. But are organizations getting better about managing their data breaches, or are they just being more cautious about reporting them? We were surprised to find almost two-thirds of respondents said their organization had not issued a security breach notice or suffered a privacy enforcement action in the past year. Interestingly, for three percent of organizations, data breach notification and enforcement actions have become a core competence, occurring more than 50 times last year.

Table 26: Frequency of privacy incidents

Frequency	Number	Share
None	426	62%
One incident	81	12%
2-5 incidents	110	16%
6-10 incidents	24	3%
11-50 incidents	27	4%
More than 50 incidents	18	3%

Table 27: Frequency of privacy incidents, by region

Frequency	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
None	357	54	12	*	*	*
One incident	65	10	*	*	*	*
2-5 incidents	93	13	*	*	*	*
6-10 incidents	21	*	*	*	*	*
11-50 incidents	23	*	*	*	*	*
More than 50 incidents	17	*	*	*	*	*

**fewer than five respondents*

Shift in budget priorities for 2011? We asked in-house corporate and government respondents about their top project priorities for the coming year. Their answers suggest there is a general move toward a more proactive approach to managing privacy risk and compliance. Three-quarters, for example, cited training and awareness and privacy audits and assessments as top priorities. Interestingly, consolidating privacy choices and consents into a common framework to enable more effective direct marketing ranked near the bottom of project priorities. This finding tracks with responses to the earlier question about the relative importance of using privacy initiatives to generate revenues.

Table 28: 2011 Priority projects for corporate and government in-house privacy professionals *

Project	Number	Share
Training and awareness	601	86%
Privacy audits and assessments	516	74%
Policy revision	503	72%
Process documentation and improvement	483	69%
Vendor and third-party assurance	322	46%
Data inventorying and mapping	306	44%
Data loss prevention technology	288	41%
Governance, risk and compliance technology	280	40%
Data use logging and monitoring technology	187	27%
Privacy choice and consent consolidation	142	20%
External certification	107	15%

* Respondents could select more than one answer.

2011 priority projects

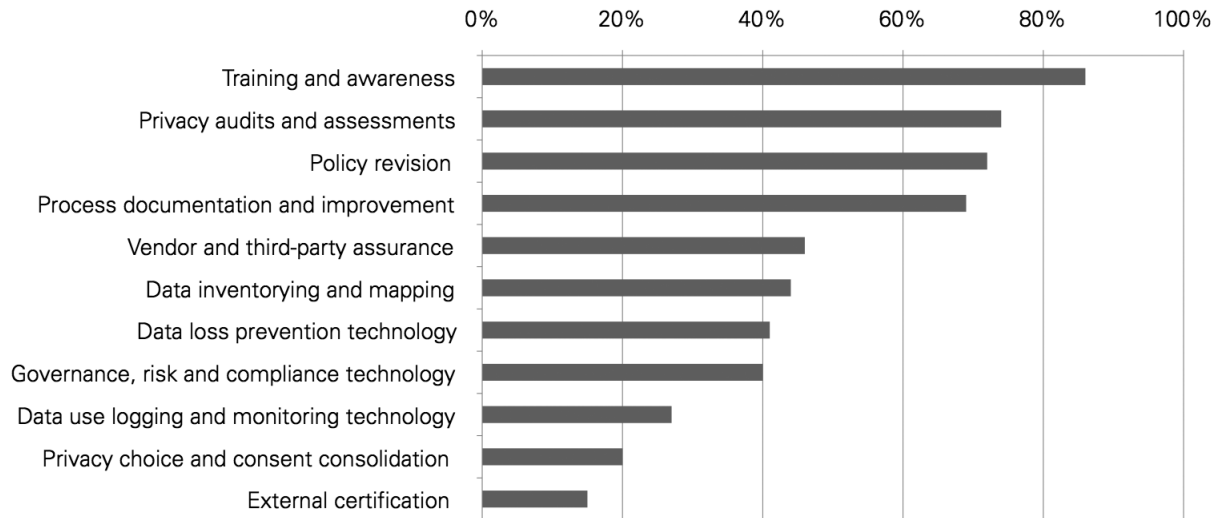


Table 29: 2011 priority projects for corporate and government in-house privacy professionals, by region *

Project	U.S.	Canada	Europe	Asia-Pacific	Latin America	Middle East & Africa
Training and awareness	42	5	*	*	*	*
Privacy audits and assessments	35	5	*	*	*	*
Policy revision	33	5	*	*	*	*
Process documentation and improvement	32	*	*	*	*	*
Data inventorying and mapping	21	4	*	*	*	*
Data loss prevention technology	21	*	*	*	*	*
Vendor and third-party assurance	20	*	*	*	*	*
Governance, risk, and compliance technology	18	*	*	*	*	*
Privacy choice and consent consolidation	9	*	*	*	*	*
External certification	5	*	*	*	*	*
Data use logging and monitoring technology	*	*	*	*	*	*

*fewer than five respondents

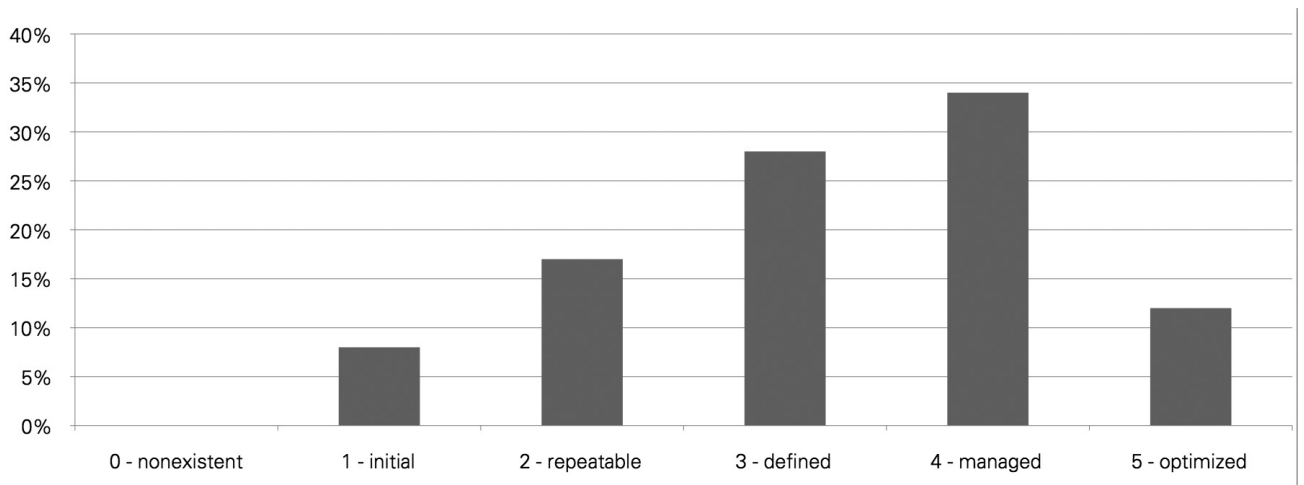
Privacy Function Outcomes

A continued high level of organizational privacy maturity. The 2010 survey revealed a high level of self-reported privacy program maturity; most respondents rated themselves a level four maturity based on a scale of one to five. This outcome seemed to contradict anecdotal evidence and other survey data at the time that suggested most organizations, and the privacy profession itself, had not reached a mature stage. For this 2011 survey, we added more objective criteria based on the MPC Privacy Maturity Model in order to better align with established program measurement frameworks. Nonetheless, the most common response remained a relatively high four rating.

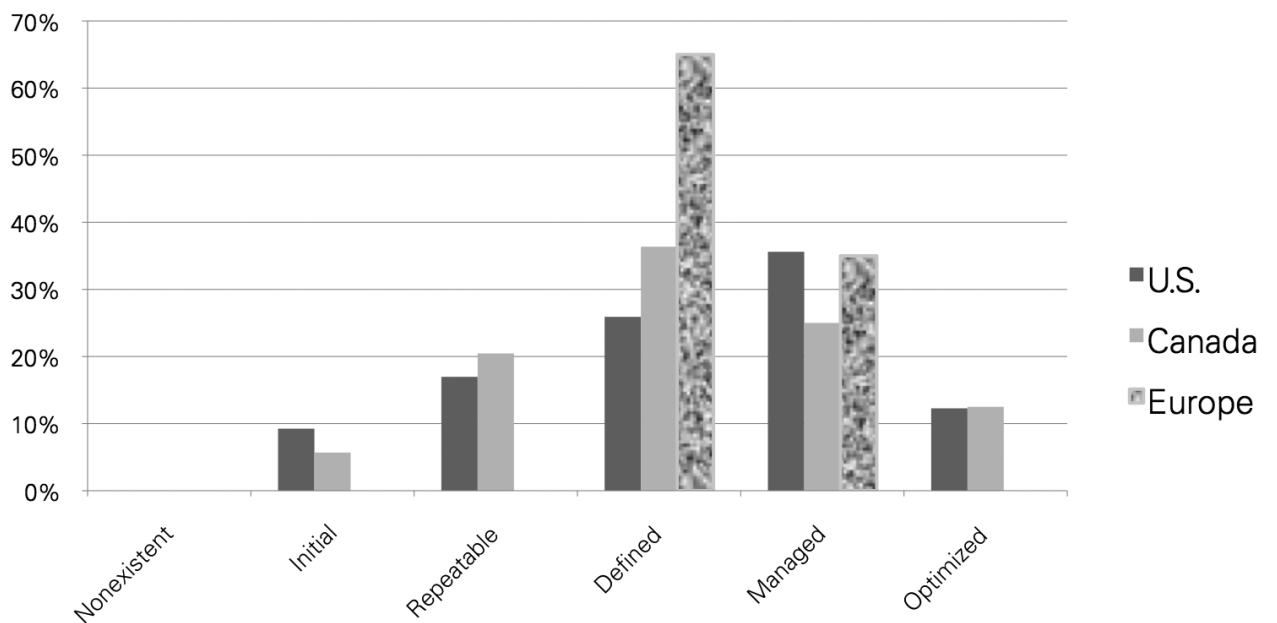
Table 30: Self-assessed privacy maturity of corporate and government organizations

Privacy Maturity Level	Number	Share
Nonexistent: nobody in the organization is working on privacy and there are no documented privacy policies or processes.	2	0%
Initial: At least some parts of the organization are following an ad hoc, albeit inconsistent, approach to data privacy, although there are no documented privacy policies or standards.	66	8%
Repeatable: The organization has a consistent overall approach in the areas of most important privacy risks and obligations, but at most there is only a minimal or general level of privacy policy and process documentation. Key business objectives for privacy are partially met, but significant privacy risks and compliance obligations remain.	133	17%
Defined: The organization has a documented, detailed approach to privacy policies and processes that apply to the entire organization, but there is no routine measurement or enforcement.	217	28%
Managed: The organization regularly measures and enforces its compliance with its privacy policies and processes, conducts ad hoc benchmarking with its peers and makes regular process improvements based on these findings.	265	34%
Optimized: The organization has refined its privacy practices to the level of recognized best practice, where instances of privacy risks and noncompliance have been mitigated to acceptable levels, and a culture of privacy is endemic across the organization.	95	12%

Self-assessed privacy maturity



Self-assessed privacy maturity by region



Salary

Many professionals joined the privacy profession because the work is intriguing and cutting-edge. Others have been assigned the privacy role in addition to previous duties as their organizations recognized the need for privacy management. Whatever their reasons for arriving in the privacy profession, the questions ultimately arise: Am I fairly compensated? What are my peers making? What are the most important factors in boosting my pay? In this section, we lay out the most comprehensive market study conducted to date about privacy professional compensation. Key findings include:

- The average base salary grew an impressive 12 percent since last year, to \$123,971, representing the highest figure we've recorded to date. With an average bonus just over \$18,000, the average total compensation for privacy pros topped out at \$142,117.
- The most highly compensating private-sector departments for privacy professionals are those that typically employ attorneys and MBAs, with marketing (\$154,654), ethics & corporate responsibility (\$153,188), and legal (\$151,396) leading the pack.
- The most highly compensated government privacy pros work in standalone privacy offices (\$105,630), IT (\$104,432) and risk management (\$103,600).
- Those working for European-headquartered firms earned the most (\$133,026), followed by firms based in the U.S. (\$126,761) and Canada (\$94,698).
- Privacy pros based in the U.S. earned the top average salary (\$127,426), followed by those in Europe (\$114,947) and Canada (\$95,909).
- The highest-paying sectors for privacy pros are utilities (\$165,000), business services and supplies (\$160,777) and telecommunications (\$160,197).

