Privacy Law Fundamentals

Daniel J. Solove
John Marshall Harlan Research Professor of Law
George Washington University Law School
and
President and CEO
TeachPrivacy, LLC

&

Paul M. Schwartz
Jefferson E. Peyser Professor of Law
U.C. Berkeley School of Law
and
Director
Berkeley Center for Law & Technology
and
Special Advisor
Paul Hastings LLC

An IAPP Publication

Cover design by -ing designs, llc.
Book design by Tammy F. Sneddon Design.

ISBN 978-0-9983223-1-5

ABOUT *PRIVACY LAW FUNDAMENTALS*

"Concise, well-organized, and masterfully detailed, *Privacy Law Fundamentals* is the authoritative and most accessible reference for privacy practitioners looking for quick, accurately distilled, and current content from two of the most preeminent scholars in the field."

– James M. Aquilina, Stroz Friedberg

"Two giants of privacy scholarship succeed in distilling their legal expertise into an essential guide for a broad range of the legal community. Whether used to learn the basics or for quick reference, *Privacy Law Fundamentals* proves to be concise and authoritative."

– Jules Polonetsky, Future of Privacy Forum

"There are no better-qualified authors than Professor Schwartz and Solove to summarize the current state of privacy law and, as a result, there is no better compact privacy law resource than *Privacy Law Fundamentals*."

– Christopher Wolf, Hogan Lovells

"This book is my go-to reference for when I need quick, accurate information on privacy laws across sectors and jurisdictions. Solove and Schwartz masterfully make complex privacy law more accessible and understandable for anyone, from the most experienced practitioner to the first year law student."

– Nuala O'Connor, Center for Democracy and Technology

"Professors Solove and Schwartz pack an enormous amount of privacy knowledge into a slim volume in *Privacy Law Fundamentals*. In our fast-paced practice, there's nothing better than a compact and accessible work that is curated by two of the great thinkers of the field. It is a gem."

– Kurt Wimmer, Covington & Burling

"The go-to privacy law reference that you will keep going to. Professors Schwartz and Solove manage to distill without distorting and to outline without obscuring. Part reference, part primer and part pathfinder, *Privacy Law Fundamentals* is the ultimate privacy law resource."

– Tom Counts, Paul Hastings

"This is the essential primer for all privacy practitioners. Professors Solove and Schwartz have done a remarkable job of keeping this volume current in the fast-changing environment of new technology, case law and legislation."

– David A. Hoffman, Intel Corporation

ABOUT THE AUTHORS

Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also the President and CEO of TeachPrivacy, http://teachprivacy.com, a company that provides privacy and data security training to organizations in an array of industries. One of the world's leading experts in privacy law, Solove is the author of numerous books, including *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale 2011), *Understanding Privacy* (Harvard 2008), *The Future of Reputation: Gossip and Rumor in the Information Age* (Yale 2007; winner of the 2007 McGannon Award), and *The Digital Person: Technology and Privacy in the Information Age* (NYU 2004). Professor Solove is also the co-author (with Paul Schwartz) of a textbook, *Information Privacy Law*, with Aspen Publishing Co., now in its fifth edition. Additionally, he is the author of several other textbooks, including *Privacy and the Media* (2nd edition, Aspen Publishing Co. 2015), *Privacy, Law Enforcement, and National Security* (1st edition, Aspen Publishing Co. 2015), and *Consumer Privacy and Data Protection* (1st edition, Aspen Publishing Co. 2015), all with Paul Schwartz. He has published more than 50 articles and essays.

Solove has testified before the U.S. Congress and has been involved as an expert and consultant in a number of high-profile privacy cases. His work has been cited by many federal and state courts, including the U.S. Supreme Court. He has been interviewed and featured in several hundred media broadcasts and articles in publications and on networks including *The New York Times, The Wall Street Journal, The Washington Post, Chicago Tribune, USA Today, Time, Newsweek, People, Reader's Digest,* Associated Press, ABC, CBS, NBC, CNN, NPR and C-SPAN's "Book TV."

More information about Professor Solove's work can be found at www.daniel-solove.com. He can also be followed on Twitter at http://twitter.com/DanielSolove. He blogs at Privacy+Security Blog, www.teachprivacy.com/privacy-security-training-blog/. As one of a select group of LinkedIn "Influencers," Professor Solove also blogs at LinkedIn, www.linkedin.com/today/post/articles/2259773. His blog has more than 1 million followers.

