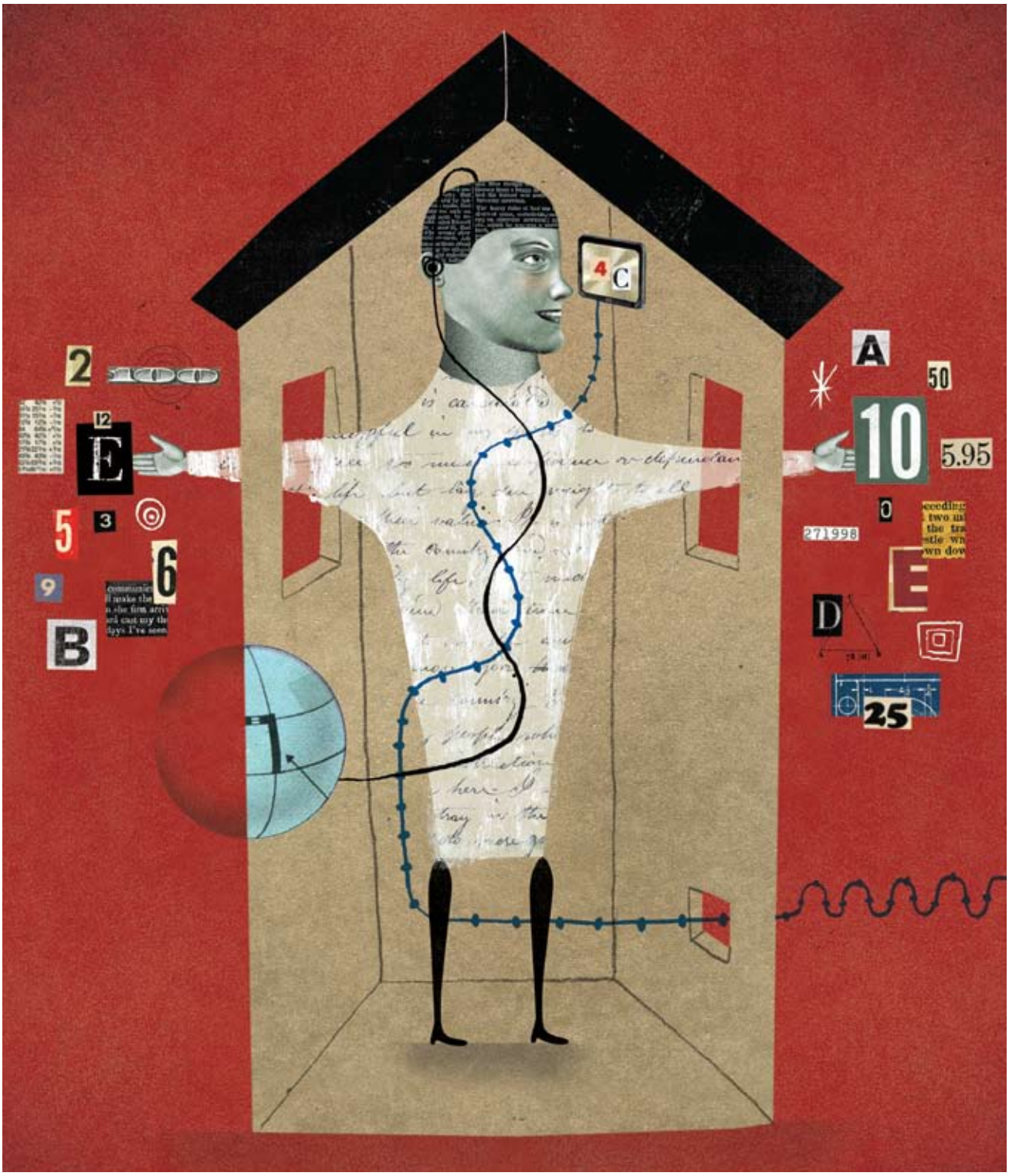
A CALL FOR AGILITY:

The Next-Generation Privacy Professional



International Association of Privacy Professionals

A CALL FOR AGILITY:
The Next-Generation Privacy Professional

International Association of Privacy Professionals

Table of Contents

A Letter from the IAPP

It is with great pleasure that we present to you the first whitepaper to be published by the IAPP on the future of the privacy profession.

"A Call for Agility: The Next-Generation Privacy Professional" is the culmination of months of coordinated effort between IAPP leadership and many of the top minds across the global privacy community — the executives, academics, officers, and regulators that helped shape and continue to define the laws, technologies, and practices that are the core of work. Most importantly, this paper reflects the real experiences and thoughts of you, our members, through the member survey process that the IAPP undertakes each year.

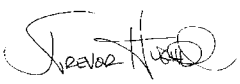
Over the past 10 years the IAPP has reperesented the ever-growing privacy community as the largest association of privacy professionals. We are committed to developing and offering educational resources, professional development programs, and forums for debate and discussion among businesses, governments, and nonprofits in the global privacy arena. We now look with great interest and enthusiasm to what we all will face in the next 10 years.

We trust that you will find the contents of this report both a worthy tribute to the history we have made together as well as an enlightened look toward the challenges only now emerging — and those we have yet to encounter. We encourage you to leverage the insights described here in planning your privacy programs and building your teams for future success. And we invite you to join us as we continue to define, promote and improve the privacy profession globally in the coming years.

Sincerely,

Nuala O'Connor Kelly, CIPP/G
Chief Privacy Leader
and Senior Counsel
General Electric Company
President, IAPP

Harriet Pearson, CIPP
VP Security Counsel and
Chief Privacy Officer
IBM Corporation
Chair, Project Advisory Board



J. Trevor Hughes, CIPP
Executive Director
IAPP

Acknowledgements

"A Call for Agility" represents the combined expertise and perspective of a diverse group of authors, contributors, and advisors without whom the report you now hold would not have been possible. The IAPP wishes to express its sincere thanks to these many talented individuals for their generous contributions of time and insight:

- To the research project chair: Harriet Pearson, CIPP, Vice President Security Counsel and Chief Privacy Officer, IBM Corporation, and to the report's author, Jay Cline, CIPP, Minnesota Privacy Consultants

- To the project advisors: Dean Forbes, CIPP Senior Director, Merck & Co., Inc.; Jeff Green, CIPP/C, Vice President, Global Compliance and Governance and Chief Privacy Officer, RBC Financial Group; Kirk Herath, CIPP/G, Vice President, Chief Privacy Officer and Associate General Counsel, Nationwide Insurance Companies; and Zoe Strickland, GIPP/G, Vice President, Chief Privacy Officer, Walmart Stores

- To the project contributors: Martin Abrams, Senior Policy Advisor, Hunton & Williams LLP; Bojana Bellamy, Director of Data Privacy, Accenture (UK) Limited; Agnes Bundy Scanlan, Esq. CIPP, Chief Regulatory Officer, TD Bank North America; Joyce Brocaglia, President & Chief Executive Officer, Alta Associates; Ann Cavoukian, Ph.D., Information & Privacy Commissioner, Ontario, Canada; Peter Cullen, CIPP, Chief Privacy Strategist, Microsoft Corporation; Malcolm Crompton, CIPP, Managing Director, Information Integrity Solutions Pty Ltd.; Michelle Dennedy, Vice President Security and Privacy Solutions, Oracle Corporation; Sandra R. Hughes, CIPP, Global Privacy Executive, Procter & Gamble Company; Alexander W. Joel, Civil Liberties Protection Officer, Office of the Director of National Intelligence; James Harlan Koenig, CIPP, Practice Leader, Privacy & Identity Theft, PricewaterhouseCoopers LLP; Deirdre K. Mulligan, Assistant Professor, School of Information, Faculty Director, Berkeley Center for Law and Technology; Brian O'Connor, Chief Security and Privacy Officer, Eastman Kodak Company; Nuala O'Connor Kelly, CIPP/G, Senior Counsel, Information Governance & Chief Privacy Leader, General Electric Company; Richard Purcell, CIPP, Chief Executive Officer, Corporate Privacy Group; and Jennifer Stoddart, Commissioner, Office of the Privacy Commissioner of Canada

Purpose and Methodology

The International Association of Privacy Professionals commissioned this work on the occasion of its tenth anniversary in March, 2010. The purpose of the project is to take a step back and help privacy professionals see the changing opportunities that lie before them. A panel of advisors gave of their time generously to offer insights and to guide the approach and methodology used in this paper.

Many privacy professionals and noted experts were interviewed for this report. Data was also drawn from the IAPP's Privacy Professional's Role, Function and Salary Survey (2010, IAPP), Benchmarking Privacy: an Executive Summary published by the IAPP and the Ponemon Institute, as well as other sources.

- The IAPP's "Privacy Professional's Role, Function and Salary Survey" (2010, IAPP) included a total of 23 items, and was fielded electronically in December of 2009 to approximately 6,000 IAPP members. More than 880 individuals completed the survey for a response rate of 14.8%. To maintain complete confidentiality, the survey instrument did not capture individual or company specific information of any kind.

- "Benchmarking Privacy: An Executive Summary" surveyed in total 336 IAPP member organizations. Each organization selected for participation included a privacy officer or the equivalent plus staff members within that group. The recipients were IAPP members and senior privacy officials in both the public and private sectors. The survey was sent by mail, and data was gathered during two periods between August 1, 2008 and mid January 2009.

Executive Summary

The next 10 years will see more types of data collected from more people, and more privacy laws in more places. A deepening and broadening of data protection regulations in the industrialized world will spread to emerging markets and place a higher premium on legal and compliance acumen. In addition, an expansion of health information networks, smart grid networks and cloud computing platforms will make industry and technology expertise a more indispensable part of practicing privacy.

Privacy career opportunities will abound. A rise in privacy awareness among small- and medium-sized businesses, government agencies and other organizations—as well as ongoing maturation of roles pertaining to information governance, risk management, data security, and compliance—will create new career paths and opportunities for privacy professionals. Indeed, the diversity of the skills that today's privacy professional has had to develop will prove useful to a number of other organizational functions. Nothing will remain static in this field, and demand will not slow down. Even amidst economic uncertainty, heightened information risks resulting from ongoing cyber crime and other threats will tend to insulate budgets dedicated to the protection of valuable personal data, and undergird strong growth in the profession.

Despite these promising opportunities, the privacy professional's success in the next decade will demand greater adaptability and most importantly, agility. The agile privacy professional is the next-generation privacy professional: an expert practitioner who is keenly attuned to cultural and regional distinctions as these continue to grow in an increasingly interconnected data economy; who can migrate and adapt to different roles within an organization and offer value at each; who exhibits both comfort and grasp of legal/compliance and technical disciplines; and who instills direction and leadership of privacy management within the organization.