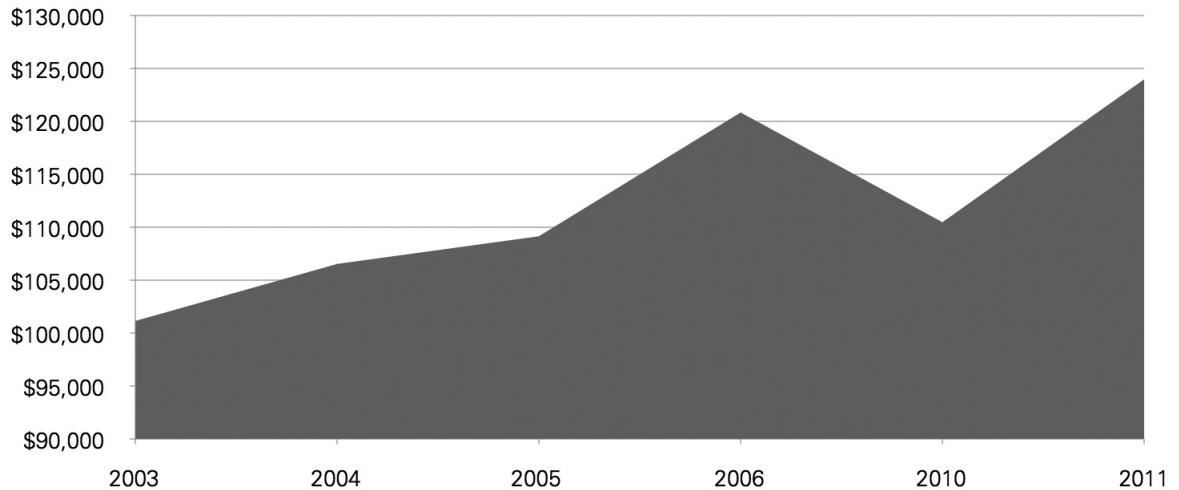
Overall Salary Measures

Average salary rebounds. This year's much-awaited survey reveals some good news on the salary front. Since last year's retrenchment, base wages have stormed back, rising an impressive 12 percent to \$123,971—the highest figure ever. With an average bonus just over \$18,000, the average total compensation for privacy pros topped out at \$142,117.

Table 31: Average privacy base salary

Year	Overall average
2003	\$101,146
2004	\$106,533
2005	\$109,146
2006	\$120,840
2010	\$110,476
2011	\$123,971

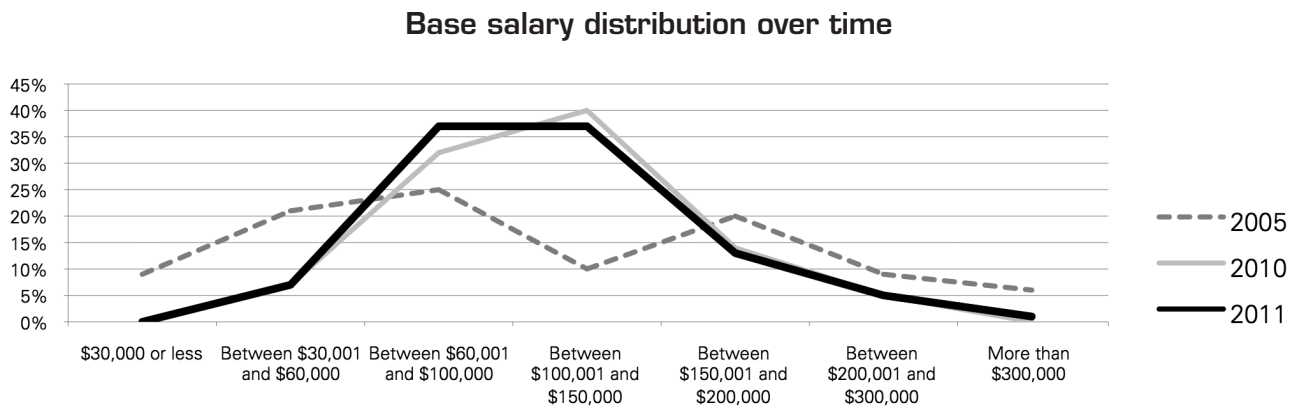
Average privacy base salary



Salary distribution remains largely unchanged. The drop in average 2010 salaries was partially explained by a proportion of relatively lower paid respondents to the survey. This year, the proportions stayed constant, so the gains in the average base salary probably reflect true gains for a broad distribution of employees, despite the ongoing sluggish world economy.

Table 32: Salary range distribution

Salary Range	2005	2010	2011
\$30,000 or less	9%	0%	0%
Between \$30,001 and \$60,000	21%	7%	7%
Between \$60,001 and \$100,000	25%	32%	37%
Between \$100,001 and \$150,000	10%	40%	37%
Between \$150,001 and \$200,000	20%	14%	13%
Between \$200,001 and \$300,000	9%	5%	5%
More than \$300,000	6%	0%	1%



Wide variance in compensation by department. The most highly compensating private-sector departments are those that typically employ attorneys and MBAs, with marketing (\$154,654), ethics and corporate responsibility (\$153,188), and legal (\$151,396) leading the pack. Meanwhile, the most highly compensated government privacy pros are located in standalone privacy offices (\$105,630), IT (\$104,432) and risk management (\$103,600). A side-by-side comparison shows, unsurprisingly, that privacy pros make substantially more than their government peers, with government employees in ethics and legal departments standing to make the most from a switch to the private sector.

Table 33: Salary by department where the privacy function resides

Residing Department	Average salary, corporate in-house	Number	Average salary, government in-house	Number
Audit & Quality Assurance	\$107,456	6	-	0
Business Unit	\$110,200	10	\$100,935	8
Compliance	\$117,005	215	\$96,533	25
Ethics & Corporate Responsibility	\$153,188	8	\$97,000	★
Human Resources	\$119,328	7	\$101,500	★
Information Security	\$116,272	53	\$94,960	32
Information Technology	\$108,120	19	\$104,432	26
Legal	\$151,396	174	\$95,229	21
Marketing	\$154,654	13	\$67,400	★
Operations	\$107,489	18	\$102,316	6
Risk Management	\$133,311	47	\$103,600	5
It is its own function reporting directly to the top executive or board	\$94,150	23	\$105,630	34
We do not have a privacy function	\$102,000	★	-	0
Other (please specify)	-	0	\$117,070	25

★fewer than five respondents

Regional and Sectoral Salary Breakdowns

Salary by region. How much does the region of the organization affect the compensation of privacy professionals? Our survey results reveal that region affects salary quite a bit. Among the three regions with a significant number of respondents, those working for European-headquartered firms earned the most (\$133,026), followed by firms based in the U.S. (\$126,761) and Canada (\$94,698). That said, the location of the respondent—which can often vary from the headquarters of the respondents’ employers—had a different impact on average salary. Privacy pros based in the U.S. earned the top average salary (\$127,426), followed by those in Europe (\$114,947) and Canada (\$95,909).

Within the U.S., salary varied greatly by region. Privacy pros in the Northeast—where most are concentrated—had the top average salary of all regions in the U.S. and worldwide at \$147,136—while the U.S. South topped only Canada among regions with a significant number of respondents.

Table 34: Base salary by region

Region	Average salary by location of respondent	Number	Average salary by location of respondents’ headquarters	Number
United States	\$127,426	870	\$126,761	846
U.S.-Northeast	\$147,136	322	na	na
U.S.-South	\$108,293	191	na	na
U.S.-Upper Midwest	\$113,410	172	na	na
U.S. -West	\$126,090	182	na	na
Canada	\$95,909	107	\$94,698	106
Europe	\$114,947	30	\$133,026	55
Asia-Pacific	\$84,574	*	\$159,000	5
Latin America	\$231,667	*	\$101,000	*
Middle East & Africa	\$149,375	*	\$96,750	*

*fewer than five respondents

Utilities, business services and telecommunications rank highest. In this year's survey, we offered a more detailed industry list in order to break down average base salary to a finer degree. Among the sectors represented by a meaningful sample size of respondents to the survey, utilities (\$165,000), business services and supplies (\$160,777) and telecommunications (\$160,197) are paying the most. On the lower end of the spectrum are government and nonprofits, both of which earned about \$100,000, on average, in wages.

Table 35: Average base salary by sector

Industry Sector	Average base salary	Number reporting
Aerospace & Defense	\$141,753	15
Banking	\$120,571	94
Business Services & Supplies	\$160,777	66
Capital Goods	\$102,000	★
Chemicals	\$186,500	★
Conglomerates (multiple sectors)	\$141,707	29
Construction	–	★
Consumer Durables	\$119,375	★
Diversified Financials	\$132,638	36
Drugs & Biotechnology	\$136,165	33
Education & Academia	\$115,385	41
Food, Drink & Tobacco	\$130,625	★
Food Markets	\$115,000	★
Government	\$98,279	204
Healthcare Equipment & Services	\$106,902	85
Hotels, Restaurants & Leisure	\$134,455	11
Household & Personal Products	\$214,000	★
Insurance	\$111,751	101
Materials	–	★
Media	\$154,466	25
Nonprofit	\$103,420	29
Oil & Gas Operations	\$154,667	6
Retailing	\$122,046	26
Semiconductors	\$128,880	7
Software & Services	\$129,794	98
Technology Hardware & Equipment	\$117,861	29
Telecommunication Services	\$160,197	35
Trading Companies	\$177,500	★
Transportation	\$120,333	6
Utilities	\$165,000	9

★fewer than five respondents

Experience and Qualification Salary Measures

High-level executives earn more, but not much more. Privacy executives with at most one level of management between them and the chief executive made only about \$5,000 more in annual salary, as a group, than the average salary for all employees involved in privacy work. In a handful of sectors—including conglomerates, hotels, media, semiconductors, trading companies, and utilities—the average base pay of privacy executives exceeded \$175,000, but the small amount of data points making up these averages prevents us from drawing firm conclusions.