Paul M. Schwartz is Jefferson E. Peyser Professor of Law at the University of California–Berkeley Law School and a director of the Berkeley Center for Law & Technology. A leading international expert on informational privacy and information law, he has published widely on these topics. In the U.S., his articles and essays have appeared in periodicals such as the *Harvard Law Review*, *Yale Law Journal*, *Stanford Law Review*, *California Law Review*, *N.Y.U. Law Review*, and *Chicago Law Review.* With Daniel Solove, he has published the leading casebook *Information Privacy Law* (Aspen, 5th ed., 2015) and other books.

Schwartz has testified as an expert before congressional committees in the United States and provided legal reports to the Commission of the European Community and Department of Justice, Canada. He has assisted numerous corporations in the United States and abroad with information privacy issues. A member of the American Law Institute, Schwartz has received scholarships and grants from the American Academy in Berlin, where he was a Berlin Prize Fellow; the Alexander von Humboldt Foundation; German Marshall Fund; Fulbright Foundation; the German Academic Exchange, and the Harry Frank Guggenheim Foundation. He is a member of the American Law Institute and the organizing committee of the Privacy Law Salon, and is Special Advisor to Paul Hastings LLP.

Schwartz belongs to the editorial boards of *International Data Privacy Law*, the *International Journal of Law and Information Technology*, and the *Zeitschrift für Datenschutz* (Data Protection Journal).

Schwartz received a JD degree from Yale Law School, where he was a senior editor on *The Yale Law Journal*, and a BA degree from Brown University. His homepage is www.paulschwartz.net. His Twitter account is @paulmschwartz.

DEDICATION

To Pamela and Griffin—DJS

To Steffie, Clara and Leo—PMS

PREFACE

This book provides a concise guide to privacy law. Privacy Law Fundamentals is designed to serve as a primer of the essential information that one needs to know about the field. For the student of privacy law or the beginning privacy professional, the book will provide an overview that can be digested readily. For the more seasoned and experienced, the book will serve as a handy reference guide, a way to refresh one's memory of key components of privacy laws and central cases. It will help close gaps in knowledge and inform on areas of the field about which one wants to know more.

In writing this book, we have aimed to avoid the "too much information" problem by singling out the essential provisions of law, regulations, and judicial decisions. A frequent risk in law books is that key definitions, provisions, and concepts will become lost in a litany of long and dense statutes and in a mass of cases. We have endeavored to distill the field down to its fundamentals and present this information in as clear and useful a manner as we could. Wherever possible, we have developed charts and lists to convey the material.

The book is organized in thirteen chapters:

- Chapter One—a review of the key privacy developments since the last edition.
- Chapter Two—an overview of privacy law in all its varied types and forms and a timeline with key points in the development of privacy law.
- Chapter Three—privacy law involving the media, including the privacy torts, defamation, and the First Amendment.
- Chapter Four—the law of domestic law enforcement, focusing on the Fourth Amendment and the statutes regulating electronic surveillance.
- Chapter Five—national security law, including the Foreign Intelligence Surveillance Act.

- Chapter Six—the laws and regulations that pertain to health and genetic data, including HIPAA.
- Chapter Seven—government records and laws, such as the Privacy Act and the Freedom of Information Act.
- Chapter Eight—the laws concerning financial information, including the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act.
- Chapter Nine—legal regulation of the privacy of consumer data and business records, involving statutes, tort protections, and FTC enforcement actions.
- Chapter Ten—data security law, including the varying laws in a majority of the states.
- Chapter Eleven—school privacy, including the Family Educational Rights and Privacy Act.
- Chapter Twelve—the regulation of employment privacy, including the different rules for government and private-sector employees.
- Chapter Thirteen—international privacy law, including the EU Data Protection Directive, the OECD Guidelines, the APEC Privacy Framework, and rules of international data transfers.

For his suggestions on our chapter about school privacy, we wish to thank Steven McDonald. This book also benefitted greatly from the research assistance of Henry Becker, Jordan Bock, Thad Houston, Richard Johnson, Lea Mekhneche, Robert Paris, and Michelle Parker.

For further references, including books, websites, statutes, and other sources of news and legal materials, visit our website (http://informationprivacylaw.com), and for our casebooks, click on the "resources" tab at the top.

We look forward to keeping this book up to date and to finding additional ways to make it as useful as possible. Please feel free to contact us with any suggestions and feedback about the book.