Introduction

In the heady days of the dot-com boom, a new profession was born. The emergence of the Internet and new privacy regulations in Europe and North America by the late 1990s had ushered into the executive suite a new arrival: the chief privacy officer. Called something different in different organizations, those chosen for this new leadership role quickly sought one another out. From this early camaraderie emerged the International Association of Privacy Professionals. The IAPP soon became the focal point for fostering the support and growth of the nascent privacy profession. Through its conferences and Certified Information Privacy Professional credentials, the IAPP gave a structure to this new discipline.

Much has changed in a decade. The information revolution has intensified, connecting people and machines worldwide through Web-enabled devices. Public-sector initiatives aimed at preventing terrorism and fighting global crime rings perpetrating identity fraud have led to the expansion of governments' accumulation and use of personal data. Moreover, a patchwork quilt of local, national, and supranational privacy and security regulations now blankets the industrialized world. Reflecting the privacy and information policy issues spawned by this historic transformation, the number of privacy professionals has grown at double-digit rates and continues to increase despite a protracted economic downturn. And while privacy professional jobs initially were clustered in a few geographies, the IAPP's increasingly international membership shows that the phenomenon of the privacy professional has spread to more than 50 countries.

What will the next 10 years portend for those earning their living enabling organizations to address privacy expectations and compliance obligations? This whitepaper offers an informed and actionable set of insights on this question.

Supplementing an association-wide membership survey, a blue-ribbon panel of seasoned privacy professionals, academics, consultants, and other advisors drew upon its collective sense of important trends in business, regulation, and technology to project the likely paths privacy professionals will take—and what it will take to navigate them.

A diverse array of professionals will benefit from the insights presented on the following pages:

- Privacy professionals who seek guidance in planning for the experiences and skills they will likely need in the years to come;
- Executive leaders with overall responsibility for human resources, legal, risk management, and technology—the leaders to whom today's privacy professionals often report—will use this document to inform organizational and leadership development;
- Prospective privacy professionals (individuals new to the field or transitioning from related fields such as legal compliance, information auditing, information security, etc.) desiring more context about privacy as a growing profession;
- Recruiters and human resources professionals looking to place candidates in a job market that continues to grow;
- Press and media seeking to cover privacy and related topics; and,
- Regulators, legislators and policy executives who increasingly interact with privacy professionals.

The Emergence of a New Profession: Drivers of Change

The privacy profession is burgeoning today due to three formative developments: the dawn of the Information Age, the regulatory tsunami, and increased data collection. The globalization of commerce and business operations has intensified the impact of these changes.

Driver One: The Dawn of the Information Age

Advances in information technology have for more than a century prompted debate in the West about how society can maintain personal privacy amidst the changes. It was the spread of the use of the photographic camera that famously led the future U.S. Supreme Court Justice Louis Brandeis to note in an 1890 edition of the Harvard Law Review, "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" The subsequent inventions of the radio, motion picture, and television prompted further public commentary about privacy. In spite of these developments, however, nothing resembling a privacy profession had materialized.

Similar ongoing developments throughout the twentieth century set the stage for a late-century revolution of sorts. For decades, organizations had been reaping the benefits of information technology-fueled productivity enhancers, and some sectors—most notably credit reporting, financial services, and data brokerage—had amassed huge quantities of consumer data. Meanwhile, households were steadily integrating personal computers into daily life. The widespread availability by the mid-1990s of the World Wide Web sparked a revolution in both of these worlds. Ordinary people armed with a desktop computer and dial-up modem could now access a rapidly proliferating network of information previously only available in libraries and filing cabinets. And organizations of any size could now conduct a wide range of business operations—including e-commerce direct to consumers instantaneously and globally. The world is still adjusting to this computing revolution...

Social commentators dubbed this emerging era "the information age." Indeed, the world had begun amassing information on an unprecedented scale. Whereas data processors in the early 1990s measured their capacities in bytes, by decade's end they had shifted that reference point to terabytes—one trillion bytes.

This rapid accumulation of digital data expanded beyond hardbound, encyclopedic reference materials. Data about individuals' behavior and preferences became much more available and easy to collect on the Web. This trend, at this point in time, became the principal driver in creating what would become a global privacy profession.

Academics and civil liberties advocates warned about the impact of this accelerated accumulation of personal information. Professor of Law Emeritus Alan Westin was one of them. In 1967, Westin published what would become known as the seminal treatment of information privacy in the modern era, the book Privacy and Freedom. In 1972, he followed with Databanks in a Free Society, and his public-opinion surveys—conducted regularly over several decades—by the 1990s indicated a growing loss of consumer confidence in institutions' protection of private data.

Several other notable academics contributed to a growing body of published work on privacy issues and risks during the 1970s and 1980s. Paul Sieghart, a British human rights lawyer and author, published Privacy and Computers in 1976 and Canadian David Flaherty authored a study on government data banks, Privacy and Government Data Banks: An International Perspective. Lastly, Frits Hondius of the Council of Europe wrote Emerging Data Protection in Europe, the purpose of which

was to "describe the dawn of a new corpus of law in Europe called "data protection".

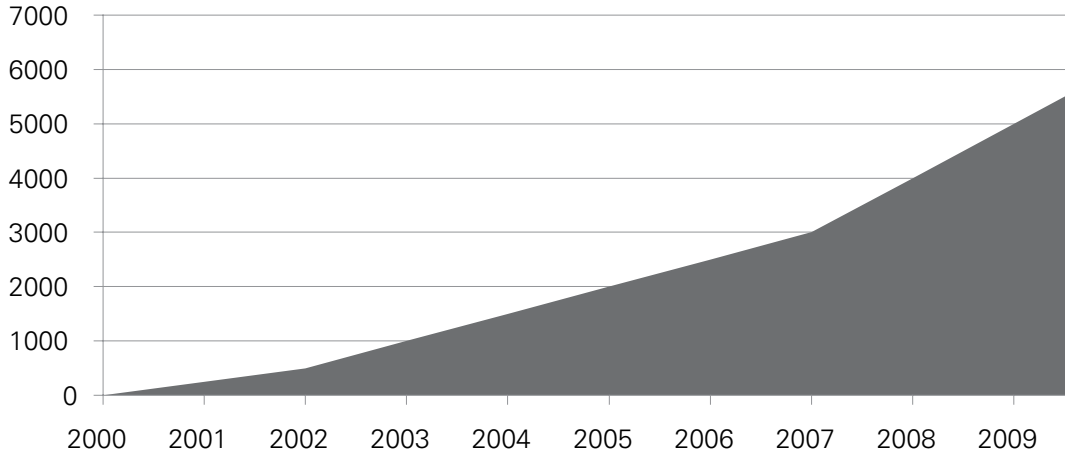
Another privacy pioneer, Washington, DC attorney Ronald Plesser, who began overseeing government-wide compliance with federal privacy law in 1975, warned of the dangers of combining federal and commercial databases. During this pivotal period, several privacy advocacy groups added their voices to the debate:

- The American Civil Liberties Union Privacy and Technology Project, 1986-1993
- The Australian Privacy Foundation, 1987
- Privacy International, London, 1990
- Privacy Rights Clearinghouse, San Diego, 1992
- The Electronic Frontier Foundation, Washington D.C., 1993
- The Electronic Privacy Information Center, Washington, D.C., 1994
- The Center for Democracy and Technology, Washington, D.C., 1994

During the same time period, the Arkansas-based databroker Axciom Corp planted a seed for the nascent privacy profession when, in 1991, it became one of the first organizations on record to appoint a chief privacy officer, Jennifer Barrett. A handful of other credit-reporting agencies and financial institutions also appointed privacy officials, further underscoring the increasing need for a senior professional focused on privacy issues in data management.

In the ensuing years, further technological developments have continued to drive the evolution of the privacy profession. Online social networks, networked digital health records, genetics-based tests and medicines, smart appliances and grids, and cloud computing are among the more noteworthy examples. People and devices are collecting and sharing more personal data than ever before. The dawn of the Information Age has become the late morning, and everyone is wide awake.

IAPP Members



Driver Two: The Regulatory Tsunami

A surge in regulatory developments in the 1990s drove waves of compliance needs that affected numerous organizations. Most of this impact concerned private sector organizations though some countries, often those that started early, addressed the public sector first then later extended into the private sector.

The European Union Data Protection Directive (95/46/EC), was and remains a regulatory epicenter. Enacted in 1995 and effective in 1998, the EU Directive drove the harmonization of data privacy regulation across the newly formed EU. It also "exported" these obligations through its most distinctive feature: a prohibition on the transfer of personal data from the European Economic Area to other jurisdictions required that the transferring organization either have appropriate contractual measures in place, make use of standard contractual clauses and/or ensure that the information was received by organizations in jurisdictions deemed by E.U. officials to be 'adequate'. At the time, very few countries outside of the E.U. had formalized an equivalent manner of data protection legislation with the notable exceptions of Australia and New Zealand, each of which enacted privacy laws in the late 1980s which were modeled around the Organization for Economic Cooperation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" (also known as the OECD Principles).

Beginning in 2000, the legislatures of Canada, Argentina, and Australia passed comprehensive privacy laws. At the same time, the U.S. Department of Commerce negotiated the Safe Harbor Agreement with the European Commission that would enable U.S. companies in most sectors to maintain streamlined compliance with EU transborder data privacy requirements.

The influence of the European approach to privacy regulation continues to be felt beyond the bloc's borders of the twenty-seven EU member states. Russia, India, South Africa, and the Philippines, for example, have studied and in some cases adapted elements of the EU approach in developing their domestic privacy laws.

Early Privacy Regulation Milestones

Several scholarly and regulatory milestones established the foundations of the 1990s wave of privacy regulations.

1890	The Right to Privacy by Louis Brandeis and Samuel Warren
1948	Article 12 of the Universal Declaration of Human Rights
1960	Privacy by William Prosser
1966	U.S. Freedom of Information Act
1967	Privacy and Freedom by Alan Westin
1970	U.S. Fair Credit Reporting Act
1973	Fair Information Practice Principles defined by the U.S. Health, Education & Welfare Privacy Commission
1974	U.S. Privacy Act
1978	France Data Protection Act
1978	First International Conference of Data Protection and Privacy Commissioners
1980	Organization for Economic Cooperation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data"
1981	Council of Europe Convention on the Protection of Personal Data

Europe was not the only regulatory epicenter of the 1990s. The United States—which had inherited a history of privacy concerns distinct from Europe's—was also active. The U.S. Congress passed a succession of privacy laws and requirements that applied to individual business sectors. For example, the Health Insurance Portability and Accountability Act of 1998 (HIPAA) applied privacy and security requirements to the U.S. healthcare and health information management sectors; the Children's Online Privacy Protection Act of 2000 (COPPA) established certain restrictions on the marketing of products and services to children aged 13 and under; and the Financial Services Modernization Act of 1998 (also known at the Gramm-Leach-Bliley Act or GLBA) articulated guidelines around the collection of personal data in the banking and insurance industries in the U.S. Continuing this sector-by-sector approach, the U.S. Congress passed the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM) regulating U.S.-based electronic mail marketing, and Fair and Accurate Credit Transaction Act (FACTA) in 2003, which amended the Fair Credit Reporting Act of 1970 (FCRA) overseeing credit reporting agencies.