Table 36: Average base salary by sector, privacy executives

Industry Sector	Average base salary	Number reporting
Aerospace & Defense	\$163,575	★
Banking	\$127,083	12
Business Services & Supplies	\$140,264	11
Capital Goods	\$102,000	★
Chemicals	\$148,000	★
Conglomerates (multiple sectors)	\$238,000	6
Construction	-	★
Consumer Durables	-	★
Diversified Financials	\$137,429	7
Drugs & Biotechnology	\$142,444	9
Education & Academia	\$150,292	18
Food, Drink & Tobacco	\$139,000	★
Food Markets	-	★
Government	\$97,021	58
Healthcare Equipment & Services	\$105,293	32
Hotels, Restaurants & Leisure	\$275,000	★
Household & Personal Products	-	★
Insurance	\$142,355	22
Materials	-	★
Media	\$188,556	9
Nonprofit	\$110,787	13
Oil & Gas Operations	-	★
Retailing	\$151,925	★
Semiconductors	\$190,000	★
Software & Services	\$141,222	18
Technology Hardware & Equipment	\$125,000	★
Telecommunication Services	\$144,424	★
Trading Companies	\$240,000	★
Transportation	-	★
Utilities	\$187,750	★

★fewer than five respondents

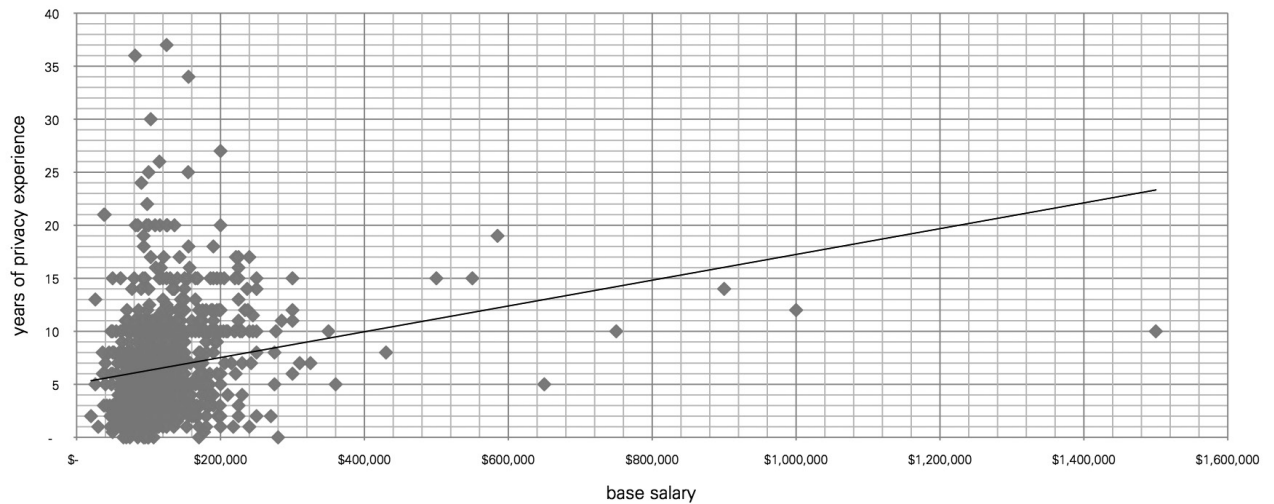
Wide distribution of salary by degree and certification. For the first time in this year's survey, we took a detailed look at the correlation between different educational achievements and average base pay. The degrees generating the top average base salaries were predictable: JD (\$168,470), PhD (\$140,691), MBA (\$131,269), MA/MS (\$125,079) and BA/BS (\$124,353). However, it was surprising that the 23 respondents with the MIS degree earned less (\$114,898) than the average bachelor's degree holder. Even more surprising was the most common certification among respondents—the Certified Business Continuity Planner—averaging \$157,153 in base pay.

Table 37: Salary by degree and certification

Degree or certification	Average salary, all respondents	Number
Juris Doctor (JD)	\$168,470	250
Certified Business Continuity Professional (CBCP)	\$157,153	12
Certified Public Accountant (CPA)	\$146,180	15
Doctorate degree (PhD)	\$140,691	22
Certified Records Manager (CRM)	\$135,045	11
Master of Business Administration (MBA)	\$131,269	144
Project Management Professional (PMP)	\$130,722	19
Certified Information Security Manager (CISM)	\$125,750	67
Master's degree (MA, MS)	\$125,079	200
Certified Information Systems Security Professional (CISSP)	\$124,460	139
Bachelors degree or equivalent (BA, BS)	\$124,353	789
Certified Information Privacy Professional (CIPP)	\$120,029	631
Certified Compliance and Ethics Professional (CCEP)	\$119,818	11
Certified Information Systems Auditor (CISA)	\$119,201	84
Master of Information Systems (MIS)	\$114,898	23
Other	\$114,814	181
Registered Nurse (RN)	\$113,509	11

There is a positive correlation between the number of years of privacy experience and base pay, but the scatter plot below shows a wide variance in the relationship between those two variables.

Years of privacy experience and base salary



Privacy Specialties

Industry Sector

The IAPP Privacy Professional's Role, Function and Salary Survey was designed originally for the in-house corporate or government privacy professional. These roles were the origin of the profession and continue to be the focal point for topics of importance for all privacy professionals. But as a sign of the profession's growing maturity and impact, more privacy specialties outside the traditional in-house function have materialized. This year's study marks the first time, to our knowledge, that an assessment has been made of the privacy professional as viewed from the perspective of a cross-section of specialty roles. Among our key findings:

- Information Technology (IT) privacy pros inhabit a more junior role than their traditional privacy counterparts; just seven percent have one or fewer levels between them and their top executive, compared to 31 percent from the rest of the survey sample.
- One-third of IT privacy pros have the CIPP/IT certification, and their average salary of \$116,486 was roughly \$5,000 more than their non-CIPP/IT peers.
- IT privacy pros only spend about half of their time on privacy and tend toward tactical rather than strategic tasks. On average, they spend 57 percent of their time on privacy, and one-third of that time is dedicated to assisting with audits, assessments and gap remediation.
- Only 26 percent of IT privacy pros ranked their organizations in the top two levels of privacy maturity, compared to 48 percent of the rest of the survey sample.
- The typical privacy advisor bills the equivalent of four days per week to clients, 55 percent of which is dedicated to privacy and billed at a rate of \$290 per hour.
- Privacy advisors are active in most sectors represented by survey respondents. Their average bill rates are in the business services and supplies (\$274) and banking (\$260) sectors and lowest in healthcare equipment and services (\$243) and government (\$224).

- Privacy advisors garner a disproportionate share of their revenues from the capital goods sector, which accounts for 11 percent of total reported advisory revenue but only three percent of all respondents.
- The top services privacy advisors plan to offer during the next two years include privacy audits and assessments (84%) and privacy program development (82%), while marketing support (31%), M&A support (23%) and litigation (20%) rank lowest on their planned offerings.
- Just 14 respondents classified themselves as vendors of privacy products. Compared to privacy advisors, privacy vendors were over 20 percentage points more prevalent in the education and academia and software & services sectors and less prevalent in the banking and telecommunications sectors.
- Seven respondents classified themselves as dedicated to researching, writing about or teaching privacy, and their top two areas of concern for 2011 are data disclosure to third parties and privacy and society.
- Of the eight survey respondents who classified themselves as privacy advocates, seven listed the security of personal data as their top agenda item for 2011.
- Fifteen respondents were responsible for enforcing privacy regulations in their jurisdictions, with the top priority for 2011 being limiting personal data uses and retention.
- The 40 respondents in the small-business category, despite their smaller size, shared the same top two concerns as their counterparts from larger organizations: complying with privacy regulations and avoiding data breaches.
- When asked about the state of privacy protection worldwide, there was broad consensus across all survey segments that there are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward more protection.

IT Professionals

IT professionals inhabit a more junior role than their traditional privacy counterparts. A cohort of IT professionals has migrated to full-time privacy work within the IT department. Nearly three-fourths are based in the information security function, but they occupy a relatively more junior role than their traditional privacy counterparts. Just seven percent have one or fewer levels between them and their top executive, compared to 31 percent from the rest of the survey sample. Similarly, 36 percent have four or more layers between them and their top executive, compared with 27 percent from the rest of the survey. The IT respondents have benefitted from the CIPP/IT certification. Of the third of the IT sample that gained the CIPP/IT, the average salary is \$116,486, roughly \$5,000 more than their non-CIPP/IT peers.

Table 38: IT Privacy roles

Role	Number	Share
Information security	50	71%
IT process improvement	7	10%
Office of the CIO	7	10%
Application development	5	7%
Database administration	1	1%
Network & infrastructure	0	0%
Data center operations	0	0%
Business continuity & disaster recovery	0	0%

Table 39: Relative seniority of IT professionals surveyed

Seniority Level	IT share	Remaining sample share	Difference
0 (You are a “C-level” executive who reports directly to the top executive)	0%	6%	-6
1 (Typically a Vice President who reports to someone who reports to the top executive)	7%	25%	-18
2 (Typically a Director or Vice President)	24%	22%	+2
3 (Typically a Manager or Director)	33%	20%	+13
4 (Typically a Senior Analyst or Manager)	19%	14%	+5
5 (Typically an Analyst or Senior Analyst)	13%	8%	+5
5+	4%	5%	-1

IT privacy pros are the arms and legs of the privacy office. How are IT privacy pros advancing the privacy agenda? It appears from the survey they are conducting functional rather than strategic work and on a part-time basis. On average, they spend 57 percent of their time on privacy, and one-third of that time is dedicated to assisting with audits, assessments and gap remediation. Looking ahead to 2011, IT privacy pros are more likely than their other privacy peers to be working on process documentation and improvement; data inventorying and mapping; data-loss prevention and monitoring; and governance, risk and compliance technology implementations.

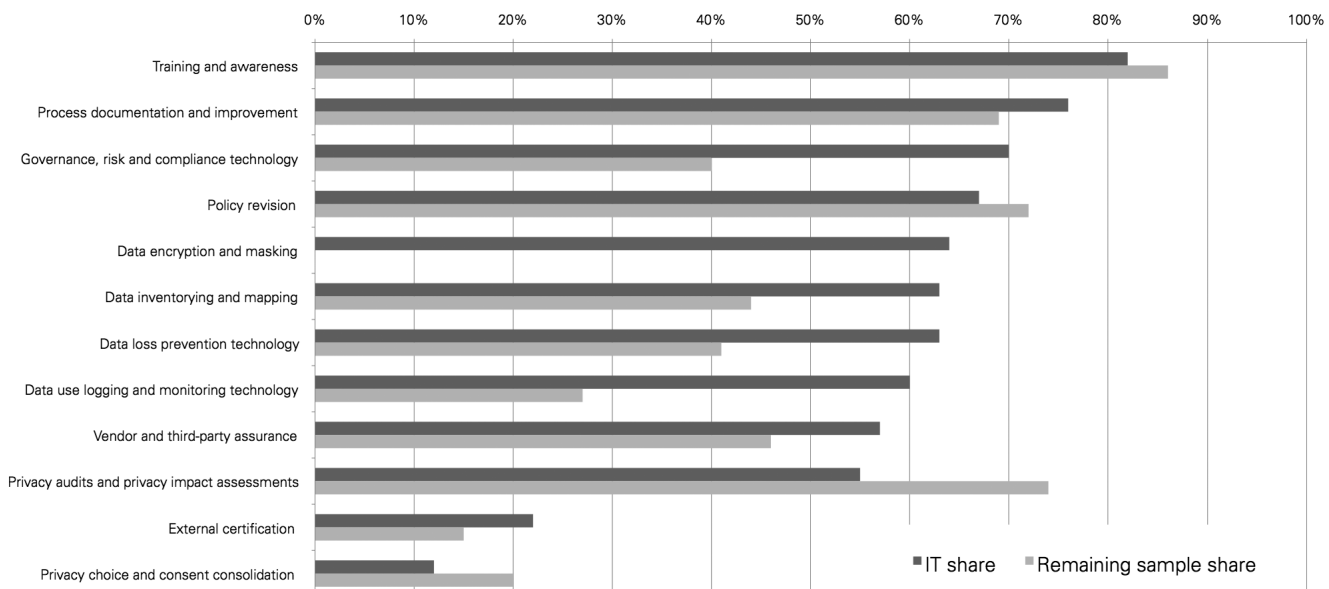
Table 40: Time allocation, IT professionals

Activity	Average share of time
Activities not related to privacy	43%
Reporting to management or privacy stakeholders	11%
Remediating our IT systems to close audit gaps	10%
Assisting with third-party audits of our IT environment	9%
Assisting with internal audits of our IT environment	9%
Responding to data incidents	7%
Assisting with audits of our service providers	6%
Performing data inventories	5%

Table 41: IT Project priorities versus other respondents

Project	IT respondents, number	IT share	Remaining sample number	Remaining sample share	Difference
Training and awareness	55	82%	601	86%	-4%
Process documentation and improvement	51	76%	483	69%	+7%
Governance, risk and compliance technology	47	70%	280	40%	+30%
Policy revision	45	67%	503	72%	-5%
Data encryption and masking	43	64%	NA	NA	0%
Data inventorying and mapping	42	63%	306	44%	+19%
Data loss prevention technology	42	63%	288	41%	+22%
Data use logging and monitoring technology	40	60%	187	27%	+33%
Vendor and third-party assurance	38	57%	322	46%	+11%
Privacy audits and privacy impact assessments	37	55%	516	74%	-19%
External certification	15	22%	107	15%	+7%
Privacy choice and consent consolidation	8	12%	142	20%	-8%

2011 project priorities, IT versus other respondents



IT privacy pros more sanguine about privacy maturity. Do IT professionals have a deeper understanding of the ground truth than other privacy pros? Their views of their organizations' privacy maturity suggest that. Only 26 percent of IT privacy pros ranked their organizations in the top two levels of privacy maturity, compared to 48 percent of the rest of the survey sample.