Daniel J. Solove
Washington, DC
dsolove@law.gwu.edu

Paul M. Schwartz
Berkeley, CA
pschwartz@law.berkeley.edu

TABLE OF CONTENTS

CHAPTER 1: NEW DEVELOPMENTS

CHAPTER 2: AN OVERVIEW OF PRIVACY LAW

CHAPTER 3: PRIVACY AND THE MEDIA

CHAPTER 7: GOVERNMENT RECORDS

CHAPTER 8: FINANCIAL DATA

CHAPTER 11: EDUCATION PRIVACY

CHAPTER 12: EMPLOYMENT PRIVACY

CHAPTER 13: INTERNATIONAL PRIVACY LAW

CHAPTER 1

New Developments

This chapter contains a detailed overview of leading developments in information privacy since the 2015 edition. Only the most important of these developments—those that served as turning points or milestones in the law—are also included in the relevant chapters of this book.

PRIVACY AND THE MEDIA

New Laws of Note

Revenge Porn Statutes
In the past few years, 34 states and the District of Columbia have passed revenge porn laws. In 2013, California led the way when it enacted legislation criminalizing the distribution of images of intimate body parts taken under circumstances where the parties agree or understand that the images would remain private. *See* Cal. Penal Code § 647(j)(4). In December 2014, Noe Iniguez became the first person convicted under the California statute for posting a topless photo of his former girlfriend on her employer's Facebook page. *See People v. Iniguez*, 202 Cal. Rptr. 3d 237 (App. Dep't Super. Ct. 2016) (complaint filed November 3, 2014). Iniguez was sentenced to one year in jail and three years' probation.

First Amendment Restrictions

***Elonis v. United States*, 135 S. Ct. 2001 (2015)**
The U.S. Supreme Court reversed a conviction under 18 U.S.C. § 875(c) that makes it a federal crime to transmit in interstate commerce "any communication containing any threat . . . to injure the person of another." The Court held that a conviction under the statue required a showing that the defendant had either the intent or knowledge that communications would be viewed as threats; negligence was not sufficient.

Music Group Macao Commercial Offshore Ltd. v. Does I-IX, No. 14-mc-80328 LB, **2015 WL 75073 (N.D. Cal. Jan. 6, 2015)**
Music Group sued anonymous Twitter users for tweeting that the company encouraged domestic violence and the CEO visited prostitutes. The court held that the plaintiffs could subpoena Twitter for the identities of the speakers without violating the First Amendment.

Notable Scholarship: Books

Samantha Barbas, *Laws of Image: Privacy and Publicity in America* (2015)
Historical account of how different areas of law—including the right of publicity, defamation, and libel—have regulated the use of one's image in public. Analysis of how "we seek publicity on our own terms" in the United States and the law's reaction to such behavior by individuals.

Lothar Determann, *California Privacy Law* (2d ed. 2017)
Comprehensive analysis of the strict standards of California privacy law.

Jim Dwyer, *More Awesome Than Money: Four Boys and Their Heroic Quest to Save Your Privacy from Facebook* (2014)
Recounting story of four undergraduates who tried, and failed, to build a social media site where people could control their personal data.

Amy Gajda, *The First Amendment Bubble: How Privacy and Paparazzi Threaten a Free Press* (2015)
Discussing how to balance privacy and freedom of the press, including how to define who counts as a "journalist" in the days of blogs and social media.

Jon L. Mills, *Privacy in the New Media Age* (2015)
Describing how to modernize the intrusion tort in a way that emphasizes both human dignity and freedom of the press. Tackles pressing question of how the new media age impacts our approach to privacy.

Jon Ronson, *So You've Been Publicly Shamed* (2015)
Case studies of individuals harmed by Twitter mobs, media attacks and cyber harassment. Ronson warns the public to consider the "level of mercilessness" with which it feels comfortable before joining in public shaming.

PRIVACY AND LAW ENFORCEMENT

Fourth Amendment

***United States v. DiTomasso*, 56 F. Supp. 3d 584 (S.D.N.Y. 2014)**
Holding users waived their Fourth Amendment rights due to AOL's terms of service, which stated that AOL monitors for criminal activity and reserves the right to reveal

criminal activity to law enforcement. In the court's view, "a reasonable person familiar with AOL's policy would understand that by agreeing to the policy, he was consenting not just to monitoring by AOL as an ISP, but also to monitoring by AOL as a government agent."