Together, the European and American privacy laws enacted between 1995 and 2003 constituted a significant regulatory wave focused on foundational privacy protections. Many organizations suddenly found themselves in need of privacy professionals.

U.S. legislative activity was simultaneously accompanied by a cluster of voluntary self-regulatory initiatives. A group coordinated by Ronald Plesser—the Individual Reference Services Group— by 1997 had adopted privacy principles to govern the data brokerage industry. The Direct Marketing Association (DMA) also was in the process of requiring members to use its "suppression" lists of consumers who had opted out of direct marketing.

This period also witnessed the emergence of trust seal programs and services. TRUSTe launched its seal in 1997, and the Better Business Bureau began offering its BBBOnline seal in 1999. Similarly, a group of large U.S.-based multinationals formed the Online Privacy Alliance in 1998, agreeing to abide by a set of common privacy principles. These quasi-regulatory initiatives contributed to a demand for privacy professionals in the United States, even within sectors not directly regulated by the federal government. Similar efforts emerged in Europe, with the EuroPriSe seal program offering certification for IT products and services, and in Asia with the Asia Trustmark Alliance.

The enforcement efforts of the Federal Trade Commission (FTC) and the state attorneys general were also a factor contributing to a greater demand for privacy professionals in the United States relative to other regions. Between 1998 and 2003, using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, and statutes such as the Fair Credit Reporting Act (FCRA) and COPPA, the FTC investigated and negotiated consent agreements with several organizations for allegedly making statements about their privacy and security practices that departed from their existing practices or violated applicable rule requirements. "The Commission carefully considered information gathered from consumers, businesses, privacy advocates, and other regulators through public workshops and other means, and recognized industry self-regulation as an 'important and powerful mechanism for protecting consumers', but also brought a compelling message regarding privacy compliance for consumers and companies through its education and enforcement activities," explains Dean Forbes, a former FTC prosecutor who worked on the agency's initial privacy and security enforcement actions and is now senior director in the privacy office at Merck, the pharmaceutical company.

Forbes cites as an example a 2000 FTC Report to Congress about online profiling which commended an innovative self-regulatory proposal intended to address privacy concerns

expressed by consumers, but also called for Congress to enact legislation that would complement industry self-regulation and provide privacy protection for consumers with regard to such practices. The agency created the Advisory Committee on Online Access and Security, comprised of industry, government, and consumer advocacy leaders, in an effort to further understand certain Fair Information Practice Principles going beyond "notice" and "choice." Moreover, the agency quickly sought to bring enforcement actions and also designed readily available consumer and business education materials that addressed privacy and security issues for adults and children. The FTC's initiative in this area created a need for U.S.-based organizations to direct resources toward aligning privacy notices with data practices.

FTC Enforcement Actions Addressing Privacy and/or Security Practices

Year	Organization Name
1999	GeoCities
1999	Liberty Financial Companies, Inc.
2000	ReverseAuction.com, Inc.
2000	Equifax, TransUnion and Experian
2000	Rennert, et al
2000	Toysmart.com
2000	Performance Capital Management, Inc.
2001	Bigmailbox.com, Inc., Monarch Services, Inc., et al. (Girls' Life), Looksmart Ltd.
2002	Eli Lilly
2002	Microsoft
2002	Quicken Loans, Inc.
2003	National Research Center for College and University Admissions

Source: www.ftc.gov

A Second Wave of Regulation

The initial wave of privacy regulation, self-regulation, and enforcement between 1995 and 2003 yielded to an aftershock of regulatory activity that continues to this day. In the United States, the second wave of privacy regulation shifted to an acute focus on information security management and data retention. California's breach-notification statute (SB-1386, passed in 2003) triggered, in the subsequent three years, similar legislation in nearly every other U.S. state, most notably in Massachusetts as recently as March 2010. As a result, hundreds of organizations disclosed data security lapses and suffered reputational and financial damage. Thousands more took steps to respond to this new set of enterprise risks. Heightened management attention to these risks often resulted in expanded duties for privacy professionals.

The popularity of breach-notification regulation eventually spread to the European Union, which in 2009 amended its Telecommunications Directive to require breach notification. Also in 2009, the U.S. Congress amended HIPAA to include health information breach-notification provisions via the Health Information Technology for Economic and Clinical Health Act (HITECH). Lastly, Germany adopted breach-notification requirements in 2009, and the French Senate began considering similar rules.

Back in the United States, the information security programs of the payment card brands merged in 2006 into the Payment Card Industry (PCI) Data Security Standard (DSS). The card brands directed their initial focus on enforcement within the United States. Information security legislation passed by the Minnesota, Nevada, and Massachusetts legislatures during this time supplemented the private industry PCI standard, raising the specter of another impending wave of state-level regulations. Meanwhile, new electronic discovery rules approved by the U.S. Supreme Court in late 2006 increased the need for organizations to conduct data inventories and implement data-retention policies.

During this timeframe, the diverse cultures of Asia began to develop a common path on privacy. The Asia-Pacific Economic Cooperation (APEC) privacy framework became the most noteworthy development of broad significance to the region. Approved in 2004, the framework blended fair information principles similar to the OECD guidelines with a harms-based approach to regulatory enforcement. The framework and accompanying commentary provided a source of privacy rulemaking and industry self-regulation for this region.

Some Asian countries have since focused legislation on the information security aspects of privacy. India, for example, in early 2009 enacted comprehensive legislation covering the security of personal information. China followed in late 2009, passing a national level duty to protect personal information. While much of Asia has yet to make a full entrance into the privacy regulatory landscape, its first common steps greatly expanded the horizon of interest for the privacy profession and introduced an approach based less on privacy as a human right than as a useful objective.

In Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA) came into force in stages, beginning in 2001. The act was passed as part of the government's Electronic Commerce Strategy , a policy initiative said to have been motivated by the desire to make Canada a world leader in electronic commerce. It was followed by the Personal Health Information Protection Act of 2004 (PHIPA), Ontario's health-specific privacy legislation, which governs the way personal health information may be collected, used, and disclosed.

The diverse approaches to privacy regulations around the world led to the creation of harmonizing initiatives. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in 2006 released the Generally Accepted Privacy Principles (GAPP Framework) which have become a leading standard for audit and consulting firms.

Today's privacy professionals—many of whom have been hired to help their organizations meet regulatory compliance needs—entered the profession while many of these rules were still being written. To this end, privacy regulation promises to continue to be a driver of change for the profession.

Driver 3: The Rise of Governmental Data Collection

Since before the times of Ancient Rome governments have sought to keep a census of their citizens. This need and ability of governments to collect information about people residing within and passing through their borders developed over time, in different ways, in different regions. But it was in the West where citizens first expressed their desire to institute a control on this power. Indeed, several of the first privacy-related statutes—Article 12 of the 1948 Universal Declaration of Human Rights; the 1966 U.S. Freedom of Information Act and subsequent FOI acts in Canada, the UK, and Australia; and the 1974 U.S. Privacy Act—were focused on the government sector.

As noted previously, these government-focused regulations were the origin of many of the first professionals dedicated full time to protecting personal privacy. Certain agencies—particularly those that interact with citizens directly, such as the U.S. Internal Revenue Service, Postal Service, and Census Bureau—were also working to address broader privacy trends. The roles of privacy professionals in such agencies mirrored those of their industry counterparts: conducting personal data inventories, developing policies and procedures, and completing privacy-impact assessments, for example. These roles continue to this day, and the number of professionals has grown.

They address new legal requirements, such as the U.S. eGovernment Act and develop best practices. Indeed, in the 2010 IAPP Privacy Professional's Role, Function and Salary survey, the government sector accounted for the second-highest number of respondents, most of whom hail from citizen-facing agencies such as the Internal Revenue Service (IRS), Department of Homeland Security (DHS) and the Veterans Affairs Administration (VA). The nature of government data collection and its impact on the privacy profession would take a turn soon after the arrival of the millennium. The September 11, 2001 terrorist attacks and subsequent bombings in London, Madrid, Bali, and other locations, brought into fresh relief for Western publics the power of governments to collect personal data. Following the 9/11 attacks, the U.S. government sought information from airlines, data brokers, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial network, among others, to identify the attackers and prevent future attacks. Massive new databases were proposed. The USA Patriot Act in particular facilitated information collection and sharing among federal agencies. Indeed, prior to the Patriot Act, the Federal Bureau of Investigation (FBI) had been issuing approximately 8,500 National Security Letters each year to obtain information from corporations and others. Following the act, that average jumped to about 50,000.

Similarly, the Third Pillar of the European Union – involving police and judicial cooperation in criminal matters – saw an increase in data collection and sharing among European governments for counterterrorism purposes.

One of the most visible icons of this new era was the surveillance camera. Led by the city of London in the United Kingdom – which had installed an estimated 1.5 to 4 million cameras principally to prevent domestic attacks by operatives of the Irish Republican Army – other cities, including Paris, Copenhagen, Oslo, New York, Washington, DC, Chicago, Winnipeg, Vancouver, and Sydney deployed thousands of new cameras in their public spaces in the years following the 9/11 attacks.

How did the rise of counterterrorism data collection change the privacy profession? In the United States, it added, albeit gradually, a new type of government privacy professional: the civil liberties and chief privacy officer whose key mandate encompasses counter-terrorism and related privacy issues. In 2003, the U.S. Department of Homeland Security became the first agency to be required by statute to appoint a chief privacy officer. It appointed Nuala O'Connor Kelly, current president of the IAPP. Similar positions were subsequently created at the Department of Justice and Office of the Director of National Intelligence. These roles, and the staff that now support them, provide an oversight function that goes beyond compliance with government privacy laws and begins to address some of the public concerns raised in the aftermath of 9/11. While other government privacy professionals continue the yeoman work of administering privacy compliance, these new roles are more visible to Congress and policymakers globally. As Western governments continue to mount coordinated defenses against terror attacks and explore new ways of collecting and sharing information, their citizens will turn to the privacy profession for guidance and support.

Other Driving Factors: Globalization and Economic Uncertainty

While technological advances and new regulations were shaping the need for a new profession, the globalization of world commerce continued, bringing new considerations to the fray. European and American organizations began outsourcing data and call center operations to emerging-market nations, Asia increased investments in the West, large-scale mergers and acquisitions and a heightened competition for all global markets began accelerating the pace of change. "There are few U.S.-only corporations anymore," notes Peter Cullen, CIPP, chief privacy strategist of Microsoft. "Almost all companies of any size now have an international partner somewhere in its value chain."

The economic slowdown that began in the West in 2008 and expanded worldwide by 2009 forced corporations to do more with less, to streamline, consolidate, and gain efficiencies. Privacy professionals were called upon to optimize the value of their organization's data, for example, by facilitating cross-border transfers of data, and by accomplishing their goals with limited resources.

