# Why Study Privacy Law?

By Peter J. Guffin

As a professor teaching privacy law, I'm often asked by students why they should study this subject. And as a practitioner specializing in privacy law, I'm likewise frequently asked by lawyers, including my colleagues in my law firm, why they should devote time learning about privacy.

For the most part my answer is the same, although the specifics vary depending on the interests of the particular individual. The reasons I give for studying privacy law, formed by my own observations and experience in this field over the years, are multifaceted and generally fall into two broad categories: practical and altruistic. While each reason is worthy of consideration in its own right, when considered together these reasons make a compelling case for lawyers and law students to learn about this area of law.

In this essay I endeavor to explain some of the major reasons for learning about privacy law, starting with the most practical ones. First, there is a growing demand for legal services in the privacy field, both in government and the private sector, in the U.S. and abroad. According to the International Association of Privacy Professionals (IAPP), for those individuals entering the privacy profession, which is still relatively new, the most common background by far is law (35 percent). And those coming to privacy from the legal field tend to make the highest salaries – a median of $141,600.

Additionally, IAPP estimates that 75,000 Data Protection Officers (DPOs) will be needed globally due to the European Union's recently enacted General Data Protection Regulation (GDPR) which goes into effect in May 2018; many of them will be lawyers. IAPP now has over 35,000 members, up more than 10,000 from just over a year ago. About 40 percent of its members are lawyers.

Anecdotally, a number of privacy lawyers in the European Union have told me that they have had to turn away business and clients as a result of being too overstretched helping other clients with regulatory compliance under the GDPR. Put simply, there are good job opportunities for lawyers who have knowledge and skills in this area.

Even if one is not interested in specializing in privacy law, however, there is another practical reason for learning about this subject. Privacy law touches nearly all aspects of general law practice today. This should not come as a surprise to anyone, given the rapid pace of development in information technology and its deployment by governments and businesses across the globe, coupled with the explosion of new data protection laws and regulations that have been enacted over the last several decades in the United States and abroad. Personal data, stored as bits on servers, is the fuel that drives the economic engine. It is said that the only companies that have to worry about specific privacy and information security requirements are those companies that have customers and/or employees. Well, this means just about everyone, for just about all personal data!

The extent of privacy law's reach into general law practice today can be seen just by looking at the nature and breadth of the topics covered in my introductory information privacy law course, which include: Privacy Torts, Fair Information Practices Principles, Health Information, International Frameworks, Financial Information, FTC Enforcement, Law Enforcement (4th Amendment and Electronic Communications Privacy Act), Government Records (FOIA and Privacy Act of 1974), National Security, Big Data, Marketing and Behavioral Advertising, Social Networking, Children's Privacy, State Attorneys General Enforcement, Information Security, Data Breach Notification, Workplace Privacy, Lawyers and Cybersecurity – Legal Ethics and Beyond, Genetic Information, GDPR and EU-U.S. Privacy Shield framework, and Practical Obscurity and Court Records.

Whatever the nature of their practice, lawyers inevitably will en-

counter privacy law issues. This is true for lawyers in every type of practice, from rural lawyers who deal with a wide variety of issues involving individuals and small businesses, to city lawyers who represent mostly large businesses. Whether their practice involves business and commercial transactions, M&A, health care, financial services, employment and labor, immigration, insurance, civil litigation, criminal justice, education, government, intellectual property, technology, or family and domestic matters, to name just a few – privacy law issues abound in each of these areas and lawyers need to be able to recognize these issues and know when to seek additional expertise.

My own experience at my law firm bears this out. I'm regularly called upon by my colleagues in different practice areas across my firm to provide a diverse range of firm clients – representing just about all major sectors of the economy – with advice and assistance on different privacy law matters. It might be assisting an organization with navigating its regulatory compliance obligations under one of the many privacy law regimes or assisting a business with privacy and data security due diligence and risk analysis in an M&A transaction. Or assisting an organization with vendor due diligence in an IT outsourcing or technology procurement matter. Or advising a U.S.-based organization with respect to compliance with the GDPR and cross-border transfer issues, including self-certification under the EU-U.S. Privacy Shield framework. Or advising and assisting a client that has been the victim of a malicious hacking incident. The list of examples goes on and on.