Drones

The growth in use of unmanned aerial vehicles has presented a series of privacy issues and public safety concerns.

Registration and Marking Requirements for Small Unmanned Aircraft, 80 Fed. Reg. 78,593 (FAA Dec. 16, 2015) (codified as amended in scattered sections of 14 C.F.R.)
Addresses the registration and marking requirements for small unmanned aircraft, including those operated as model aircraft.

Mail Covers

Office of Inspector Gen., U.S. Postal Serv., HR-AR-14-001, Postal Inspection Service Mail Covers Program (2014)
Recommending better procedures for mail covers program to ensure that the Postal Inspection Service can lead effective investigations and assuage public concerns over privacy of the mail.

Electronic Communications

***In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016)**
Denying the Government's request for an order requiring Apple, Inc. to bypass the passcode security on an Apple iPhone in order to extract data relevant to an ongoing drug investigation. The court rejected the Government's argument that the All Writs Act provides a court with the authority to grant any relief not outright prohibited by law.

In re the Search of an Apple iPhone, No. ED 15–0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016)
After initially requesting that Apple, Inc. assist the Government in unlocking the iPhone used by San Bernardino shooter Syed Farook, the Justice Department announced that it had employed a third party to break into the phone. As a result, the Government requested that the order compelling Apple to assist the government be vacated, resolving a brewing battle between Apple and the Obama administration.

Twitter, *Transparency Report – United States* (2015)
Discusses increased demands on Twitter by governments, including an 18% increase in the number of accounts impacted by government information requests.

Google, *Transparency Report* (2015)
Contains data and qualitative explanation of government removal requests. In 2015 Google received 3,467 government requests to remove information from Google products, a slight decrease from the peak of 3,846 requests in 2013.

***Microsoft Corp. v. United States*, No. 14-2985, 2016 WL 3770056 (2d Cir. July 14, 2016)**
Finding a lack of extra-territorial reach to a warrant issued pursuant to the Stored Communications Act. The Second Circuit ruled: "Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas."

State Electronic Surveillance Law: Recording Police Encounters

Nat'l Inst. Of Justice, Office of Justice Programs, U.S. Dep't of Justice, *A Primer on Body-Worn Cameras for Law Enforcement*, (Sept. 2012)
The National Institute of Justice (NIJ) Sensor, Surveillance, and Biometric Technologies (SSBT) Center of Excellence (CoE) discusses issues that law enforcement organizations should consider both before and during the implementation of body-worn cameras in law enforcement.

Notable Scholarship: Books

After Snowden: Privacy, Secrecy, and Security in the Information Age (Ronald Goldfarb ed., 2015)
Collection of essays by Thomas Blanton, David Cole, John Mills, Hodding Carter, Barry Siegel, and Edward Wasserman. Topics include the Snowden leaks, the state secrets doctrine, journalists and whistleblowers, classification of government documents, and more.

Bernard E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (2015)
Documenting how "[d]igital surveillance capabilities have reached new heights in ordinary digital existence and have begun to converge on carceral monitoring." Calling for "digital disobedience" to "challenge our virtual transparency."

Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (2015)
Examining NSA surveillance, the Snowden revelations, and other recent issues in privacy and data collection. Developing a core set of principles and solutions for government, corporations, and "the rest of us."

Notable Scholarship: Articles and Other Sources

William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821 (2016)
Advocating for a positive law approach to the Fourth Amendment. Fourth Amendment protections should be based on "background positive law," and the key question in search-and-seizure analysis should be "whether government officials have done something forbidden to private parties."

Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015)
Discusses how the "subjective expectation of privacy" portion of the *Katz* test is a superfluous doctrine and should be excised by the Supreme Court.

Martina Kitzmueller, *Are You Recording This?: Enforcement of Police Videotaping*, 47 Conn. L. Rev. 167 (2014)
Discussing different methods states use for law enforcement to make and preserve videos of their interactions.

Gregory S. McNeal, *Drones and the Future of Aerial Surveillance*, 84 Geo. Wash. L. Rev. 354 (2016)
Arguing that unmanned aerial surveillance could be more protective of privacy than manned surveillance. Proposes looking beyond a warrant-based approach for protecting privacy from aerial surveillance.

Brandon Nagy, *Why They Can Watch You: Assessing the Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement*, 29 Berkeley Tech. L.J. 135 (2014)
Reviewing current regulatory framework surrounding unmanned aircraft systems and discussing potential constitutional challenges to unmanned aerial surveillance.