The combination of these two powerful trends — economic activity spreading rapidly across borders and the pressures of doing more with less brought on by the worldwide recession — have pushed information privacy practices into an ever increasing focus. The privacy profession's origins in technology, regulation, and counterterrorism within the context of expanding globalization will continue to shape the trajectory of the profession.

Today's Privacy Professional: At a Crossroads

As addressed in this paper, three dynamics have largely shaped the privacy profession to date: the dawn of the information age, a tsunami of privacy regulation, and the rise of governmental data collection. In addition, growing scrutiny of data security breaches and an increasingly intertwined global economic marketplace have exerted additional influences on the scope of the privacy role.

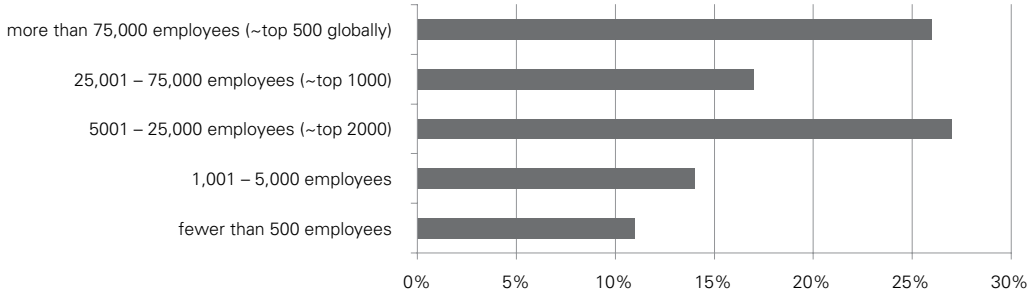
The profile of today's privacy professional suggests a role in transition. This change is being driven by a number of factors: Organizations of a growing variety of sizes are employing privacy professionals ("organizational diversification"); the profession is expanding outside its North American locus ("regional diversification"), privacy professionals are being positioned at many organizational levels and in a variety of functions ("migration across the organization"); and while most professionals see their responsibilities changing or expanding in the coming year many common tasks remain intact ("stabilization of daily privacy tasks").

Organizational Diversification

In the first 10 years of the privacy profession, large organizations—those ranking in the equivalent of the top 2,000 companies worldwide—employed the lion's share of privacy professionals. In the 2010 IAPP salary survey, three quarters of respondents worked for organizations with more than 5,000 employees. This is likely because only large organizations thought they could afford a privacy leader.

But even this is starting to change. As the risk of noncompliance rises for organizations of all sizes, small- and medium-sized organizations are starting to adjust their cost-benefit analysis on hiring data protection and privacy experts. "I think we are already seeing a trend where many medium-sized firms now also rely on a privacy professional," notes Zoe Strickland, CIPP/G, chief privacy officer at Walmart.

Today's Privacy Professionals are Concentrated in Large Organizations



Source: Benchmarking Privacy: An Executive Summary and Forbes Magazine Global 2000.

It's a trend that seems likely to continue and grow further. According to credit card issuer VISA more than 80 percent of credit card breaches occur at the smallest level merchant. Each breach carries with it the potential for fines originating from the payment card brands, as well as more costly compliance obligations. Smaller companies that provide services to larger corporations are also falling within the purview of the larger corporations' vendor-assurance programs, which are dictating privacy requirements to them.

"At IAPP events we're already seeing more people from small- to mid-size organizations," added Sandy Hughes, CIPP, global privacy executive at Procter & Gamble and past president of the IAPP.

This shift could significantly change how the privacy profession meets and learns and what issues become its top priorities. The complex organizational challenges of large multinationals may be joined by the more tactical and sector-specific realities of the small business.

Regional Diversification

In the first decade of the privacy profession, most professionals were employed by North American organizations. This may seem counterintuitive given that EU member states were the first to enact national data protection laws. Why wouldn't Europe dominate the profession? Some observers have noted that North American businesses, particularly those in the United States, have a commercial custom of collecting more information about people than their European counterparts and therefore have more information risk to be managed.

"Our benchmarks show that European companies collect less personal information about customers," Larry Ponemon, founder of the Ponemon Institute, explained in a related study, "and [they] are less likely to use this information for unrelated, secondary purposes."

So the North American appetite for data may have led to a high concentration of privacy professionals on the continent. But some suggest the numbers could be deceiving.

Bojana Bellamy, Accenture's global data privacy compliance lead, offers another perspective. "European companies do employ privacy professionals and have done so for 10 years," she said. "But the role is not at the level of the U.S. based CPO." In Europe, it is more legally and compliance focused, she says, often sitting in the legal department or mid-level management. Although I do believe this is starting to change - following some high profile data breaches in Europe the role has become higher level and more strategic."

Deirdre Mulligan, a former privacy advocate and current assistant professor at the University of California School of Information, agrees. Says Mulligan, "to a greater extent than in other geographies, the most strategic and high-level privacy officers tend to work for U.S.-based organizations where they are tasked with creating and deploying sophisticated information-governance strategies for highly visible brands."

"There are interesting directions being taken right now in the transatlantic debate," notes Malcolm Crompton, managing director of Information Integrity Solutions and former privacy commissioner of Australia. "A new dynamism is emerging—a more questioning approach on what might work because there is a feeling that more work is needed."

Nonetheless, the profession continues to evolve. The number of non-U.S. members of the IAPP has increased over the past several years. Moreover, the respondents to the IAPP salary survey showed an even greater diversification outside the U.S. The adoption of breach-notification requirements across Europe and Asia could accelerate the diversification of the profession, as organizations become compelled to make their data practices more transparent to the public. If the center of gravity of the privacy profession shifts from Washington and Ottawa toward Brussels, Buenos Aries, and Beijing, the profession will likely get an injection of fresh new ideas on how to conduct privacy assessments, how to document and communicate privacy policies, how to hold vendors accountable, and even how to define what privacy is.

"When I'm speaking to business partners about the importance of privacy," said Sandy Hughes, "the argument of ensuring trust among constituents seems to resonate more in the U.S., in my experience, than in Europe or Asia where whether a country has a law or not seems to be the first concern."

"In Europe, satisfying laws and regulations seems to be the primary focus. Similarly, in Asia, a common first response to a privacy requirement of mine is 'well it isn't against the law' to do such and such. However, when I share data that shows consumers do care about privacy the trust argument does work outside the U.S."

"We share more fundamental values about respect for fellow human beings than we differ over," notes Nuala O'Connor Kelly. "There is a "We share more fundamental values about respect for fellow human beings than we differ over," notes Nuala O'Connor Kelly. "There is a common desire for decency in the private zone that we can all build upon."

"I never use the word 'privacy' in Asia," explains Michelle Dennedy vice president of security and privacy solutions, Oracle Corporation. "'Information strategy' works better."

In Canada, privacy regulation is based on an ombudsman model, where the emphasis is less on court action than on dialogue, guidance and the search for better business practices.

"Indeed," says Canadian Privacy Commissioner Jennifer Stoddart, "One of the most interesting trends in that country is the evolution of 'soft law.' Emerging in the space between the traditional legislative and judicial branches of government, soft law uses tools as model codes, best practices, informal dispute resolution processes, and alternate modes of redress."

"It's widely argued that the adversarial court system is no longer as appropriate for the kinds of issues we face," notes Stoddart. "It's too cumbersome and costly, and the courts may not be set up to grasp the intricate, specialized issues that are our bread and butter."

The profession could be ripe for a paradigm shift as it becomes fully international.

Migration Across the Organization

The first companies to appoint chief privacy officers in the late 1990s and early 2000s typically placed these leaders within senior positions but with limited budget and staff. A lot has changed in 10 years. While large multinationals and government agencies still employ high-ranking CPOs, more than half of the respondents to the 2010 IAPP salary survey indicated that they were positioned below the director level in their organizations. This suggests that there is no longer a single recipe model for privacy professionals' placement within an organization. It could also be indicative of a growth in privacy departments across multiple levels.

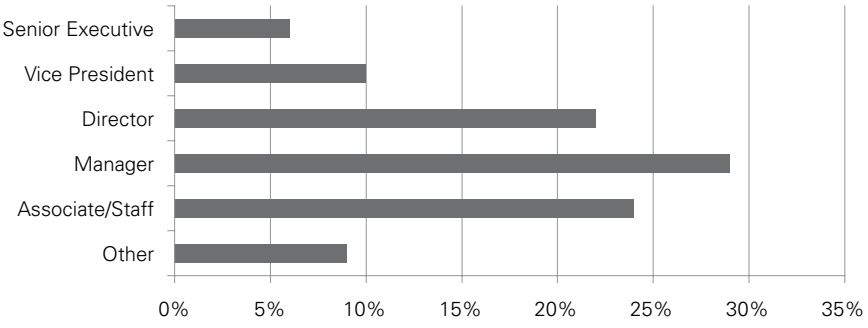
"It takes a team to develop and then to support an organization's implementation of information privacy policies," adds Harriet Pearson, CIPP, vice president security counsel & chief privacy officer at IBM. "Our team members come from a wide range of disciplines and levels, but we're united by our common strategy."

Today's privacy professionals also find themselves in a variety of departments. Three reporting structures are emerging as dominant:

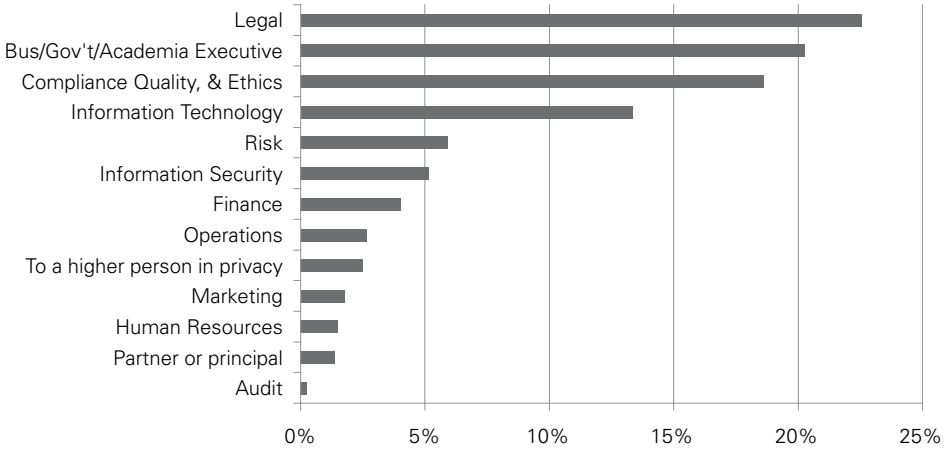
- reporting up through the general counsel
- reporting up through a business executive
- reporting up through the chief information officer

The heightened risk of privacy noncompliance —of data breaches in particular—has probably contributed to the focus on the legal and compliance areas.