Table 42: Relative privacy maturity of IT professionals' organizations versus others

Privacy Maturity Level	IT share	Remaining sample share	Difference
0 - Nonexistent	0%	0%	0
1 - Initial	19%	7%	+12
2 - Repeatable	26%	16%	10
3 - Defined	28%	28%	0
4 - Managed	19%	35%	-16
5 - Optimized	7%	13%	-6

Privacy Advisors

Privacy advising is a part-time vocation. The attorneys, consultants and auditors—referred to collectively as “advisors”—that organizations hire to assist them with their privacy programs are most commonly focusing on privacy as a primary but not exclusive subject matter. The typical privacy advisor bills the equivalent of four days per week to clients, 55 percent of which is dedicated to privacy and billed at a rate of \$290 per hour.

Table 43: Rates and hours billed by external privacy advisors

	Average	Number
Days per week billed to clients	4	86
Share related to privacy	55%	83
Typical hourly rate	\$290	61

Table 44: Privacy advisors' annual level of focus on privacy

Hours providing privacy advisory services	Number	Share
0-400 (about 1 day per week)	9	10%
401-800 (about 2 days per week)	3	3%
801-1,200 hours (about 3 days per week)	10	12%
1,201-1,600 hours (about 4 days per week)	16	19%
1,601-2,000 hours (about 5 days per week)	40	47%
2,001-2,400 hours (about 6 days per week)	8	9%

Privacy advisor rates vary widely by sector. Privacy advisors are active in most sectors represented by the survey sample. Perhaps owing more to low sample sizes than to anything else, the average rate they command in each sector varies from a high of \$890 in conglomerates to a low of \$100 in aerospace and defense. Among sectors with more than five reporting advisors, the variance is tighter, ranging from business services and supplies (\$274) and banking (\$260) on the top end to healthcare equipment and services (\$243) and government (\$224) on the lower end. Privacy advisors garner a disproportionate share of revenues from the capital goods sector, which accounts for 11 percent of total reported advisory revenue but only three percent of all respondents. Conversely, they are most underrepresented in the software and services sector, which accounts for 10 percent of survey respondents but only four percent of advisory revenue.

Table 45: Privacy advisor rates by sector

Industry sector	Average billing rate	Share of all advisor revenue earned in this sector**	Number
Aerospace & Defense	\$100	0%	★
Banking	\$260	14%	11
Business Services & Supplies	\$274	8%	7
Capital Goods	-	0%	0
Chemicals	-	0%	0
Conglomerates (multiple sectors)	\$890	11%	★
Construction	-	0%	0
Consumer Durables	-	0%	0
Diversified Financials	\$273	1%	★
Drugs & Biotechnology	\$450	3%	★
Education & Academia	-	0%	0
Food, Drink & Tobacco	-	1%	0
Food Markets	\$200	1%	★
Government	\$224	21%	12
Healthcare Equipment & Services	\$243	9%	8
Hotels, Restaurants & Leisure	\$465	1%	★
Household & Personal Products	\$500	3%	★
Insurance	\$415	7%	★
Materials	-	0%	0
Media	-	1%	0
Nonprofit	\$225	1%	★
Oil & Gas Operations	-	0%	0
Retailing	\$350	4%	★
Semiconductors	-	0%	0
Software & Services	\$177	4%	★
Technology Hardware & Equipment	\$525	2%	★
Telecommunication Services	\$272	6%	★
Trading Companies	-	0%	0
Transportation	-	0%	0
Utilities	-	1%	0

★fewer than five respondents

**Based on 63 respondents, working 1,009 privacy hours and earning \$311,000 in revenues in a week

Table 46: Sectoral concentration of privacy advisors versus in-house privacy pros

Sectors served by external privacy advisors, 2011	Privacy advisors revenue share from this sector	Share of all respondents from this sector	Difference
Aerospace & Defense	0%	1%	+1%
Banking	14%	10%	-4%
Diversified Financials	8%	7%	-1%
Insurance	0%	0%	0%
Business Services & Supplies	0%	0%	0%
Capital Goods	11%	3%	-8%
Chemicals	0%	0%	0%
Conglomerates	0%	0%	0%
Construction	1%	3%	+2%
Consumer Durables	3%	4%	+1%
Drugs & Biotechnology	0%	4%	+4%
Education & Academia	1%	0%	-1%
Food, Drink & Tobacco	1%	0%	-1%
Food Markets	21%	21%	0%
Government	9%	9%	0%
Healthcare Equipment & Services	1%	1%	0%
Hotels, Restaurants & Leisure	3%	0%	-3%
Household & Personal Products	7%	10%	3%
Materials	0%	0%	0%
Media	1%	2%	+1%
Nonprofits	1%	3%	+2%
Oil & Gas Operations	0%	0%	0%
Retailing	4%	3%	-1%
Semiconductors	0%	1%	+1%
Software & Services	4%	10%	+6%
Technology Hardware & Equipment	2%	3%	+1%
Telecommunication Services	6%	3%	-3%
Trading Companies	0%	0%	0%
Transportation	0%	1%	+1%
Utilities	1%	1%	0%

Privacy advisors bullish on their future. In spite of the slow growth in many economies where privacy is regulated, privacy advisors are optimistic. Ninety percent see the market for their services expanding over the next two years instead of contracting. The top services privacy advisors plan to offer during that time include privacy audits and assessments (84 percent) and privacy program development (82 percent), while marketing support (31 percent), M&A support (23 percent) and litigation (20 percent) rank lowest on their planned offerings.

Table 47: Privacy advisor services offered and planned *

Planned service to offer	Current offerings
Privacy audits and assessments	84%
Privacy program development	82%
Documenting privacy policies and processes	78%
Interpretation of privacy regulations	75%
Employee awareness and training	66%
Data breach response	53%
Data inventorying & mapping	48%
Crossborder data transfer	48%
IT transactions	45%
Outsourcing and third-party assurance	43%
Marketing support	31%
Mergers and acquisitions	23%
Privacy litigation	20%

**Respondents could select more than one answer.*

Table 48: Privacy advisor views of the privacy advisory market in next two years

View held	Number	Share
Grow more than 10%	37	43%
Grow between 0 and 10%	41	47%
Stay the same	7	8%
Contract between 0 and 10%	1	1%
Contract more than 10%	1	1%

Privacy advisors know why they're hired. Privacy advisors share the view of their corporate peers for why executives fund the privacy budgets—to meet regulatory compliance obligations and to reduce the risk of data breach notification. Within that backdrop, three quarters of privacy advisors say their clients hire them to get answers and guidance from experiences that they haven't had.

Table 49: Privacy advisor views of why executives fund the privacy function * *

Executive reasons for funding the privacy function	Views of internal privacy pros	Views of external privacy advisors	Difference
To meet regulatory compliance obligations	97%	97%	0%
To reduce the risk of data breach notification and publicized data breaches	83%	73%	-10%
To enhance the organization's brand and public trust	70%	49%	-21%
To meet the expectations of business clients and partners	69%	*	*
To reduce the risk of employee and consumer lawsuits	56%	42%	-14%
To enable global operations and entry into new markets	35%	28%	-7%
To increase the value and quality of data	33%	15%	-18%
To provide a competitive differentiator	31%	25%	-6%
To increase revenues from cross-selling and direct marketing	20%	10%	-10%

* Privacy advisors inadvertently were not provided the option "To meet the expectations of business clients and partners."

** Respondents could choose more than one answer.

Table 50: Privacy advisor views of why clients engage them *

View	Number	Share
Obtain expert information	68	78%
Gain access to new methodologies	45	52%
Receive guidance on experiences they haven't had	67	77%
Temporarily increase staff to accomplish tasks that outstrip internal capabilities	38	44%
Receive services that only an outside entity can provide	35	40%

* Respondents could choose more than one answer.

Privacy Product Vendors

Privacy products are an untapped market. Just 14 survey respondents classified themselves as vendors of privacy products such as policy or training software. Of those 14, 93 percent were small businesses generating \$25 million or less in annual revenues. Compared to privacy advisors, privacy vendors were over 20 percentage points more prevalent in the education and academia and software and services sectors and less prevalent in the banking and telecommunications sectors.

Table 51: Size of vendor firms, by revenue *

Size	Number	Share
Less than \$1 million	6	43%
\$1 million to \$25 million	7	50%
\$25 million to \$100 million	1	7%
Over \$100 million	0	0%

* Respondents could make one selection.

Table 52: Sectors served by privacy product vendors

Industry sector	Privacy vendors	Privacy advisors	Difference
Aerospace & Defense	27%	11%	+16%
Banking	27%	36%	-9%
Diversified Financials	40%	31%	+9%
Insurance	20%	5%	+15%
Business Services & Supplies	13%	3%	+10%
Capital Goods	20%	9%	+11%
Chemicals	13%	2%	+11%
Conglomerates	20%	10%	+10%
Construction	20%	8%	+12%
Consumer Durables	27%	20%	+7%
Drugs & Biotechnology	33%	15%	+18%
Education & Academia	27%	3%	+24%
Food, Drink & Tobacco	13%	11%	+2%
Food Markets	53%	43%	+10%
Government	40%	33%	+7%
Healthcare Equipment & Services	27%	18%	+9%
Hotels, Restaurants & Leisure	13%	9%	+4%
Household & Personal Products	33%	23%	+10%
Materials	13%	2%	+11%
Media	27%	23%	+4%
Nonprofits	20%	18%	+2%
Oil & Gas Operations	13%	6%	+7%
Retailing	27%	24%	+3%
Semiconductors	20%	1%	+19%
Software & Services	53%	31%	+22%
Technology Hardware & Equipment	40%	23%	+17%
Telecommunication Services	20%	24%	-4%
Trading Companies	13%	2%	+11%
Transportation	13%	6%	+7%
Utilities	27%	11%	+16%

Table 53: Primary privacy vendor service areas*

Vendor services offered	Current offerings	Two years from now	Difference
Privacy Management	17%	21%	+4%
Privacy Notices	13%	0%	-13%
Privacy Choices	4%	7%	+3%
Limiting Personal Data Collection	6%	7%	+1%
Limiting Personal Data Uses	8%	0%	-8%
Limiting Personal Data Retention	8%	0%	-8%
Data Subject Access	2%	0%	-2%
Quality of Personal Data	4%	7%	+3%
Data Disclosure to Third Parties	4%	7%	+3%
Security of Personal Data	13%	21%	+8%
Privacy Monitoring and Enforcement	15%	29%	+14%
Privacy and Society	6%	0%	-6%

* Respondents could choose one answer.

Privacy Researchers, Writers and Academics

Privacy research is another emerging niche in the profession. Fewer than a dozen respondents classified themselves as being dedicated to researching, writing about or teaching privacy. Predictably, this small community is interested in the full spectrum of privacy topics, with data disclosure to third parties and privacy and society ranking at the top of the 2011 agenda for 71 percent of them.

Table 54: 2011 Primary research agenda areas for researchers, writers and academics*

Research area	Number	Share
Data Disclosure to Third Parties	5	71%
Privacy and Society	5	71%
Privacy Management	4	57%
Security of Personal Data	4	57%
Privacy Monitoring and Enforcement	4	57%
Privacy Notices	3	43%
Privacy Choices	3	43%
Limiting Personal Data Uses	3	43%
Limiting Personal Data Collection	2	29%
Limiting Personal Data Retention	2	29%
Data Subject Access	2	29%
Quality of Personal Data	2	29%

* Respondents could choose more than one answer.