The Rules of Professional Conduct are yet another practical reason to learn about privacy law. To fulfill our ethical and legal obligations to protect client confidential information from unauthorized disclosure, we as lawyers must now possess a certain level of competence in the areas of privacy and cyber security, regardless of the nature of our law practice. The need for lawyers to become more knowledgeable about these subjects is driven in large part by the law profession's increasing embrace of new and various technologies designed to improve productivity and efficiency in the delivery of legal services and the concomitant risks of the use of such technologies. It's also driven by the ever-increasing use of social media and reliance on digital records in all business and government sectors.

By way of illustration, on the subject of securing communication of protected client information, in its Formal Opinion 477 issued in May 2017, the ABA advises that "[a] lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct *where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access."* (Emphasis added.) As lawyers, we need to learn how to protect client information in this new technological world. Determining what constitutes "reasonable efforts" requires an analytical framework that includes factors such as the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, cost of employing additional safeguards, and difficultly of implementing the safeguards. Such frameworks are familiar territory for privacy lawyers and can be useful to help inform attorneys as to their ethical obligations.

Maine Ethics Opinion #207 issued in 2013 similarly addresses the obligations of Maine attorneys who wish to use cloud computing and storage on client matters, advising lawyers in some technical detail about the types of privacy and data security safeguards that they must put in place to ensure that the attorney's use of this technology does not result in the violation of any of the attorney's obligations under the various Maine Rules of Professional Conduct.

In sum, as far as practical reasons go for the study of privacy law, whatever the nature of your law practice, all lawyers inevitably will encounter privacy and data security issues. Having basic knowledge of these subjects is necessary to be able to provide competent advice to clients as well as to meet the lawyer's ethical and legal obligations. Moreover, regardless whether one wants to specialize in privacy law or not, demand for lawyers with information privacy and cyber security skills is strong and growing.

Next we turn to the altruistic reasons, including civic engagement and public service. These arguably are the most compelling reasons for learning about privacy law. Privacy is one of today's most pressing and important societal issues. Every day brings news about some advance in information technology or new threats to our individual and collective privacy interests resulting from the deployment of certain technologies, including social media. These advances include facial recognition software, artificial intelligence, self-driving cars, drones, and personal assistant robots. Some of these developments raise serious civil liberties issues, including concerns about government and private sector surveillance and interference with the election process at the state and national levels. Many raise far-reaching questions about the future of privacy, including difficult questions about how to protect the most vulnerable persons in our society from being victimized. The role of law is central to answering many of these questions.

For example, recent developments in technology have dramatically altered society's conception of citizens' privacy rights and expectations. We see this change being recognized in an increasing

number of recent federal court decisions involving the Fourth Amendment of the U.S. Constitution. Illustrative of this recognition is Justice Sotomayor's concurring opinion in *United States v. Jones*, in which she wrote:

> "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." (565 U.S. 400, 417 Sotomayor, J., concurring).

The cases remind us of the critical role the courts must play to "keep pace with the inexorable march of technological progress," creating rules that can evolve as technology develops. *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010) (holding that individuals have a "reasonable expectation of privacy" in their electronic communications). They also remind us of the important constitutional and public policy issues at stake. In *re United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) (requiring search warrant to obtain historical CSLI records, stating: "While the government's monitoring of our thoughts may be the archetypical Orwellian intrusion, the government's surveillance of our movements over a considerable time period through new technologies, such as the collection of cell-site-location records, without the protections of the Fourth Amendment, puts our country far closer to Oceania than our Constitution permits. It is time that the courts begin to address whether revolutionary changes in technology require changes to existing Fourth Amendment doctrine.")[1]

An example closer to home is the Maine Judicial Branch's planned move to the digital world and putting court records in electronic form, resulting in increased accessibility to the public. Personal information in those records, once protected by the practical difficulties of gaining access to the records, would thus become increasingly less obscure. The question presently facing the Maine court system is what policies and rules to put in place to try to strike the appropriate balance between the twin goals of open access to court records and protection of citizens' privacy rights.