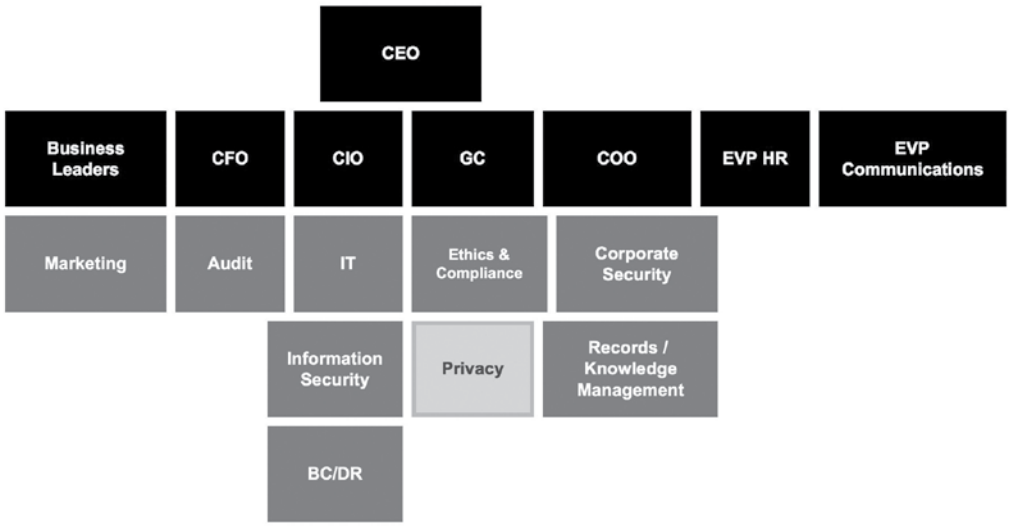
Today's Privacy Professionals are Positioned at All Levels in the Organization



Privacy Professionals Report through a Variety of Functions

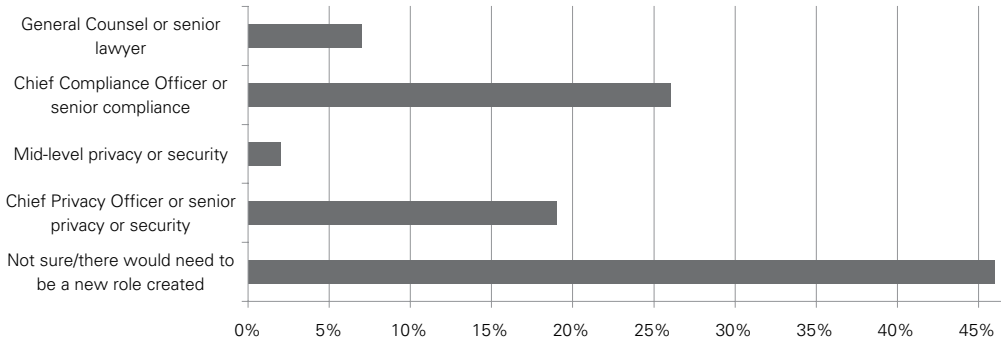


Many corporate privacy professionals find themselves within a structure similar to that depicted below, where privacy reports in through legal or compliance and information security reports in through the CIO.



But the information governance organizational structure is in flux, and as a result, today's privacy professional is at a crossroads. Indeed, 53 percent recently reported that they expect their job responsibilities will change in the next year or two. Most believe that promotion possibilities depend upon the creation of a new role in the organization. Short of creating a new role, privacy professionals responding to the IAPP salary survey indicated a desire to assume responsibility for data security as well.

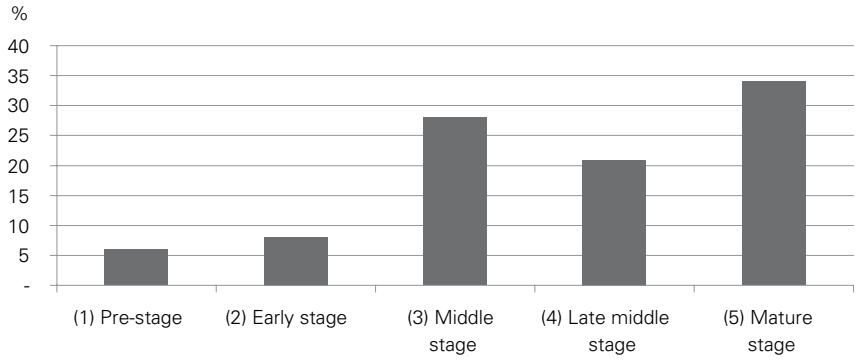
Likely Next Promotions of Today's Privacy Professionals



Stabilization of Daily Privacy Tasks

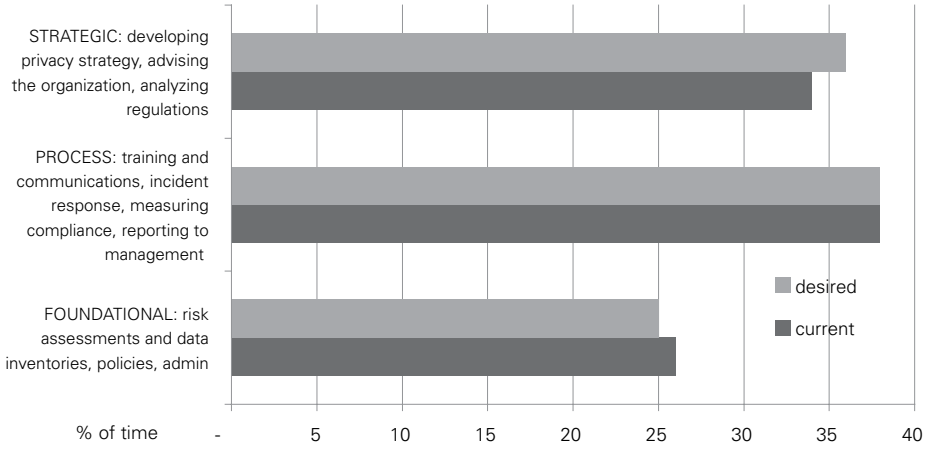
In the last 10 years, many privacy professionals have been focused on developing policies and procedures and responding to incidents. As a result, many of the privacy programs led by privacy veterans may be reaching maturity. A full 34 percent of the respondents to the IAPP's Privacy Professional's Role, Function and Salary Survey (2010) say their privacy programs are in the mature stage, and 49 percent say they are in the middle or late-middle stage.

Privacy Professionals Rate Highly the Maturity of Their Programs



When asked where they currently spend their time versus where they wish they could spend their time, respondents to the survey said they had found the right balance between foundational, process, and strategic tasks. This is an indicator that the privacy professional's daily tasks may be arriving at some predictability. It may also suggest that privacy professionals are self-directed, and have a good amount of control over establishing and prioritizing work items.

Privacy Professionals Spend One-third of Their Time on Strategic Tasks and Desire Slightly Higher Share



That said, the daily tasks of the privacy professional are not on the verge of becoming stale. "Most organizations today are in constant flux; changing products, business, employees," explains Kirk Herath, CIPP/G, chief privacy officer at Nationwide Insurance Companies. "Governing this will continue to mean updating policies and procedures and monitoring legacy programs."

"There will always be work in the program-build area as programs seek to improve, and as underlying laws and risks change," adds Zoe Strickland. "However, privacy programs will

indeed mature. That will allow the privacy leader to work strategically, beyond compliance, regarding the management of personal or business data."

Richard Purcell, former chief privacy officer at Microsoft and presently founder of the Corporate Privacy Group, sees much more work to be done. "An important question before us as we look forward to the next 10 years is this: 'How can we establish accountability and self-discipline while maintaining localized autonomy?'" Purcell says one answer may lie in, "how well we separate ourselves from the bad actors and free riders through stronger and more harmonized policy frameworks, compliance practices, and accountability standards."

Anecdotal evidence from privacy consultants operating across multiple sectors and geographies suggests that corporate privacy programs have been maturing over time, but at different paces in different regions. Canada has been a noteworthy leader. "I look to Canada frequently to see the future of where we're going," notes Michelle Dennedy, Oracle's vice president of business development for privacy and security.

A number of factors have spurred North American (and particularly American) organizations to dedicate more resources to privacy process improvement: most notably, PCI DSS enforcement, FTC enforcement, and data breach notification. Emerging enforcement and data breach notification in other OECD countries has prompted privacy process improvement there, too, but to a lesser degree. "The privacy process focus in Europe, driven in part by database registrations and compliance with certain other country-specific requirements, has prompted a different approach to resource allocation for privacy and data protection issues than in the United States," explains Dean Forbes, CIPP, senior director of the privacy office at Merck Corporation. "But that may change with additional focus on data breaches and related enforcement."

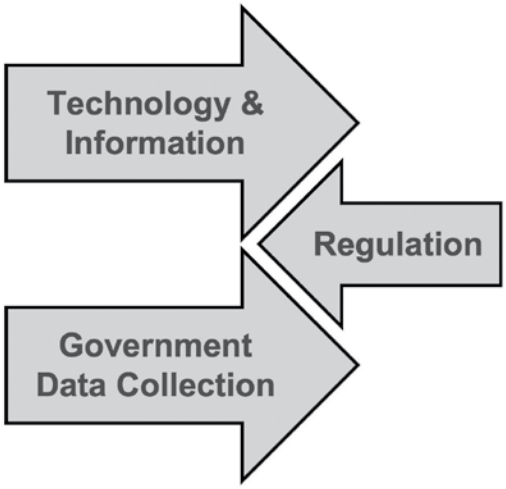
A lack of enforcement and resources at other organizations has left them in the earliest stages of privacy maturity. Maturity levels may also be varying geographically, potentially causing the agendas of privacy professionals to vary by region. Regardless of the sector, region, or position in the organization, following a transformative decade, today's privacy professional is poised to take advantage of an expanding horizon of opportunities.

The Privacy Profession in 2020

Predicting specific outcomes, even near-term outcomes, with any level of accuracy is difficult. Given the known drivers that have shaped the profession's first decade and the current state of transition in which privacy roles appear to be, we offer some possible scenarios for the privacy role circa 2020. The trajectories of the original drivers of change offer some plausible outlines to consider.

Technology and Information

One of the clear directions of technology in the past 10 years as it pertains to personal data has been more—more types of data collected from more people in more ways, and shared with more entities. The emergence of cloud computing—essentially a new computing paradigm in which data is stored off-premises and by a range of third parties—sets the pace for the next decade. Short of a wholesale social movement to opt out of information technology and "go dark," the conveniences and commercial benefits of more data collection and sharing seem to point in the direction of more. People will not "go dark," we estimate, because the utility of sharing information will continue to well exceed the risks of doing so. If the collection and sharing of personal data will increase over the next 10 years, will we approach an age of near-perfect information about ourselves and one another? If so, what will that mean for the privacy profession?