Privacy Advocates

Privacy advocates want to see better security. Those who make their living advocating for better privacy protections in governments and the private sector represent the smallest segment of survey respondents. Of the eight survey respondents who classified themselves as privacy advocates, seven listed the security of personal data as their top agenda item for 2011.

Table 55: 2011 Privacy advocate agenda issues *

Issue	Number	Share
Security of Personal Data	7	88%
Privacy Management	3	38%
Privacy Monitoring and Enforcement	3	38%
Privacy Notices	2	25%
Limiting Personal Data Collection	2	25%
Privacy and Society	2	25%
Limiting Personal Data Uses	1	13%
Limiting Personal Data Retention	1	13%
Quality of Personal Data	1	13%
Privacy Choices	0	0%
Data Subject Access	0	0%
Data Disclosure to Third Parties	0	0%

* Respondents could choose more than one answer.

Privacy Regulators

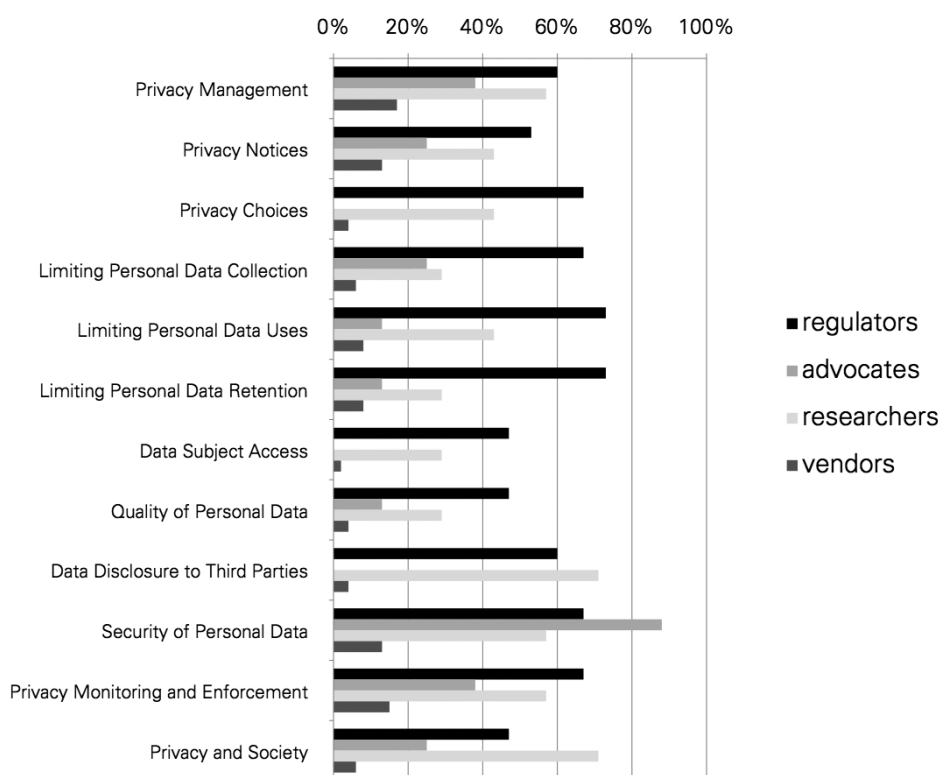
Privacy regulators plan to move on multiple fronts. Fifteen respondents are responsible for enforcing privacy regulations in their jurisdictions. While limiting personal data uses and retention was the top priority for 11 of them, no fewer than seven regulators planned to take action on any one of the 12 privacy principles listed as options. This suggests no data practice will be safe from scrutiny in 2011.

Table 56: 2011 Privacy regulator agenda issues *

Issue	Number	Share
Limiting Personal Data Uses	11	73%
Limiting Personal Data Retention	11	73%
Privacy Choices	10	67%
Limiting Personal Data Collection	10	67%
Security of Personal Data	10	67%
Privacy Monitoring and Enforcement	10	67%
Privacy Management	9	60%
Data Disclosure to Third Parties	9	60%
Privacy Notices	8	53%
Data Subject Access	7	47%
Quality of Personal Data	7	47%
Privacy and Society	7	47%

* Respondents could choose more than one answer.

2011 plans by privacy principle



Small Businesses

Privacy concerns are emerging within small businesses. About 40 respondents said the “small business” category best described their current role relative to the eight other choices. In spite of their smaller size, they shared the top two concerns as their counterparts from larger organizations: complying with privacy regulations and avoiding data breaches. How they meet these needs may differ, however. Privacy pros in small businesses first seek referrals from their employees and then look to local business associations for privacy support.

Table 57: Primary type of privacy support sought by small businesses*

Support sought	Number	Share
Understanding what the law requires us to do	11	28%
Understanding how to reduce the risk of a data breach	9	23%
Assistance with developing a privacy program	6	15%
Assistance with meeting the contractual requirements of our clients	7	18%
Answering our ad hoc questions about privacy	6	15%

* Respondents could choose one answer.

Table 58: Where small business seek their privacy support*

Source of support	Number	Share
Personal networks of our employees	7	58%
Local business associations	2	17%
Local business publications	0	0%
National professional associations	9	75%
Online searches	7	58%

* Respondents could choose more than one answer.

All Specialties

Table 59: Perceived worldwide state of privacy protection, views of different parts of the privacy profession

View	Private sector	Public sector	Privacy regulators	Privacy advisors	Privacy product vendors	IT pros	Privacy advocates	Privacy researchers & academics
No protection	1%	1%	0%	3%	0%	1%	0%	8%
Mostly no protection	10%	14%	0%	17%	14%	17%	25%	23%
Mixed, but trending toward less protection	15%	22%	41%	16%	29%	28%	0%	23%
Mixed, trending toward more protection	68%	59%	59%	63%	57%	53%	75%	38%
Mostly there is protection	5%	4%	0%	1%	0%	0%	0%	8%
Protection everywhere	1%	1%	0%	0%	0%	0%	0%	0%

When asked about the state of privacy protection worldwide, there was broad consensus across all survey segments that there are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward protection.

The language choices for the six levels as they appeared in the survey were:

- There is no meaningful protection of personal privacy anywhere in the world.
- There are some geographic areas or segments of society where privacy is sufficiently protected, but mostly there is no meaningful protection.
- There are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward less protection.
- There are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward more protection.
- There are only some geographic areas or segments of society where privacy is not sufficiently protected, but mostly there is meaningful protection.
- There is meaningful protection of personal privacy everywhere in the world.

Privacy Concerns for 2011

This year, for the first time, we polled respondents on their views of the most significant privacy concerns facing them in 2011. The answers reflect concerns about the risks of changing technologies and globalization; heightened data collection and sharing among the private and public sectors; increased and discordant regulation; and the public response to these rapid changes. Interestingly, these were the same drivers called out in last year's IAPP publication *A Call for Agility: The Future of the Privacy Professional*.

We asked privacy academics this question:

What is the most important unanswered question in privacy?

Among the answers we received:

- “When and if the U.S. will move to a comprehensive, EU-style federal information privacy statutory scheme.”
- “Will industry step up to self-regulation activities globally together?”
- “How important is the privacy of your personal information?”
- “What is the actual link between customer trust in an organization and its privacy policies?”
- “How do we measure privacy protections and risks?”

We asked privacy advocates this question:

What do you think is the biggest threat to privacy?

Among the answers we received:

- “Cloud technologies”
- “Lack of strong, two-factor authentication in cyberspace”
- “Incomplete contracts between covered entities and service providers”
- “Government”
- “Incompetence”
- “Lack of education of the general public”

We asked privacy regulators this question:

Besides resource constraints, what do you think is the biggest challenge to regulating privacy?

Among the answers we received:

- “Carefully monitoring the growing trend toward information sharing when the potential for abuses may be increasing”
- “Conflicting laws/regulations in different jurisdictions”
- “The insistence that national security interests trump privacy, rather than that these two things can work together”
- “Independence from agency influence”
- “Education and training”
- “Lack of public knowledge, and lack of knowledge within the health professions”

III. Survey Methodology

The IAPP sponsored and initiated this survey of its membership in December 2010 to generate the results detailed in this report. This section explains the survey objectives, questions, delivery and sample and outlines the limitations of the survey.

Survey Objectives

Following the publication in March 2010 of our landmark report *A Call for Agility: The Next Generation Privacy Professional*—which projected a dramatic growth in the privacy profession in the coming decade—this year we decided to make major improvements in our annual member salary survey. Our objective was to prepare a solid baseline for years to come. We defined our research goals with the following baseline questions from past surveys:

- How do privacy professionals allocate their time across different responsibilities?
- What career paths are privacy professionals pursuing?
- In which departments are privacy offices situated?
- How far from the top executive are privacy leaders positioned?
- What is the compensation level of privacy professionals by sector, region, organization size, reporting line, certification, level of organizational privacy maturity and other variables?

This year, we endeavored to increase the value of the survey by adding the following questions:

- How do privacy professionals self-assess their level of expertise?
- What are the average funding and staffing levels of privacy offices?
- What are the key drivers of the agendas of privacy offices?
- What learning and growth opportunities do privacy professionals have support for?
- Where do government privacy offices find talent?
- What are the 2011 agendas for privacy regulators, privacy researchers and academics and privacy advocates?
- What are the average rates that privacy lawyers and consultants are charging?
- Where do privacy vendors see the market heading in 2011?
- How are IT professionals integrating privacy into their work?
- What are the career paths of the most successful privacy professionals?

Survey Questions

IAPP staff developed a first draft of the 2011 survey in November 2010, building upon questions from previous IAPP salary surveys. Experts in the field reviewed this draft and suggested improvements, which IAPP staff then incorporated into the final version.

Among the proposals gathered from external review was the suggestion to provide custom, tailored sections corresponding to the major branches of the profession that have emerged over the past decade. As a result, this year the survey contained a core set of questions followed by nine different branches of supplementary questions. Respondents were presented with a particular branch of questioning based on their responses to a question about their current position. By comparison, the 2010 survey contained a single branch of 23 items.

The survey was developed with the goal of collecting information from privacy practitioners in a convenient fashion. In an attempt to maximize completion rates, we designed it to be completed in about 10 minutes. The actual average measured time to take the 2011 survey was 12 minutes. We also sought to track trends and key parameters and therefore maintained at least a subset of questions from previous surveys.

To maintain confidentiality, the survey instrument did not request individual or company-identifying information. The questions and the multiple-choice answers provided to the respondents follow.

Survey Limitations

There are inherent limitations to survey research that need to be carefully considered before drawing conclusions from sample findings. The following items are specific limitations that are relevant to this study.

- The current findings are based on a sample of survey returns. It is always possible that individuals who did not participate are substantially different in terms of compensation and other job-related functions from those who completed the instrument.
- Financial services, government and healthcare are the largest industry groups within the IAPP today. Hence, while other industry concentrations are represented, the IAPP membership list is skewed toward highly regulated organizations.
- The IAPP membership is located primarily in North American-based organizations. While European and Asia-Pacific members exist within the association today and are growing as a total share, results of this study cannot yet be generalized to other parts of the world.

Change in salary questions. This year, we removed the option to provide salary ranges, asking instead for an exact salary number. Our goal was to improve the accuracy of salary-based comparisons with other variables in the survey, providing members and their HR departments a richer data set from which to base market surveys for the purpose of salary adjustments.

Unmeasured Demographics. To keep the survey concise and focused, we decided to omit other normatively important variables from our analysis. The extent to which omitted variables might explain salary cannot be estimated at this time.

Self-Reported Results. The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Survey Delivery

The IAPP fielded the survey via e-mail to its membership (approximately 7,500 members) initially on December 10, 2010. The survey remained open until January 10, 2011. The e-mail included a link to the survey questions displayed via an online survey tool. Respondents answered the survey by reading the questions and clicking their responses via radio buttons or entering text into an open text box and finished by clicking a submit button.

The IAPP received 1,052 substantially completed and 955 fully completed responses, a response rate of 12.7 percent. When the survey closed, the IAPP downloaded the results from the online survey tool.