NATIONAL SECURITY AND FOREIGN INTELLIGENCE

Foreign Intelligence Gathering

USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in scattered sections of 50 U.S.C.)
Bans the bulk collection of Americans' Internet metadata and telephonic records under Section 215 of the Patriot Act. The government must now identify a person, account, address, or personal device when requesting records, limiting the scope of tangible things sought "to the greatest extent reasonably possible." However, the bill permits authorities to collect phone records two degrees (or "hops") of separation from targeted individuals.

Leading Cases on Foreign Intelligence Gathering

***ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015)**
Holding collection of telephone metadata exceeded authority granted by FISA, as the metadata was not relevant to authorized counterterrorism investigations. The Second Circuit found the Section 215's statutory text did not authorize the telephone metadata program. The opinion did not address the constitutionality of the metadata collection. A follow-up opinion after the enactment of the Freedom Act permitted a 180-day transition period to Congress to wind down the program.

National Security Letters (NSLs)

FBI, *Termination Procedures for National Security Letter Nondisclosure Requirement* (2015)
The FBI revised the NSL disclosure policy, permitting letter recipients to disclose the receipt of the letter at "the earlier of 3 years after the opening of a fully predicated investigation or the investigation's close." Previously, the FBI was permitted to enforce NSL gag orders indefinitely. Gag orders may be enforced beyond the 3-year period if the FBI determines that a statutory exception applies.

Notable Reports

Privacy & Civil Liberties Oversight Board. (PCLOB), *Recommendations Assessment Report* (Feb. 5, 2016)
Report noting full or partial implementation of all 22 recommendations made by PCLOB regarding Section 215 and Section 702 surveillance programs. These recommendations included ending the NSA's bulk collection of metadata, greater transparency by the government and private companies supplying data, expansion of appellate review of FISC decisions, and revised targeting and minimization procedures. PCLOB contends the measures would strengthen civil liberties without hindering counterterrorism efforts.

Nat'l Sec. Agency, *NSA Reports to the President's Intelligence Oversight Board* (2001 – 2013)
Following a FOIA lawsuit filed by the ALCU, the NSA released a series of redacted reports prepared for the Intelligence Oversight Board. The released documents do not make clear the exact number of violations that had occurred during this time period. A declassified Inspector General report noted 12 cases of "intentional misuse" of the organization's monitoring capabilities, including several instances of operators targeting their own significant others.

Notable Scholarship: Books

Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (2016)
Examines the expansion of U.S. intelligence gathering and offers solutions for scaling back intrusive national security measures.

Notable Scholarship: Articles and Other Sources

Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 Stan. L. Rev 285 (2015)
Examines tensions between the Fourth Amendment and global data transfers, offering proposals on adapting the Amendment to the digital age.

Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J.L. & Pub. Pol'y 757 (2014)
Contends that the NSA's bulk telephonic metadata collection runs counter to Congress's original intent in enacting FISA in 1978.

Robert M. Chesney, *Computer Network Operations and U.S. Domestic Law: An Overview*, 89 Int'l L. Stud. 218 (2013)
Examines the use of computer network operations for intelligence gathering purposes with a particular emphasis on Congressional and Executive oversight.

HEALTH PRIVACY

Health Insurance Portability and Accountability Act (HIPAA)

Office for Civil Rights, U.S. Dep't of Health & Human Servs., *HIPAA Privacy in Emergency Situations* (Nov. 2014)
Guidance document from OCR in response to the Ebola crisis. The OCR provides guidance about HIPPA's rules for sharing personal health information in emergency situations.

Office for Civil Rights, U.S. Dep't of Health & Human Servs., *OCR Launches Phase 2 of HIPAA Audit Program* (2015)
HHS Office for Civil Rights began its next phase of audits. After emailing covered entities and business associates to request contact information for the audit, OCR will send a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees. This information will, in turn, be used to create potential audit subject groups.

Notable Cases

***Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433 (2014)**
Holding that HIPAA "does not preempt the plaintiff's state common-law causes of action for negligence or negligent infliction of emotional distress." Even though HIPAA lacks a private right of action, plaintiffs can use HIPAA to inform the standard of care in a negligence case (and other state common law causes of action).