Nuala O'Connor Kelley, CIPP/G, chief privacy officer at General Electric and current IAPP president, and Oracle's Michelle Dennedy together draw a picture of daily life for tomorrow's privacy professional as it may appear in the not-so-distant future…

I*magine waking up in the morning, not because of an alarm clock, but because your bioalarm identified the peak time within your REM cycles to awaken you fully refreshed. You jump on the treadmill and it sends your exercise performance and bio-readings over the Internet to your personal health record (PHR). You grab some orange juice from the refrigerator, which records the amount taken via an RFID reader. It also sends that information to your PHR and updates your weekly grocery list, which is stored on your handheld device. The monitor in the kitchen displays all the social network updates and news stories—translated from foreign news organizations around the world—that it has learned you are most interested in. It has also prioritized all your incoming e-mails, texts, and voicemails from the previous eight hours based on your past message management. At the top is a meeting invite from your doctor, who would like you to come in to receive your DNA-personalized nutritional supplements and anti-carcinogen nanobots, and also talk about the cholesterol alerts he's been getting from your PHR. You hop in your electric car, which recharged at two o'clock that morning at the direction of the smart grid. You drive, obeying the posted speed limit, knowing that your insurance company will drop your rate if you do so. As you pass by your dry cleaner, your car's speakers sound an alert to let you know that your suit is ready. It's only nine in the morning, but you've already generated a terabyte of data in your personal account in the cloud.*

While such a scenario may incite a certain degree of consternation, if not alarm, in the eyes of privacy and consumer protection advocates, it remains a very possible extension of capabilities that technologies and systems offer today. Quite simply, if people do embed these types of innovations into their daily lives, a new role may materialize: the privacy engineer.

Companies that hope to market their innovations to a public more informed about their privacy risks will need to hire engineers who are also privacy experts. Their task will be to "bake in" privacy to their product designs.

The accumulation of sensitive personal data on the scale illustrated in the scenario above may also give rise to a new market niche: the personal privacy planner. This person could help erase past mistakes, monitor the public persona, and check on the security of the personal data account. If this development occurs, the privacy profession in 10 years may well expand out of organizational compliance into direct-to-consumer assistance.

In 2010, "there will be more technology in the hands of consumers," predicts Zoe Strickland. "This will range from simple RFID codes on products for easy returns, to complex and integrated applications offered through mobile devices." At the same time, Strickland adds, companies and other entities will have even more sophisticated back-end technologies to aggregate and analyze data from disparate sources. "Technology will absolutely remain a key driver for privacy."

Brian O'Connor, chief security and privacy officer for Eastman Kodak Company counters that this may only amount to a "numbing crush of boring information. At some point," he says, "there may be so much information out there that a data thief has a hard time finding anything usable."

Where the first chapters in privacy were defined largely by privacy notices, breach notifications, and international data transfers, Jim Koenig, practice leader of privacy and identity theft at PricewaterhouseCoopers, feels that the next era will be defined by corporate organizations and increased marketing sophistication as well as developments in health information technology. "Privacy will be profoundly shaped by companies desires to share information for business intelligence and derive revenue from direct and interactive marketing, the increasing inclusion of specific security controls in privacy laws, and the changes and investment in healthcare information used and the advent of electronic health records." he says.

Certainly, the privacy professional plays a key role in managing the data privacy issues inherent in any future scenario. The question for the next decade will be 'How many of the remaining 75 percent of the world not now online will become Internet users?' And how many people will participate in online social networks and media, or other connected technology? These questions raise another: What role will the privacy profession play in the globally networked civil society? Will the profession passively observe the phenomenon? Or will it take an active role in building trust in the Internet ecosystem? The path the profession chooses could well determine whether privacy will be viewed as something bad that happens to you, or an enabler of new horizons.

The Future of Regulation

As long as citizens and consumers remain concerned about their personal information and legislators see an issue to be addressed, new privacy laws will be enacted. Looking out to the year 2020, what part of the privacy arena that is currently unregulated will catch the attention of legislators?

"Employee privacy in the United States," notes Agnes Bundy Scanlan, CIPP, chief regulatory officer of TD Bank North America and former president of the IAPP.

"Corporate video monitoring in the U.S.," says Brian O'Connor. "This is already hard to do in Canada and Europe."

The "Internet of things" may continue to come under regulatory scrutiny, speculates Sandy Hughes, referring to smart devices such

as sensors and RFID that communicates to and from humans and with one another to provide conveniences and efficiencies for consumers. "Right now the opportunities, economics, and technology are still developing, but that could speed up dramatically," she explained.

"Compliance-driven information security requirements will very likely increase in the coming decade," says IBM's Harriet Pearson.

The popularity of security breach notification has already gained traction in Canada, the United Kingdom, Germany, France, Australia, New Zealand, and Japan, and could well expand to all OECD countries. If breach notifications expose underlying weaknesses in corporate data practices, the laws could trigger a second wave of information-security regulation. Similarly, the success of the PCI Council in enforcing the PCI DSS in North America could result in enforcement of the standard in Europe, Asia, and beyond.

Canada's voluntary data breach notification guidelines, introduced in 2007, have been generally well received, because industry was integral to the process.

"We consulted broadly in the development of the guidelines, and we followed up with detailed interpretive documents," said Stoddart, the federal privacy commissioner. "We recognized that businesses are more likely to confess to serious data breaches if they have clarity on what is expected of them." Building on its experience in voluntary notification, Canada is now preparing to roll out a mandatory reporting regime.

The prominence of the European market and the requirements of the EU Data Protection Directive may well continue to persuade new countries to adopt national data protection laws. South Africa and Malaysia are already poised to do so and other APEC and Latin American countries might then find it more difficult to remain unregulated.

"Legislation will continue to increase," notes Brian O'Connor. "This will be a significant compliance issue, requiring privacy professionals to drive corporate programs."

As more countries regulate privacy, and if privacy is regulated across more sectors and technologies, will world privacy regulations begin to converge? Opinions vary.

Zoe Strickland sees convergence. "As rules converge, they will be principle-driven and technology neutral," she explains.

Jennifer Stoddart, now in the final months of her seven-year term as Canada's federal privacy commissioner is encouraged by the many initiatives underway that are seeking common ground among regulators. "A single, enforceable global standard for privacy won't materialize overnight, if ever," she says. But we are seeing a very determined push—in Europe, the Asia-Pacific region, within the OECD, and even in the U.S.—toward a more consistent and collaborative approach to the protection of personal information."

Stoddart notes that important global corporations have embraced these initiatives and are active in the dialogue. "They understand that a set of well-understood regulations, common to major jurisdictions, would bring a measure of legal certainty," she says. "That would promote both data privacy and robust global data flows."

Kirk Herath and Brian O'Connor, on the other hand, see further Balkanization of privacy laws into conflicting local and regional variances. But Jeff Green, chief privacy officer at Royal Bank of Canada, takes a middle ground. "I don't hold out a lot of hope for perfectly harmonized global regulations," he said, "but I think we'll continue to see a convergence of the key requirements found in the patchwork of laws and regulations already out there."

Sandy Hughes takes a similar stand. "I see more convergence of privacy frameworks, but continued local regulations. Ideally, if a company follows the framework it should get a 'free pass' for some of the local requirements in countries who recognize the framework."

What does this mean for the privacy professional of 2020? More laws in more places mean an extended role for legal experts both inside and outside of corporations, governments, nonprofits, and universities. It also means new positions within government agencies to enforce the new laws.

A landscape of conflicting privacy laws could leave the privacy profession mired in a protracted period of untangling the conflicts and adding less value to organizations and society. A Balkanized regulatory landscape could leave organizations viewing their privacy professionals as necessary tacticians, but not strategists invited to the planning table. To avoid this perception, "today's CPO needs to think broadly beyond legal terms and more about information risk and social impact," says Peter Cullen of Microsoft. Michelle Dennedy of Oracle Corporation believes it's incumbent on privacy officers to take the initiative. "It's up to us to be more strategic and less reactionary," she says.

The increasing importance of a proactive approach to privacy is a message frequently delivered by Ontarios Information and Privacy Commissioner Ann Cavoukian. "Fifteen years ago, taking a strong regulatory approach was the preferred course of action—but no longer. "Over the years, I have argued that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must come from making privacy the default within technology, business practices and networked infrastructure."

Richard Purcell thinks corporations can forestall more regulation through more comprehensive approaches to information governance. "At the end of this decade of growth in the professionalization of privacy and data protection," he explained, "there have been a number of leading companies such as Microsoft, HP, IBM, GE, Intel, Oracle, and Schering-Plough that have established enterprise-wide programs to manage personal information in strategically smart and responsible ways." He added that these approaches "have helped to diminish the appetite and perceived need for legislative and regulatory interventions."

If organizations continue on a more fragmented approach toward information governance, however, Purcell sees more regulation in the future. "That tolerance for independent judgment and decision (within autonomous operating units) may have the unintended consequences of data breaches and regulatory non-compliance that invite external control."

Nonetheless, ongoing regulation could have the indirect positive effect of propelling the upward maturity of privacy programs across all regions. Law firms, consultancies, and technology vendors serving privacy professionals in this scenario would face a market of increasing but still varied levels of privacy maturity. In order to remain competitive, they would need to offer high-end products and services to the North American, European, and some Asian markets, and foundational products and services to emerging markets.

At the same time, a rising awareness among small- and medium-sized businesses of the need for privacy compliance would generate new markets for delivering privacy products and services in a mass-produced, low-cost manner. As privacy compliance needs spread to new geographies and the vast market of small- and medium-sized businesses, today's privacy professionals will be best poised to compete for these new career opportunities.

Governmental Data Collection

A more speculative future lies ahead for government agencies' exploration of new information technologies and the potential citizen response. Two scenarios could unfold, with differing impacts on the privacy profession. The table below portrays how we chose these two scenarios from among four potential intersections between government data collection and public response:

Increased Government Data Collection	Scenario 1: Most likely	Scenario 2: Next most likely
Decreased Government Data Collection	Unlikely	Less likely
	Backlash (strong public reaction)	**Acceptance** (minimal public reaction)

The actions of many governments around the world suggest more not less collection of personal data as time goes on. Examples of Initiatives already in progress include: the implementation of new national ID cards, expansion of health information networks, and more intensive collection of air passengers' data. With this variable constant, a differing public reaction to these trends might alter the course of the privacy profession.

Scenario One: Backlash

In this scenario, government agencies and related parties continue the initiatives noted above to advance information technologies toward the fulfillment of their missions. But they take it a step further. In order to achieve healthcare cost reductions for example, agencies use access to patient data to identify at-risk individuals whose health could be improved by an early medical intervention. To achieve energy conservation and greenhouse gas-reduction goals, agencies monitor households' consumption levels and intervene when households exceed allowable limits. A new round of terror strikes could heighten government monitoring of commercial transactions. Tax agencies use advanced computing power to greatly increase the ratio of audited tax returns, and political candidates use advanced databases to engage in microtargeting of individual voters. Taken as a whole, in this scenario the individual citizen perceives a dramatic loss in freedom and lives each day with a growing sense that he is under siege.