Survey Sample

The target sample for the survey was IAPP members with a current e-mail address on record. IAPP members are those who were up to date with either their individual or corporate membership dues for 2010 at the time of fielding. The table below details the sample and delivery statistics.

Survey e-mails sent	7,500
Surveys started	1,345
Surveys substantially completed	1,052 (14.0% of contacted IAPP members)
Surveys fully completed	955 (12.7% of contacted IAPP members)
Average time to complete survey	12 minutes

IV. Appendix: Survey Questions

1. In what country or region are you primarily based?

- a. United States
- b. Canada
- c. Latin America
- d. Europe
- e. Africa
- f. Middle East
- g. Asia
- h. Australia/New Zealand

2. Which region of the United States are you based in?

- a. Northeast (CT, DC, DE, MA, MD, ME, NH, NJ, NY, RI, VT)
- b. South (AL, AR, FL, GA, KY, LA, MS, NC, OK, SC, TN, TX, VA, WV)
- c. Upper Midwest (IA, IL, IN, KS, MI, MN, MO, ND, NE, OH, SD, WI)
- d. West (AK, AZ, CA, CO, ID, HI, MT, NM, NV, OR, UT, WA, WY)

3. What is the primary location of your organization's headquarters?

- a. United States
- b. Canada
- c. Latin America
- d. Europe
- e. Africa
- f. Middle East
- g. Asia
- h. Australia/New Zealand

4. Your organization has employees located in:(check all that apply)

- a. United States
- b. Canada
- c. Latin America
- d. Europe
- e. Africa
- f. Middle East
- g. Asia
- h. Australia/New Zealand

5. What is the total number of employees in your organization?

- a. Fewer than 250 employees
- b. 250 to 1,000 employees
- c. 1,001 to 5,000 employees
- d. 5,001 to 25,000 employees
- e. 25,001 to 75,000 employees
- f. More than 75,000 employees

6. Which sector listed below best describes how your company would be classified?

- a. Aerospace & Defense
- b. Banking
- c. Business Services & Supplies
- d. Capital Goods
- e. Chemicals
- f. Conglomerates (multiple sectors)
- g. Construction
- h. Consumer Durables
- i. Diversified Financials
- j. Drugs & Biotechnology
- k. Education & Academia
- l. Food, Drink & Tobacco
- m. Food Markets
- n. Government
- o. Healthcare Equipment & Services
- p. Hotels, Restaurants & Leisure
- q. Household & Personal Products
- r. Insurance
- s. Materials
- t. Media
- u. Nonprofit
- v. Oil & Gas Operations
- w. Retailing
- x. Semiconductors
- y. Software & Services
- z. Technology Hardware & Equipment
- aa. Telecommunication Services
- bb. Trading Companies
- cc. Transportation
- dd. Utilities

7. What are your total years of business experience?

8. What are your total years of privacy experience?

9. Which degrees and certifications do you have? (Check all that apply.)

- a. Bachelors degree or equivalent (BA, BS)
- b. Masters degree (MA, MS)
- c. Master of Business Administration (MBA)
- d. Master of Information Systems (MIS)
- e. Doctorate degree (PhD)
- f. Juris Doctor (JD)
- g. Nurse (RN or LPN)
- h. Certified Public Accountant (CPA)
- i. CIPP
- j. CISSP
- k. CISM
- l. CISA
- m. CRM
- n. CBCP
- o. Other

10. What is your current base salary expressed in U.S. dollars?

11. In the past year, how much did you earn in bonuses, expressed in U.S. dollars?

12. On the following scale, how do you rate your own privacy experience and expertise?

- a. 1 – I am new to privacy.
- b. 2 – I can fulfill some of the privacy needs of our organization very well.
- c. 3 – I have the knowledge, skills and experience to manage all aspects of our organization's privacy needs.
- d. 4 – I have the knowledge, skills and experience to lead a privacy function or privacy practice in a regulated industry (ex: healthcare, finance, government, telecom) and regulated jurisdiction (ex: Europe, Canada, U.S., Australia, Japan).
- e. 5 – I have the knowledge, skills and experience to lead a privacy function of a large multinational in any type of industry or the privacy practice of a large advisory firm.

13. On the following scale, how do you rate the current state of privacy protection worldwide?

- a. 0 – There is no meaningful protection of personal privacy anywhere in the world.
- b. 1 – There are some geographic areas or segments of society where privacy is sufficiently protected, but mostly there is no meaningful protection.
- c. 2 – There are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward less protection.
- d. 3 – There are many geographic areas and segments of society where privacy is both protected and not protected, but the trend is toward more protection.
- e. 4 – There are only some geographic areas or segments of society where privacy is not sufficiently protected, but mostly there is meaningful protection.
- f. 5 – There is meaningful protection of personal privacy everywhere in the world.

14. How would you rate the current state of privacy protection in your industry?

- a. 0 – There is no meaningful protection of personal privacy in my industry.
- b. 1 – There are some organizations in my industry that protect privacy well, but mostly there is no meaningful protection.
- c. 2 – There are many organizations in my industry where privacy is both protected and not protected, but the trend is toward less protection.
- d. 3 – There are many organizations in my industry where privacy is both protected and not protected, but the trend is toward more protection.
- e. 4 – There are only some organizations in my industry where privacy is not sufficiently protected, but mostly there is meaningful protection.
- f. 5 – There is meaningful protection of personal privacy everywhere in my industry.

15. Which learning and growth activities are you authorized and planning to do in 2011? (Check all that apply.)

- a. Subscribe to a privacy information or news service
- b. Attend educational web conferences
- c. Attend local conferences or seminars
- d. Travel to conferences or seminars once per year
- e. Travel to conferences or seminars more than once per year
- f. Pursue a professional certification
- g. Get leadership training
- h. Get legal training
- i. Get technical training
- j. Get business training
- k. Pursue foreign-language training or an international assignment
- l. Participate in a temporary position change within my organization

16. Which of the following best describes the sector of the last job you held prior to your current position?

- a. Private sector in-house: I worked on the internal privacy needs of a company, nonprofit or university
- b. Government in-house: I worked on the internal privacy needs of a government agency
- c. Regulator: I worked for a government agency that monitors and enforces compliance with privacy regulations
- d. In-house IT: I worked on the internal information-technology needs of my organization
- e. Researcher or academic: I worked as a researcher, professor or writer on the topic of privacy
- f. External privacy advisor: I worked as a privacy consultant, attorney, barrister or auditor on the privacy needs of other organizations
- g. Vendor: I worked for a company that sells privacy related products or services
- h. Small business: I managed or worked for a small business that needs to manage customer privacy
- i. Privacy advocate: I raised public awareness about privacy, worked toward open debate on privacy risks and lobbied for privacy regulations
- j. Other (please specify)

17. Which of the following best describes your current employment? Pay special attention to this selection—it will determine which set of concluding survey questions you receive.

- a. Private sector in-house: I work on the internal privacy needs of a company, nonprofit or university.
- b. Government in-house: I work on the internal privacy needs of a government agency.
- c. Regulator: I work for a government agency that monitors and enforces compliance with privacy regulations.
- d. In-house IT: I work on the internal information-technology needs of my organization.
- e. Researcher or academic: I work as a researcher, professor or writer on the topic of privacy.
- f. External privacy advisor: I work as a privacy consultant, attorney, barrister or auditor on the privacy needs of other organizations.
- g. Vendor: I work for a company that sells privacy products or services.
- h. Small business: I manage or work for a small business that needs to manage customer privacy.
- i. Privacy advocate: I raise public awareness about privacy, work toward open debate on privacy risks and lobby for privacy regulations.

Private sector in-house

18. Your company serves consumers or customers located in: (check all that apply)

- a. United States
- b. Canada
- c. Latin America
- d. Europe
- e. Africa
- f. Middle East
- g. Asia
- h. Australia/New Zealand

19. Which of the following best describes the department or unit in which your organization's privacy function is situated.

- a. Legal
- b. Compliance
- c. Audit & Quality Assurance
- d. Ethics & Corporate Responsibility
- e. Risk Management
- f. Information Security
- g. Information Technology
- h. Marketing
- i. Human Resources
- j. Operations
- k. Business Unit
- l. It is its own function reporting directly to the top executive or board
- m. We don't have a privacy function

20. How many levels of individuals are between you and your organization's top executive?

- a. 0
- b. 1
- c. 2
- d. 3
- e. 4
- f. 5
- g. 5+

21. How many levels of individuals are between your organization's top privacy leader and your organization's top executive?

- a. 0
- b. 1
- c. 2
- d. 3
- e. 4
- f. 5
- g. 5+
- h. We don't have a privacy leader

22. Which of the following words occur in the formal title of your organization's top privacy leader? (Check all that apply.)

- a. Chief
- b. Privacy
- c. Data Protection
- d. Security
- e. Governance
- f. Risk
- g. Compliance
- h. Officer
- i. Official

23. About how many full-time equivalent individuals work on privacy in your organization?

- a. Less than 1
- b. 1
- c. 2
- d. 3
- e. 4
- f. 5
- g. 6-10
- h. 11-25
- i. 26-50
- j. 51-100
- k. 101+

24. What would you say is the approximate budget your organization allocates to privacy, excluding salaries and benefits?

- a. \$0
- b. Less than \$25,000
- c. \$25,000-75,000
- d. \$75,001-150,000
- e. \$150,001-250,000
- f. \$250,001-1,000,000
- g. \$1,000,001-5,000,000
- h. More than \$5,000,000

25. To your knowledge, how many publicized data breaches and privacy regulatory enforcement actions has your organization experienced in the past year?

- a. None
- b. One incident
- c. 2-5 incidents
- d. 6-10 incidents
- e. 11-50 incidents
- f. More than 50 incidents

26. To your knowledge, which of the following external privacy services has your privacy function engaged in over the past year? (Check all that apply.)

- a. We've used a privacy attorney
- b. We've used a privacy consultant
- c. We've used other privacy services firms

27. The executives of your organization support and fund your privacy function for the following reasons: (Check all that apply.)

- a. To meet regulatory compliance obligations
- b. To reduce the risk of data breach notification and publicized data breaches
- c. To reduce the risk of employee and consumer lawsuits
- d. To reduce the cost of storing data
- e. To increase the value and quality of data
- f. To enable global operations and entry into new markets
- g. To meet the expectations of business clients and partners
- h. To increase revenues from cross-selling and direct marketing
- i. To enhance the organization's brand and public trust
- j. To provide a competitive differentiator

28. Looking ahead to your 2011 privacy agenda, in which of the following areas will your organization launch new projects? (Check all that apply.)

- a. Policy revision
- b. Process documentation and improvement
- c. Training and awareness
- d. Vendor and third-party assurance
- e. Data inventorying and mapping
- f. Privacy audits and assessments
- g. External certification
- h. Privacy choice and consent consolidation
- i. Data loss prevention technology
- j. Governance, risk and compliance technology
- k. Data use logging and monitoring technology
- l. Additional Comments

29. Estimate the privacy maturity level of your organization based on the description of each level.

- a. Nonexistent: Currently no one in the organization is working on privacy and there are no documented privacy policies or processes.
- b. Initial: At least some parts of the organization are following an ad hoc, albeit inconsistent, approach to data privacy, but there are no documented privacy policies or standards.
- c. Repeatable: The organization has a consistent overall approach in areas where it has its most important privacy risks and obligations, but at most there is only a minimal or general level of privacy policy and process documentation.
- d. Defined: The organization has a documented, detailed approach to privacy policies and processes that apply to the entire organization, but there is no routine measurement or enforcement.
- e. Managed: The organization regularly measures and enforces its compliance with its privacy policies and processes, conducts ad hoc benchmarking with its peers and makes regular process improvements based on these findings.
- f. Optimized: The organization has refined its privacy practices to the level of recognized best practices, where instances of privacy risks and noncompliance have been mitigated to acceptable levels, and a culture of privacy is endemic across the organization.