There is a vast difference between digital records which are made available online 24/7 via the internet and paper-based records which are accessible only at the courthouse during regular business hours. In addition to unfettered accessibility, broad and widespread dissemination, and no user accountability, there is a complete loss of control with digital records, such that they effectively become permanently available – the internet never forgets.

The Maine state court system handles many different types of matters and special dockets, which often involve the collection by the courts of very intimate and sensitive personal information of individuals, some of whom are extremely vulnerable. Individuals generally are not in a position to refuse providing this information to the court, so choice is not always an option for individuals. In addition, many of the matters in the Maine state court system, such as divorce, parental rights, parentage, veteran, and domestic violence proceedings, are handled by the parties without representation of counsel.

If appropriate policies and rules are not put in place to protect such personal information by the Maine Judicial Branch, individuals may be at significant risk of potential physical, emotional and other harm, including blackmail, extortion, stalking, bullying, and sexual assault. In addition to privacy rights, other constitutionally protected citizens' rights may be implicated if the court grants online public access to such information without appropriate controls in place.

Unwarranted invasion of privacy should not be the price citizens have to pay to litigate private matters in court. As Justice Brennan once cautioned: "[B]road dissemination by state officials of [sensitive personal] information . . . would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests. *Whalen v. Roe*, 429 U.S. 589, 606 (1977) (Brennan J., concurring). As he also presciently observed: "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology." (Id. at 607)

Similarly, in a case quashing a government subpoena for redacted medical records relating to late-term abortions performed at a hospital, Judge Posner observed:

> "Some of these women will be afraid that when their redacted records are made a part of the trial record in New York, persons of their acquaintance, or skillful "Googlers," sifting the information contained in the medical records concerning each patient's medical and sex history, will put two and two together, "out" the 45 women, and thereby expose them to threats, humiliation, and obloquy. . . . "[W]hether the patients' identities would remain confidential by the exclusion of their names and identifying numbers is questionable at best. The patients' admit and discharge summaries arguably contain histories of the patients' prior and present medical conditions, information that in the cumulative can make the possibility of recognition very high." (*Northwestern Memorial Hosp. v. Ashcroft*, 362 F.3d 923, 929 (7th Cir. 2004)).

For those who are interested in learning about privacy law for altruistic reasons, there is much work to be done. Whether it be taking on individual *pro bono* matters or volunteering on advisory boards, commissions, or court committees, civic engagement and public service can take many forms. For my part, I have been fortunate to find opportunities to use my knowledge and experience in privacy law by taking on *pro bono* matters, such as advising a government intelligence agency with respect to its privacy practices, counseling an animal welfare organization and its veterinarian members with respect to privacy and data security issues under the state's prescription monitoring program, serving as a member of the Maine Judicial Branch Task Force on Transparency and Privacy of Court Records (TAP),[2] where I have been able to lend my voice to the debate regarding open access and privacy, and volunteering to teach and mentor students, lawyers and others who are interested in learning about privacy law or entering the field.

Public service, the highest calling of those in our profession, can be extremely fulfilling. In addition to the personal satisfaction that comes from being able to help others, lawyers who are involved in public service activities get to work on cutting edge issues. Of course, that is the very nature of public interest work. It is law-reforming, a challenge to the status quo. It also can be fun, intellectually stimulating and richly rewarding.

Finally, I'd like to leave you with this single cautionary note. Whatever your reasons or motivations, if you choose to study and learn about privacy law, be forewarned that the study of privacy can get a hold on you. Privacy issues stand out because of their immense complexity, philosophical, cultural and historical richness, and contemporary relevance. For nearly a decade, the topic of privacy has had a strong hold on me. However, talking from personal experience, it is worth every bit of the adventure.

**PETER GUFFIN** *is Visiting Professor of Practice at the University of Maine School of Law, co-Director of Maine Law's Information Privacy Program, and a partner at Pierce Atwood LLP.*

[1] Oceania is the setting for the novel "Nineteen Eighty-Four" published in 1949 by English author George Orwell. The adjective *Orwellian* is often used to describe a totalitarian dystopia that is characterized by government control and subjugation of the people.
[2] More information about TAP is available here: http://www.courts.maine.gov/maine_courts/committees/tap/index.html.