What if civil societies subjected to these types of advancements in government data collection marshaled a strong reaction? A couple of outcomes could affect the privacy profession. First, demand for greater accountability and restriction of agency data practices could result in a surge of demand for privacy professionals inside agencies as well as on oversight boards. According to Bundy Scanlan, "Any tightening of homeland security measures that involve more intrusive use of personal data could lead to more calls for government privacy protections."

Second, citizens could seek to take matters into their own hands and shield their data from the government. Their fears could increase demand for privacy enhancing technologies.

Scenario Two: Acceptance

In this scenario, government agencies continue the initiatives noted above, but do not pursue the individual targeting and monitoring outlined in Scenario 1. They collect more data, but do so in a way that is moderated by transparency and privacy best practices.

A greater likelihood is for citizens in this scenario to accept the benefits of their governments more efficiently accomplishing their missions, as weighed against only an incremental change in the quantity and types of their data that would need to be disclosed. With only a minimal public reaction to these changes, privacy compliance becomes a routine part of government administration, and government data collection fades as a driver of change for the profession.

The Agile Privacy Professional: A Call to Action

If regulation, information technology, and government data collection continue to shape the profession, how can today's privacy professional take full advantage of the emerging opportunities? According to the experts, more agility is a must. The agile privacy professional, amid a period of ongoing transformation, will be able to clearly identify new opportunities, move to these, and manage them responsibly.

What defines the agile privacy professional? And what can today's privacy professional start doing now in order to successfully achieve agility in the future? The IAPP sees five strategies for action: (1) Redefine the privacy role; (2) Rotate through departments/business units; (3) Develop multi-cultural literacy; (4) Understand legal and technical disciplines; and, (5) Instill direction and leadership. Any one, if not all, of these strategies will enable today's privacy professional with greater agility in confronting the privacy challenges of the next 10 years.

Redefine the Privacy Role

As organizations struggle to determine where to place privacy in the organization and with what responsibility to endow it, opportunities will emerge for agile professionals to provide answers. Experts interviewed for this research believe that the role of the privacy professional will grow beyond regulatory compliance into the information risk arena and, finally, into information governance and information optimization. In this scenario, the privacy discipline becomes a subset of the broader practice of minimizing the cost of information and maximizing its value. Above the chief privacy officer, chief information security officer, and records-management director will be an information optimization officer. Agile privacy professionals will socialize these concepts and seek sponsors and advocates.

"The percent of usable information among all of the noise that we're collecting is going down," says Michelle Dennedy. "Tomorrow's privacy professional will need to help articulate the value of information and then what would be a reasonable cost to protect it."

"I think privacy becomes information governance," echoes Bundy Scanlan.

Many feel that privacy programs and enforcements will evolve to focus more on data usage versus data protection. Jim Koenig of PricewaterhouseCoopers sees integrated frameworks emerging versus the more siloed, law-by-law regulatory approaches often seen today. The health information industry offers an example. "Healthcare companies, given the change in information uses and investments from ARRA/HITECH (the American Recovery and Reinvestment Act of 2009 and the HITECH Act of 2009), will help to set best practices versus financial institutions and retailers who are historically known for this," says Koenig.

Commissioner Ann Cavoukian, believes that there is a real opportunity for privacy professionals to adopt a new role of "privacy ambassador", within their organization. "… privacy professionals can advance the goal of proactively embedding privacy into their organizations' programs. And if privacy is proactively designed into technology, business practices, and infrastructure right from the outset, then the maximum degree of privacy protection can be ensured."

Rotate Through Departments/Business Units

Today's privacy professional is adept at meeting compliance requirements and crafting policy, but the agile privacy professional of the next decade will rotate through business units and field operations where higher level decisions about information management are being made and implemented. Privacy professionals who embed themselves where value is created in an organization will expand their network and influence the role their organizations play in building trust in the global information ecosystem and with stakeholders. Those who don't will risk being among the last to know about critical changes to business strategy and information uses.

"Business experience is probably the most important success factor for tomorrow's privacy professional," says Sandy Hughes. "You can always learn the privacy requirements afterward. The best way to obtain this business experience as a privacy professional is to conduct an inventory of where and when and how personal data is collected and used." "It's important to signal your willingness to take on broadening experiences," adds Harriet Pearson. "The fact that I've had assignments in legal, human resources and public affairs has enhanced the perspective that I bring to my responsibilities."

"Anti money laundering and healthcare expertise" will be increasingly valuable skill sets for privacy professionals to obtain, adds Bundy Scanlan.

Develop Multicultural Literacy

As privacy regulations take root in a greater number of jurisdictions around the world and as the value chains of organizations further internationalize, privacy professionals—particularly those based in the more culturally homogenous North America—may face a crossroads. The privacy professional of today may be inclined to completely delegate questions of local concern to local subject-matter experts and local privacy champions. Western leadership training often teaches the value of delegation, after all. But an agile privacy professional will see opportunity in understanding how variances in culture create variances in information risk and optimization. After acquiring this understanding, the agile professional will be able to communicate strategy, policies, and solutions across cultural boundaries.

"I see four success factors for tomorrow's privacy professionals," notes Nuala O'Connor Kelly. "One, making the case for privacy in positive, measurable terms. Two, obtaining cross-functional talent beyond privacy. Three, obtaining enough knowledge about technology and data systems to ask probing questions. Four, gaining international experience and cross-cultural literacy. This will only grow over time."

"You may not need to speak the local language, particularly if you collaborate with colleagues in local markets whom you may help train to be knowledgeable in and accountable for privacy and security issues as part of their jobs," says Merck's Dean Forbes. "But you will need to listen, work to understand the cultures of these colleagues, assess reasonably foreseeable risks, and prioritize and provide direction accordingly to cross-functional global and local teams to address such risks in relevant areas of their business operations."

Understand Legal and Technical Disciplines

While there is little debate as to whether privacy professionals ought to have a basic grasp of legal and technical concepts around data privacy and security, experts' opinions diverged on whether tomorrow's privacy professional would by necessity need a legal or technical degree. The central role of regulatory and IT drivers shaping the privacy profession almost ensures an ongoing need for privacy professionals to be conversant in not one, but both of these disciplines. Some may indeed become mid-career attorneys or mid-career masters of information systems. The most agile privacy professionals may also recognize the need to pursue literacy in finance and economics in order to quantify the value of information.

"One of the interesting things about the privacy profession is how many disciplines can provide useful background," says Zoe Strickland. "Legal or IT experience is common. Other desirable backgrounds, depending on the goals of the organization, are marketing, customer service, compliance, and communications." "Knowing more is always better than knowing less," says Kirk Herath. "Privacy is inherently legal and, in my humble opinion, a law degree is extremely helpful in this space, as is at least a good understanding of technology."

"We need two types of privacy professionals," proposes Michelle Dennedy. "One, the great lawyer who is a tactical, focused specialist. Two, the broad-thinking, stragetic person who integrates technology, law, marketing, and sociology."

Bojana Bellamy counters, "I believe the real privacy professional does both. I think this is somebody with a legal degree or background who has transcended a pure legal-advisory role and has become a trusted business advisor, as well as a complaints ombudsman, technologist, strategist, and government-relations person, a diplomat."

Instill Direction and Leadership

Many things change, but some remain the same. Amidst continuing change, organizations will need charismatic strategists who can lead, persuade, persevere and provide stability. And with a forecast of ongoing regulation, the effective privacy leader will be a public speaker who works a vast personal network of legislators, industry groups, and standards bodies to articulate a vision and position.

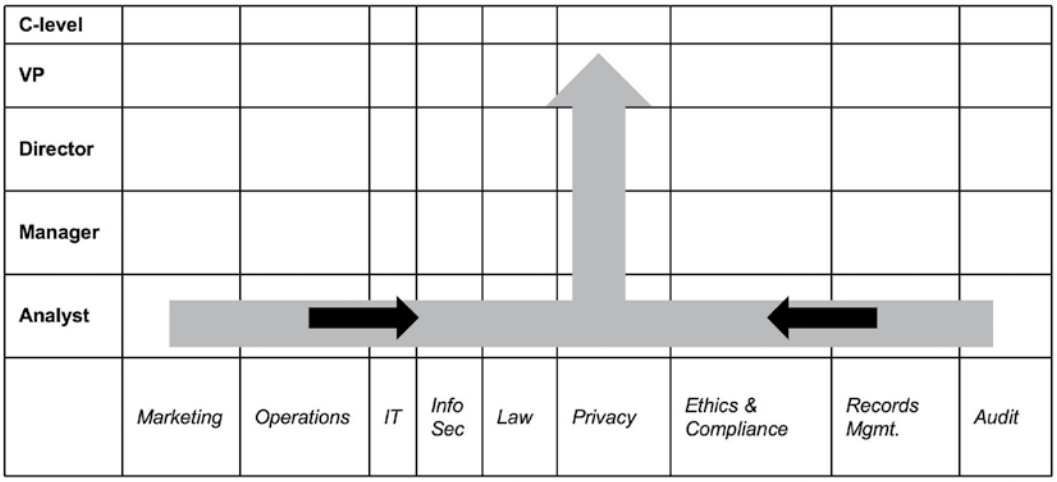
"Strong leadership abilities will be the biggest success factor for privacy professionals in the future," notes RBC's Jeff Green. "To be successful, they must be able to influence across all lines of business and the operational and functional areas that support them to drive a consistent approach to information governance."

Agile Privacy Career Paths

Career development tracks for the agile privacy professional will likely follow one of several discrete paths. As privacy questions bleed into new parts of organizations, sectors, and geographies, the privacy professional of the next 10 years might well see themselves choosing one the following options.

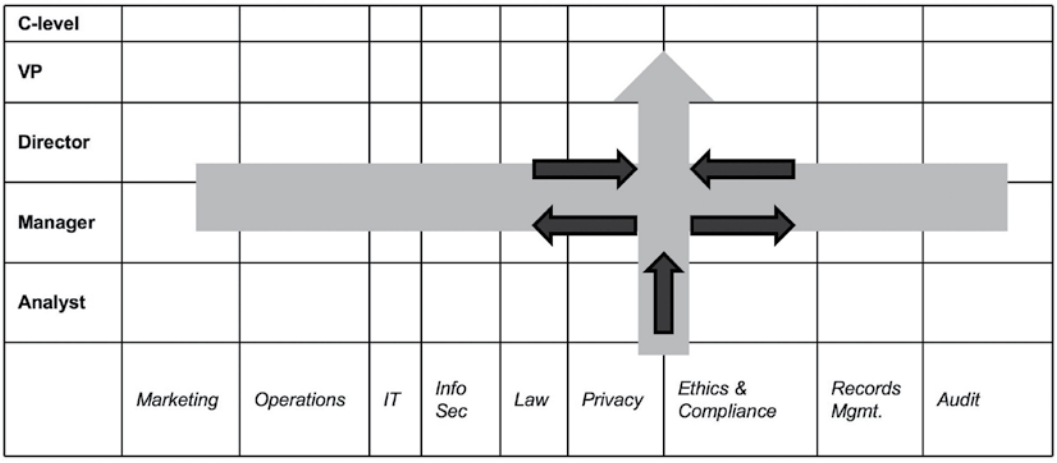
Path 1: Start anywhere, and rise through privacy

In this scenario, the privacy professional follows a traditional ascent up through a privacy program. Getting a start anywhere in an organization, this person gravitates toward the privacy department and becomes a master in the privacy discipline. Depending upon the sector, size, and geographic reach of the organization, an entire career could be spent building and maturing a privacy program.