30. About how many hours do you work in a typical week?

Please estimate the time you spend on the following activities. Note this is an estimate only—percentages don't need to total exactly 100.

	0-5%	6-10%	11-15%	16-20%	21-25%	Over 25%
Developing privacy strategy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analyzing privacy regulations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advising and consulting the organization on privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Developing and performing privacy training and communications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitoring and measuring privacy compliance and enforcement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Responding to data incidents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reporting to management or privacy stakeholders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Performing privacy risk assessments and data inventories	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Developing and implementing privacy policies and guidance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administration of privacy personnel and budget	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activities not related to privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Government in-house

31. Which of the following best describes the department or unit in which your agency's privacy function is situated.

- a. Legal
- b. Compliance
- c. Audit & Quality Assurance
- d. Ethics & Corporate Responsibility
- e. Risk Management
- f. Information Security
- g. Information Technology
- h. Marketing
- i. Human Resources
- j. Operations
- k. Business Unit
- l. It is its own function reporting directly to the top executive
- m. We don't have a privacy function
- n. Other (please specify)

32. How many levels of individuals are between you and your agency's top executive?

- a. 0 (You are a "C-level" executive who reports directly to the agency head)
- b. 1 (You report to someone who reports to the agency head)
- c. 2
- d. 3
- e. 4
- f. 5
- g. 5+

33. How many levels of individuals are between your organization's top privacy leader and your organization's top executive?

- a. 0 (Our top privacy leader is a "C-level" executive who reports directly to the agency head)
- b. 1 (Our privacy leader reports to a person who reports to the agency head)
- c. 2
- d. 3
- e. 4
- f. 5
- g. 5+
- h. We don't have a privacy leader

34. Which of the following words occur in the formal title of your agency's top privacy leader?

- a. Chief
- b. Privacy
- c. Data Protection
- d. Security
- e. Governance
- f. Risk
- g. Compliance
- h. Officer
- i. Official

35. About how many full-time equivalent people work on privacy in your agency?

- a. Less than 1
- b. 1
- c. 2
- d. 3
- e. 4
- f. 5
- g. 6-10
- h. 11-25
- i. 26-50
- j. 51-100
- k. 101+

36. What is the approximate budget your agency allocates to privacy, excluding salaries and benefits?

- a. \$0
- b. Less than \$25,000
- c. \$25,000-75,000
- d. \$75,001-150,000
- e. \$150,001-250,000
- f. \$250,001-1,000,000
- g. \$1,000,001-5,000,000
- h. More than \$5,000,000

37. About how many publicized data breaches and investigations has your agency experienced in the past year that you know about?

- a. None
- b. One incident
- c. 2-5 incidents
- d. 6-10 incidents
- e. 11-50 incidents
- f. More than 50 incidents

38. Which of the following external privacy services has your privacy function engaged in the past year, to your knowledge?

- a. We've used a privacy attorney
- b. We've used a privacy consultant
- c. We've used other privacy services firms

39. The executives of your organization support and fund the privacy function for the following reasons: (Check all that apply.)

- a. To meet regulatory compliance obligations
- b. To reduce the risk of data breach and publicized data breaches
- c. To reduce the risk of employee and citizen lawsuits
- d. To reduce the cost of storing data
- e. To increase the value and quality of data
- f. To enhance the agency's brand and public trust
- g. To better enable the agency's operations and mission

40. Looking ahead to your 2011 privacy agenda, in which of the following areas will your agency launch new projects? (Check all that apply.)

- a. Policy revision
- b. Process documentation and improvement
- c. Training and awareness
- d. Vendor and third-party assurance
- e. Data inventorying and mapping
- f. Privacy audits and privacy impact assessments
- g. External certification
- h. Privacy choice and consent consolidation
- i. Data loss prevention technology
- j. Governance, risk and compliance technology
- k. Data use logging and monitoring technology
- l. Additional comments

41. Estimate the privacy maturity level of your agency based on the description of each level.

- a. Nonexistent: Currently, no one in the agency works on privacy and there are no documented privacy policies or processes.
- b. Initial: At least some parts of the agency are following an ad hoc, albeit inconsistent, approach to data privacy, but there are no documented privacy policies or standards.
- c. Repeatable: The agency has a consistent overall approach in areas where it has its most important privacy risks and obligations, but at most there is only a minimal or general level of privacy policy and process documentation.
- d. Defined: The agency has a documented, detailed approach to privacy policies and processes that apply to the entire agency, but there is no routine measurement or enforcement.
- e. Managed: The agency regularly measures and enforces its compliance with its privacy policies and processes, conducts ad hoc benchmarking with its peers and makes regular process improvements based on these findings.
- f. Optimized: The agency has refined its privacy practices to the level of recognized best practices, where instances of privacy risks and noncompliance have been mitigated to acceptable levels, and a culture of privacy is endemic across the agency.

42. About how many hours do you work in a typical week?

Estimate the percent of time you spend on the following activities. Note that this is an estimate only—your percentages don't need to total 100.

	0-5%	6-10%	11-15%	16-20%	21-25%	Over 25%
Developing privacy strategy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analyzing privacy regulations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advising and consulting the organization on privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Developing and performing privacy training and communications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitoring and measuring privacy compliance and enforcement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Responding to data incidents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reporting to management or privacy stakeholders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Performing privacy risk assessments and data inventories	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Developing and implementing privacy policies and guidance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Administration of privacy personnel and budget	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activities not related to privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

43. About how many reports does your agency deliver to external stakeholders each year?

44. Do you have a CIPP/G certification?

- a. Yes
- b. No

In-house IT

45. How many levels of people are between you and your organization's top executive?

- a. 0 (You are a "C-level" executive who reports directly to the top executive)
- b. 1 (Typically a vice president who reports to someone who reports to the top executive)
- c. 2 (Typically a director or vice president)
- d. 3 (Typically a manager or director)
- e. 4 (Typically a senior analyst or manager)
- f. 5 (Typically an analyst or senior analyst)
- g. 5+

46. Which of the following best describes the area of IT that you currently work in?

- a. Network and infrastructure
- b. Application development
- c. Database administration
- d. Data center operations
- e. Information security
- f. Business continuity and disaster recovery
- g. IT process improvement
- h. Office of the CIO

47. Looking ahead to your 2011 agenda, in which of the following areas will your organization launch new projects related to privacy and security? Check all that apply.

- a. Policy revision
- b. Process documentation and improvement
- c. Training and awareness
- d. Vendor and third-party assurance
- e. Data inventorying and mapping
- f. Privacy audits and privacy impact assessments
- g. External certification
- h. Privacy choice and consent consolidation
- i. Data loss prevention technology
- j. Governance, risk and compliance technology
- k. Data use logging and monitoring technology
- l. Data encryption and masking
- m. Additional comments

48. Estimate the privacy maturity level of your organization based on the description of each level.

- a. Nonexistent: There is currently nobody in the organization working on privacy and no documented privacy policies or processes.
- b. Initial: At least some parts of the organization are following an ad hoc, albeit inconsistent, approach to data privacy, although there are no documented privacy policies or standards.
- c. Repeatable: The organization has a consistent overall approach in areas where it has its most important privacy risks and obligations, but at most there is only a minimal or general level of privacy policy and process documentation.
- d. Defined: The organization has a documented, detailed approach to privacy policies and processes that apply to the entire organization, but there is no routine measurement or enforcement.
- e. Managed: The organization regularly measures and enforces its compliance with its privacy policies and processes, conducts ad hoc benchmarking with its peers and makes regular process improvements based on these findings.
- f. Optimized: The organization has refined its privacy practices to the level of recognized best practices, where instances of privacy risks and noncompliance have been mitigated to acceptable levels, and a culture of privacy is endemic across the organization.

49. About how many hours do you work in a typical week?

Estimate the time you spend on the following activities. Note this is an estimate only—percentages don't need to total 100.

	0-5%	6-10%	11-15%	16-20%	21-25%	Over 25%
Assisting with third-party audits of our IT environment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assisting with internal audits of our IT environment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assisting with audits of our service providers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remediating our IT systems to close audit gaps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Responding to data incidents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reporting to management or privacy stakeholders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Performing data inventories	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Activities not related to privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

50. Do you have a CIPP/IT certification?

- a. Yes
- b. No

Researcher or Academic

51. Looking ahead to your 2011 research agenda, on which of the following privacy areas will you focus? (Check all that apply.)

- a. Privacy Management – topics relating to the placement, scope and operations of the privacy function
- b. Privacy Notices – topics relating to the content and delivery of privacy notices
- c. Privacy Choices – topics relating to the nature and methods of privacy choices, preferences, authorizations and permissions
- d. Limiting Personal Data Collection – topics relating to inappropriate data collection and policies and methods to minimize collection of personal data
- e. Limiting Personal Data Uses – topics relating to inappropriate data uses and policies and methods to minimize uses of personal data
- f. Limiting Personal Data Retention – topics relating to inappropriate data retention and policies and methods to minimize retention of personal data
- g. Data Subject Access – topics relating to the nature, importance, policies and methods of providing data subjects access to their personal data
- h. Quality of Personal Data – topics relating to nature, importance, policies and methods of ensuring the accuracy, completeness and currency of personal data
- i. Data Disclosure to Third Parties – topics relating to the risks, policies and methods of third-party processing and hosting of personal data
- j. Security of Personal Data – topics relating to the policies, methods of and technologies preventing unauthorized access to personal data
- k. Privacy Monitoring and Enforcement – topics relating to assessing, auditing and certifying privacy compliance, including accountability and privacy by design
- l. Privacy and Society – topics relating to the cultural meaning and importance of privacy and the social impact when privacy is compromised

52. What is the most important unanswered question in privacy?

Privacy Advocate

53. Where is the majority of your organizations privacy advocacy focused?

- a. Influencing legislators
- b. Educating the public
- c. Filing Freedom of Information Act requests
- d. Filing lawsuits
- e. Conducting research
- f. Other (please specify)

54. From which of the following sources does your organization obtain a significant amount of its funding? (Check all that apply.)

- a. Corporate grants
- b. Foundation and public grants
- c. Funds set up by court settlements
- d. Member dues
- e. Service fees
- f. Other (please specify)

55. Looking ahead to your 2011 agenda, in which of the following privacy areas will you focus? (Check all that apply.)

- a. Privacy Management – concerns relating to the placement, scope and operations of the privacy function
- b. Privacy Notices – concerns relating to the content and delivery of privacy notices
- c. Privacy Choices – concerns relating to the nature and methods of privacy choices, preferences, authorizations and permissions
- d. Limiting Personal Data Collection – concerns relating to inappropriate data collection and policies and methods to minimize collection of personal data
- e. Limiting Personal Data Uses – concerns relating to inappropriate data uses and policies and methods to minimize uses of personal data
- f. Limiting Personal Data Retention – concerns relating to inappropriate data retention and policies and methods to minimize retention of personal data
- g. Data Subject Access – concerns relating to the nature, importance, policies and methods of providing data subjects access to their personal data
- h. Quality of Personal Data – concerns relating to the nature, importance, policies and methods of ensuring the accuracy, completeness, and currency of personal data
- i. Data Disclosure to Third Parties – concerns relating to the risks, policies and methods of third-party processing and hosting of personal data
- j. Security of Personal Data – concerns relating to the policies, methods and technologies of preventing unauthorized access to personal data
- k. Privacy Monitoring and Enforcement – concerns relating to assessing, auditing and certifying privacy compliance, including accountability and privacy by design
- l. Privacy and Society – concerns relating to the cultural meaning and importance of privacy and the social impact when privacy is compromised

56. What do you think is the biggest threat to privacy?

Regulator

57. Looking ahead to your agency's 2011 enforcement priorities, in which of the following privacy areas will you focus? (Check all that apply.)