***Walgreen Co. v. Hinchy*, 21 N.E. 3d 99 (Ind. Ct. App. 2014), *aff'd on reh'g*, 25 N.E.3d 748 (Ind. Ct. App. 2015)**
Reviewing a $1.44 million jury verdict, an Indiana appellate court affirmed that the plaintiff had raised a viable claim of negligence based on using HIPAA as the standard of care. Court affirmed original result on rehearing.

***United States v. Michel*, No. 2:07-cr-00889-JFB, 2013 WL 9903336 (E.D.N.Y. Apr. 10, 2013)**
After a three-week jury trial, Helene Michel was convicted of identity theft, Medicare fraud, and wrongful disclosure of private medical information under HIPAA. Michel used her position as owner of a medical equipment company to enter health facilities and steal patient records, which she then used to submit false Medicare billings. Michel was sentenced to twelve years in prison and ordered to forfeit $1.3 million that was seized by the government when she was indicted.

***United States v. Hippler*, No. 6:14-cr-00018-MHS-JDL (E.D. Tex. Feb. 18, 2015)**
Hippler, a former hospital employee, was sentenced to 18 months in prison for HIPAA violations after he pleaded guilty to wrongful disclosure of individually identifiable health information. Hippler had been charged with wrongful disclosure of individual identifiable health information with the intent to sell, transfer, and use the information for personal gain.

New HHS OCR HIPAA Enforcement Cases

***Advocate Entities* (July 8, 2016)**
Three breaches affected the PHI of 4 million individuals. Violations: failed to assess risks to PHI, failed to implement procedures to limit access to files in data support center, failed to ensure that business associate would protect PHI, and failed to secure unencrypted laptop left in unlocked vehicle overnight. $5.55 million penalty.

***Univ. of Miss. Med. Ctr.* (Jul. 7, 2016)**
Breach of PHI affected 10,000 individuals. Violations: failed to implement procedures to correct security lapses, failed to implement physical safeguards for workstations with access to PHI, failed to use a unique user name and/or number to track PHI, and failed to notify individuals whose PHI was likely disclosed. $2.75 million penalty.

***Or. Health & Sci. Univ.* (Jul. 18, 2016)**
Multiple breaches involving unencrypted laptops and a stolen unencrypted thumb drive exposed the PHI of thousands, including 1,361 patients with a significant risk of harm. Violations: did not implement measures to address security risks, did not implement policies to correct security violations, and did not encrypt PHI on workstations. $2.7 million penalty.

***Catholic Health Care Servs. of the Archdiocese of Phila.* (Jun. 24, 2016)**
Theft of mobile device exposed PHI of 412 nursing home residents. Violations: failed to encrypt or physically protect mobile device, failed to implement policies governing mobile devices, and failed to conduct risk analysis. $650,000 penalty.

***N.Y. & Presbyterian Hosp.* (Apr. 19, 2016)**
Hospital released PHI of two patients to film crews and staff during filming of "NY Med" TV series. Violations: allowed individuals receiving urgent medical care to be filmed without their authorization and failed to safeguard PHI during filming. $2.2 million penalty.

***Raleigh Orthopaedic Clinic* (Apr. 14, 2016)**
Clinic gave PHI of 17,300 patients to potential business partner without first implementing a business associate agreement. Violations: disclosed PHI to unauthorized entity and failed to implement business associate agreement. $750,000 penalty.

***The Feinstein Inst. for Med. Research* (Mar. 16, 2016)**
Unencrypted laptop containing PHI of 13,000 patients and research participants stolen from an employee's car. Violations: failed to implement sufficient security procedures, including policies governing devices. $3.9 million penalty.

***N. Mem'l Health Care* (Mar. 16, 2016)**
Unencrypted laptop stolen from locked vehicle belonging to North Memorial's business associate, exposing the PHI of 9,497 individuals. Violations: failed to implement business associate agreement and failed to complete a risk analysis. $1.55 million penalty.

***Complete P.T., Pool & Land Physical Therapy, Inc.* (Feb. 02, 2016)**
Company impermissibly disclosed PHI when it posted patient testimonials to its website without proper authorization. Violations: failed to safeguard PHI, impermissibly disclosed PHI, and failed to implement procedures to comply with HIPAA authorization requirements. $25,000 penalty.

***Lincare, Inc.* (Mar. 1, 2016)**
Employee of in-home medical care provider abandoned documents containing the PHI of 278 individuals after moving residences. Violations: failed to implement procedures to safeguard PHI offsite, despite providing in-home care, and allowed employees to store PHI in personal vehicles for extended periods of time. $239,800 penalty.