Path 2: Create rotational experiences that remain centered on privacy

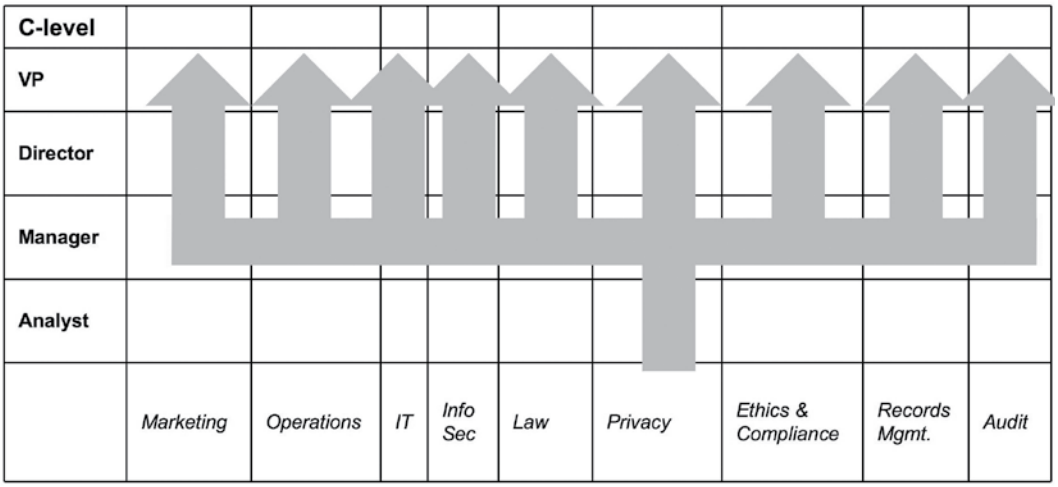
In this scenario, a privacy professional seeks one or more opportunities to spend time in other departments or business units before coming back to the privacy program. In larger privacy programs where there is competition for the top privacy job, these types of rotational experiences may prove to be the differentiators in demonstrating greater leadership potential.



"Data-intensive businesses may need a more complex privacy organization with career paths," says Brian O'Connor. "Other businesses that only collect routine personal data for basic marketing and finance functions will gravitate toward smaller privacy functions, often integrated into the IT or Legal organizations."

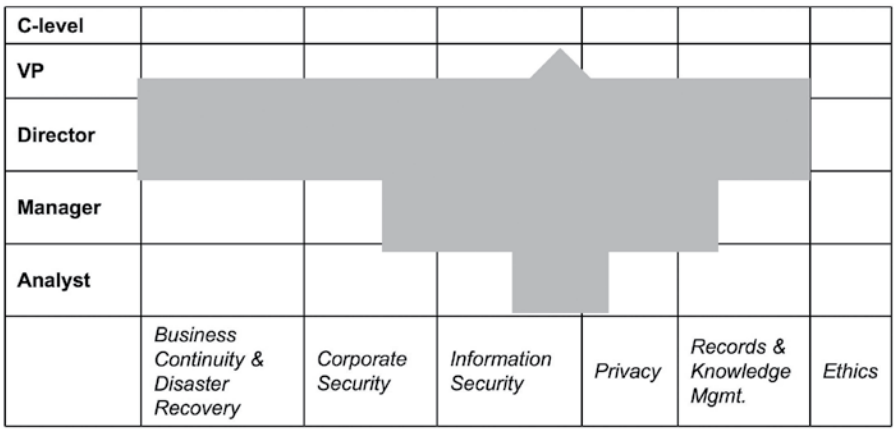
Path 3: Start in privacy, move to anywhere

On this path, a privacy professional is sought after by other organizational functions that need to embed privacy into their DNA. Rather than being rotational experiences, this time outside the privacy program becomes a launching pad for an entirely new career where privacy becomes a differentiator for excelling in the new discipline.



Path 4: Grow the privacy function

There has been much discussion in privacy circles about a convergence of information-related functions into an information-governance department. While some organizations will have a regulatory or other need to maintain a separation between the CPO and CISO functions in particular, other privacy professionals may have an opportunity to redefine their roles over time to more broadly encompass information risk and policy.



"I think we'll see more companies converging privacy, information security, and records management under a common framework of policies and procedures," comments RBC's Jeff Green.

"As organizations seek to manage the risk associated with managing data," said IBM's Harriet Pearson, "the worlds of the traditional IT security professional and the privacy professional will converge even more than we have already seen."

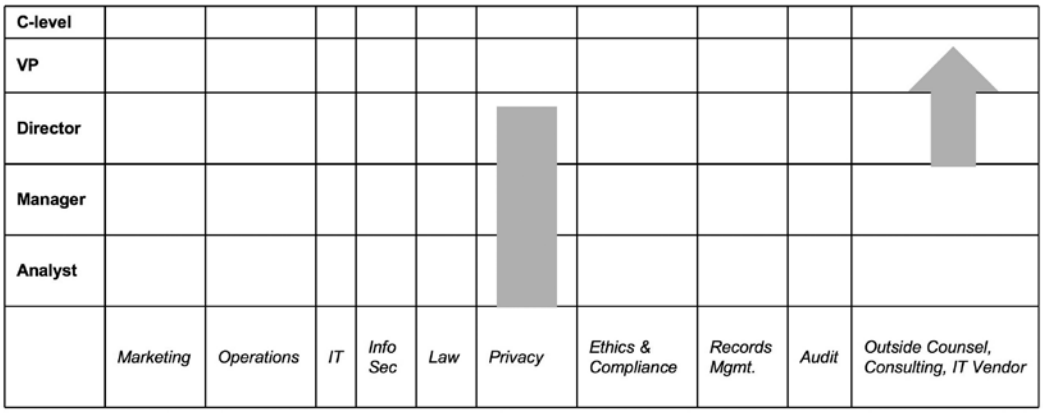
Walmart's Zoe Strickland offers a somewhat contrarian viewpoint in this regard: "I think we may actually see more divergence between the security and privacy functions. Many issues coming to the fore involve technology and uses of data that are separate from security. Security departments will likely stick to their core functions as those risks are not abating."

"The privacy professional needs a seat at the executive table," says Michelle Dennedy, "but security is going in the opposite direction, becoming more tactical."

"The unknown for me," says Brian O'Connor, "is whether surveillance technologies continue to develop and become so prevalent that companies will need to continue or expand the role of 'privacy advocate' separate from IT, Legal, and Compliance functions."

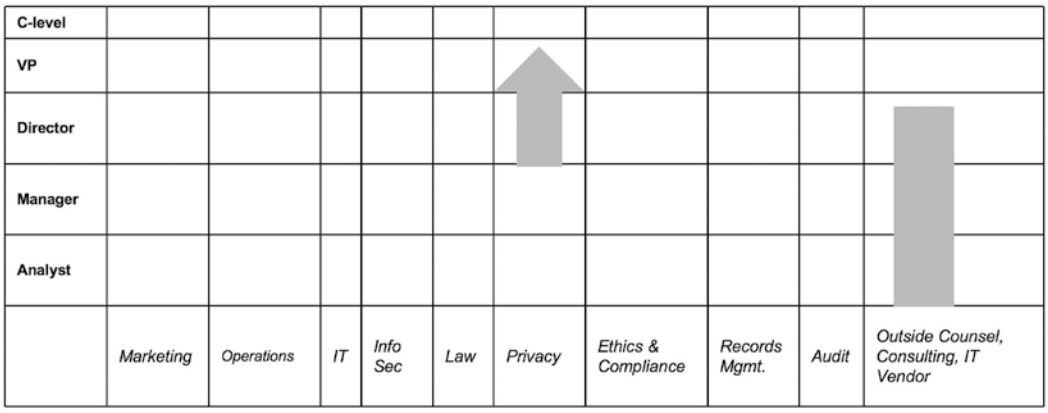
Path 5: Working inside out

Some privacy professionals may seek to parlay the practical and unparalleled experience of working as a corporate privacy leader into an external path serving multiple organizations in a consulting capacity. Typically, this kind of an opportunity would not emerge until the privacy professional has reached a senior or leadership level that provides a sufficient basis of experience for imparting advice in many different scenarios.



Path 6: Working outside in

Conversely, outside privacy practitioners may ultimately seek the relative predictability of a corporate executive job. With the diverse experience that an external position offers, the privacy consultant may be able to enter a corporate privacy path at a relatively high level.



The outside-in career path may become more prevalent if the CPO position becomes regulated or stipulated by more data protection laws. Bellamy notes that France, Germany, Netherlands, Sweden, Japan, and some U.S. agencies currently follow this approach. If more of these positions are created, new opportunities may open up for people inside and outside of the privacy profession who can garner the trust of regulators.

Adding the dimension of foreign assignments to any of these career paths—as is likely to be increasingly the case in the next decade—the career opportunities for driven privacy professionals will multiply.

About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest association of privacy professionals, representing more than 6,500 members from businesses, governments and academic institutions across 50 countries.

The IAPP was founded in 2000 with a mission to define, promote and improve the privacy profession globally. 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 many thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds the annual Privacy Summit, Privacy Academy and Practical Privacy Series conferences. These events 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, President of Minnesota Privacy Consultants, is a former chief privacy officer of Carlson Companies, IT management consultant at EDS, and international trade-law expert in the U.S. Government. Cline, a Certified Information Privacy Professional (CIPP), has held leadership positions in the International Association of Privacy Professionals, and is a privacy columnist for Computerworld and INSIDE 1to1: Privacy.

About the Artist

The image on the cover of this whitepaper was commissioned by the IAPP to celebrate the tenth anniversary of the organization. Artist David Plunkert worked in a collage-style with an image that evokes the modern privacy professional. From within an organization a privacy professional reaches outward to bring order to disparate worlds of data. The connection to a global economy, technology, the Internet and the central role of privacy are all themes presented in the piece.

Plunkert is an award winning illustrator and graphic designer based in Baltimore, MD. A prolific artist, his work has appeared on the pages of *Esquire, Forbes, GQ, The New Yorker, Time, Reader's Digest* and *Rolling Stone* magazines, as well as in the *New York Times* and the *Wall Street Journal*. Plunkert has also worked extensively with publishers and recording artists. Among his credits are the covers for Natan Sharansky's "Case for Democracy" and Richard Thompson's "You? me? us?"

International Association of Privacy Professionals

170 Cider Hill Road | York, Maine 03909 USA | +1 207.351.1500 | www.privacyassociation.org