- a. Privacy Management – concerns relating to the placement, scope and operations of the privacy function
- b. Privacy Notices – concerns relating to the content and delivery of privacy notices
- c. Privacy Choices – concerns relating to the nature and methods of privacy choices, preferences, authorizations and permissions
- d. Limiting Personal Data Collection – concerns relating to inappropriate data collection and policies and methods to minimize collection of personal data
- e. Limiting Personal Data Uses – concerns relating to inappropriate data uses and policies and methods to minimize uses of personal data
- f. Limiting Personal Data Retention – concerns relating to inappropriate data retention and policies and methods to minimize retention of personal data
- g. Data Subject Access – concerns relating to the nature, importance, policies and methods of providing data subjects access to their personal data
- h. Quality of Personal Data – concerns relating to the nature, importance, policies and methods of ensuring the accuracy, completeness and currency of personal data
- i. Data Disclosure to Third Parties – concerns relating to the risks, policies and methods of third-party processing and hosting of personal data
- j. Security of Personal Data – concerns relating to the policies, methods of and technologies preventing unauthorized access to personal data
- k. Privacy Monitoring and Enforcement – concerns relating to assessing, auditing and certifying privacy compliance, including accountability and privacy by design
- l. Privacy and Society – concerns relating to the cultural meaning and importance of privacy and the social impact when privacy is compromised

58. Besides resource constraints, what do you think is the biggest challenge to regulating privacy?

59. Do you have a CIPP/G certification?

- a. Yes
- b. No

External Privacy Advisor

60. In which sector have you spent the most time personally advising clients on privacy-related topics in the past year?

- a. Aerospace & Defense
- b. Banking
- c. Business Services & Supplies
- d. Capital Goods
- e. Chemicals
- f. Conglomerates (multiple sectors)
- g. Construction
- h. Consumer Durables
- i. Diversified Financials
- j. Drugs & Biotechnology
- k. Education & Academia
- l. Food, Drink & Tobacco
- m. Food Markets
- n. Government
- o. Healthcare Equipment & Services
- p. Hotels, Restaurants & Leisure
- q. Household & Personal Products
- r. Insurance
- s. Materials
- t. Media
- u. Nonprofit
- v. Oil & Gas Operations
- w. Retail
- x. Semiconductors
- y. Software & Services
- z. Technology Hardware & Equipment
- aa. Telecommunication Services
- bb. Trading Companies
- cc. Transportation
- dd. Utilities

61. In which sectors did you personally advise clients on privacy-related topics in the past year? (Check all that apply.)

- a. Aerospace & Defense
- b. Banking
- c. Business Services & Supplies
- d. Capital Goods
- e. Chemicals
- f. Conglomerates (multiple sectors)
- g. Construction
- h. Consumer Durables
- i. Diversified Financials
- j. Drugs & Biotechnology
- k. Education & Academia
- l. Food, Drink & Tobacco
- m. Food Markets
- n. Government
- o. Healthcare Equipment & Services
- p. Hotels, Restaurants & Leisure
- q. Household & Personal Products
- r. Insurance
- s. Materials
- t. Media
- u. Nonprofit
- v. Oil & Gas Operations
- w. Retail
- x. Semiconductors
- y. Software & Services
- z. Technology Hardware & Equipment
- aa. Telecommunication Services
- bb. Trading Companies
- cc. Transportation
- dd. Utilities

62. Which of the following types of advisory services has your firm provided in the past year? (Check all that apply.)

- a. Privacy program development
- b. Interpretation of privacy regulations
- c. Documenting privacy policies and processes
- d. Privacy audits and assessments
- e. Data inventorying & mapping
- f. Data breach response
- g. Crossborder data transfer
- h. Marketing support
- i. Outsourcing and third-party assurance
- j. Employee awareness and training
- k. IT transactions
- l. Mergers and acquisitions
- m. Privacy litigation

63. Looking ahead to two years from now, which one of the following areas do you see generating the most demand for your firm?

- a. Privacy program development
- b. Interpretation of privacy regulations
- c. Documenting privacy policies and processes
- d. Privacy audits and assessments
- e. Data inventorying & mapping
- f. Data breach response
- g. Crossborder data transfers
- h. Marketing support
- i. Outsourcing and third-party assurance
- j. Employee awareness and training
- k. IT transactions
- l. Mergers and acquisitions
- m. Privacy litigation
- n. Other (please specify)

64. Over the next two years, do you expect the market for privacy advisory services will:

- a. Grow more than 10%
- b. Grow between 0 and 10%
- c. Stay the same
- d. Contract between 0 and 10%
- e. Contract more than 10%

65. Your clients' top executives fund their privacy functions for the following reasons: (Check all that apply.)

- a. To meet regulatory compliance obligations
- b. To reduce the risk of data breach and publicized data breaches
- c. To reduce the risk of employee and consumer lawsuits
- d. To reduce the cost of storing data
- e. To increase the value and quality of data
- f. To enable global operations and entry into new markets
- g. To increase revenues from cross-selling and direct marketing
- h. To enhance the organization's brand and public trust
- i. To provide a competitive differentiator

66. Why do you think your clients engage outside privacy advisors? (Check all that apply.)

- a. To get the answers to questions they don't know
- b. To obtain access to methodologies they don't have
- c. To gain guidance from experiences they haven't had
- d. To gain a temporary increase in staff to accomplish tasks that outstrip internal capabilities
- e. To receive services that only an outside entity can provide
- f. Other (please specify)

67. About how many hours did you bill to client projects in the past year?

- a. 0-400 (about 1 day per week)
- b. 401-800 (about 2 days per week)
- c. 801-1,200 hours (about 3 days per week)
- d. 1,201-1,600 hours (about 4 days per week)
- e. 1,601-2,000 hours (about 5 days per week)
- f. 2,001-2,400 hours (about 6 days per week)

68. About what percent of those hours were related to privacy?

69. If you bill on an hourly basis for at least some of your clients, what was the typical hourly rate, in U.S. dollars, that you billed in the past year?

Vendor

70. In which sector have you spent the most time serving clients on privacy-related topics in the past year?

- a. Aerospace & Defense
- b. Banking
- c. Business Services & Supplies
- d. Capital Goods
- e. Chemicals
- f. Conglomerates (multiple sectors)
- g. Construction
- h. Consumer Durables
- i. Diversified Financials
- j. Drugs & Biotechnology
- k. Education & Academia
- l. Food, Drink & Tobacco
- m. Food Markets
- n. Government
- o. Healthcare Equipment & Services
- p. Hotels, Restaurants & Leisure
- q. Household & Personal Products
- r. Insurance
- s. Materials
- t. Media
- u. Nonprofit
- v. Oil & Gas Operations
- w. Retail
- x. Semiconductors
- y. Software & Services
- z. Technology Hardware & Equipment
- aa. Telecommunication Services
- bb. Trading Companies
- cc. Transportation
- dd. Utilities

71. What are all of the sectors in which you served clients on privacy-related topics in the past year? (Check all that apply.)

- a. Aerospace & Defense
- b. Banking
- c. Business Services & Supplies
- d. Capital Goods
- e. Chemicals
- f. Conglomerates
- g. Construction
- h. Consumer Durables
- i. Diversified Financials
- j. Drugs & Biotechnology
- k. Education & Academia
- l. Food, Drink & Tobacco
- m. Food Markets
- n. Government
- o. Healthcare Equipment & Services
- p. Hotels, Restaurants & Leisure
- q. Household & Personal Products
- r. Insurance
- s. Materials
- t. Media
- u. Nonprofits
- v. Oil & Gas Operations
- w. Retail
- x. Semiconductors
- y. Software & Services
- z. Technology Hardware & Equipment
- aa. Telecommunication Services
- bb. Trading Companies
- cc. Transportation
- dd. Utilities

72. Which of the following types of products has your firm provided in the past year? (Check all that apply.)

- a. Privacy Management – products relating to the placement, scope and operations of the privacy function
- b. Privacy Notices – products relating to the content and delivery of privacy notices
- c. Privacy Choices – products relating to managing privacy choices, preferences and suppression lists
- d. Limiting Personal Data Collection – products relating to identifying, classifying and mapping personal data
- e. Limiting Personal Data Uses – products relating to logging and monitoring data uses and limiting inappropriate data uses
- f. Limiting Personal Data Retention – products relating to identifying and managing retention schedules and destroying or de-identifying data
- g. Data Subject Access – products related to providing data subjects access to their personal data
- h. Quality of Personal Data – products related to ensuring the accuracy, completeness and currency of personal data
- i. Data Disclosure to Third Parties – products related to identifying and managing the risk and compliance of third-party processing and hosting of personal data
- j. Security of Personal Data – products related to the policies, methods and technologies of preventing unauthorized access to personal data
- k. Privacy Monitoring and Enforcement – products related to assessing, auditing and certifying privacy compliance
- l. Privacy and Society – public outreach to educate, inform and equip citizens with the means to protect their privacy

73. Looking ahead to two years from now, which one of the following privacy areas will generate the most demand for your firm?

- a. Privacy Management – products relating to the placement, scope and operations of the privacy function
- b. Privacy Notices – products relating to the content and delivery of privacy notices
- c. Privacy Choices – products relating to managing privacy choices, preferences and suppression lists
- d. Limiting Personal Data Collection – products relating to identifying, classifying and mapping personal data
- e. Limiting Personal Data Uses – products relating to logging and monitoring data uses and limiting inappropriate data uses
- f. Limiting Personal Data Retention – products relating to identifying and managing retention schedules and destroying or de-identifying data
- g. Data Subject Access – products related to providing data subjects access to their personal data
- h. Quality of Personal Data – products related to ensuring the accuracy, completeness and currency of personal data
- i. Data Disclosure to Third Parties – products related to identifying and managing the risk and compliance of third-party processing and hosting of personal data
- j. Security of Personal Data – products related to the policies, methods and technologies of preventing unauthorized access to personal data
- k. Privacy Monitoring and Enforcement – products related to assessing, auditing and certifying privacy compliance
- l. Privacy and Society – public outreach to educate, inform and equip citizens with the means to protect their privacy

74. Over the next two years, do you expect the market for privacy products will:

- a. Grow more than 10%
- b. Grow between 0 and 10%
- c. Stay the same
- d. Contract between 0 and 10%
- e. Contract more than 10%

75. Approximately what level of revenue does your firm earn from its privacy-related products?

- a. Less than \$1 million
- b. \$1 million to \$25 million
- c. \$25 million to \$100 million
- d. More than \$100 million

Small Business

76. About how many employees and contractors work for your business?

77. As a small business, what type of privacy support do you need? (Check all that apply.)

- a. Understanding what the law requires us to do
- b. Understanding how to reduce the risk of a data breach
- c. Assistance with developing a privacy program
- d. Assistance with meeting the contractual requirements of our clients
- e. Answering our ad hoc questions about privacy
- f. Other (please specify)

78. Where do you look for the privacy support you need? (Check all that apply.)

- a. Personal networks of our employees
- b. Local business associations
- c. Local business publications
- d. National professional associations
- e. Online searches
- f. Other (please specify)

79. What is your top privacy concern?

80. How much have you budgeted for privacy in 2011?

About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest association of privacy professionals, representing more than 8,000 members from businesses, governments and academic institutions across 68 countries.

The IAPP was founded in 2000 with a mission to define, support and improve the privacy profession globally through networking, education and certification. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP). The CIPP remains the leading privacy certification for professionals who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations. The program has since grown to include the CIPP/G, CIPP/C and CIPP/IT. Today, many thousands of professionals worldwide hold an IAPP privacy certification.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.

About the Author

Jay Cline, CIPP, president of Minnesota Privacy Consultants, is the former chief privacy officer of Carlson Companies, IT management consultant at EDS and international trade law expert in the U.S. government. Cline has held leadership positions in the International Association of Privacy Professionals and is a privacy columnist for *Computerworld* and the IAPP's *Inside 1to1: Privacy*.

The IAPP expresses sincere thanks to the privacy practitioners who generously dedicated their time and insights to this survey.

To participate in future IAPP research efforts, or to provide feedback on this survey, please contact us at research@privacyassociation.org.

IAPP

Pease International Tradeport, 75 Rochester Ave., Suite 4, Portsmouth, NH 03801 USA
+1 603.427.9200 www.privacyassociation.org