***Bd. of Regents of the Univ. of Wash.* (Dec. 14, 2015)**
Employee downloaded an email attachment with malware, infecting the organization's IT system and compromising the data of over 90,000 patients. Violations: failed to implement policies to address security violations and failed to ensure that affiliated entities conducted and responded to risk assessments. $750,000 penalty.

***Triple-S Mgmt. Corp.* (Nov. 30, 2015)**
Series of breaches affected the unsecured PHI of thousands of individuals. Violations: failed to implement administrative, physical, and technical safeguards to protect PHI, impermissibly disclosed PHI to outside vendor without appropriate business associate agreement, failed to conduct and respond to risk assessments, and failed to implement proper security measures. $3.5 million penalty.

***Lahey Clinical Hosp., Inc.* (Nov. 19, 2015)**
Workstation laptop stolen from an unlocked hospital treatment room, exposing the PHI of 599 individuals. Violations: failed to conduct risk analysis, failed to physically safeguard workstations, failed to implement policies regarding PHI maintained on workstations, and failed to use unique user names to track user identity. $850,000 penalty.

***Cancer Care Grp., P.C.* (Aug. 31, 2015)**
Computer and unencrypted backup media stolen from an employee's car, exposing the PHI of 55,000 patients. Violations: widespread non-compliance with the HIPAA Security Rule, including failure to implement policy governing removal of hardware and electronic media and failure to conduct risk analysis. $750,000 penalty.

***St. Elizabeth's Med. Ctr.* (July 8, 2015)**
Employees used an Internet-based document sharing application to store the PHI of at least 498 individuals without assessing the risks associated with the application. Separately, breach of unsecured PHI on former employee's personal laptop and USB flash drive compromised PHI of 595 individuals. Violations: failed to assess risks associated with document practices and failed to identify and respond to known security incident. $218, 400 penalty.

***Cornell Prescription Pharmacy* (Apr. 22, 2015)**
Pharmacy disposed of documents containing PHI of 1,610 patents in an unlocked, open container. Violations: No written policies or procedures and no employee training. $125,000 penalty.

***Anchorage Cmty. Mental Health Servs.* (Dec. 2, 2014)**
Malware infected health facility's technology infrastructure, compromising PHI of 2,743 patients. Violations: did not follow HHS Security Rule policies and procedures and did not address basic technological risks. $150,000 penalty.

New State HIPAA Enforcement Cases

***Women & Infants Hosp. of R.I.* (Mass. July 22, 2014)**
Lawsuit brought under HIPAA and state consumer protection and data security statutes after hospital lost 19 unencrypted backup tapes containing the PHI of 12,127 Massachusetts residents. Violations: failed to implement inventory and tracking system and failed to adequately protect PHI. $110,000 penalty.

***Beth Israel Deaconess Med. Ctr.* (Mass. Nov. 20, 2014)**
Lawsuit brought under HIPAA and state consumer protection and data security statutes after doctor's unencrypted personal laptop was stolen from an unlocked office, exposing the PHI of 4,000 individuals. Violations: failed to encrypt and physically secure laptop. $100,000 penalty.

***Bos. Children's Hosp.* (Mass. Dec. 19, 2014)**
Lawsuit brought under HIPAA and state consumer protection and data security statutes after doctor's unencrypted hospital-issued laptop was stolen at a conference. Breach exposed PHI of 2,159 patients, including 1,700 minors. Violations: failed to encrypt and physically secure laptop. $40,000 penalty.

State Laws

New Jersey, 2014 N.J. Sess. Law Serv. Ch. 88 (West) (effective Aug. 1, 2015)
Provides that health insurance carriers must encrypt patient data; password-protection access is no longer sufficient. Contrast this N.J. law with HIPAA, where encryption is not required. The N.J. statute applies just to health insurance carriers, not to providers. Moreover, a violation of the encryption mandate constitutes a violation of New Jersey's Consumer Fraud Act.

Constitutional Right to Privacy

***Stuart v. Camnitz*, 774 F.3d 238 (4th Cir. 2014)**
On First Amendment grounds, a federal appeals court struck down North Carolina's Woman's Right to Know Act, which compelled doctors to display a sonogram and describe the image of the fetus to a patient before performing an abortion. Statute found to be compelled speech and the restriction to be ideologically motivated.

GOVERNMENT RECORDS

FOIA Amendment

FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 (codified at 5 U.S.C. § 552)
The bill, enacted on June 30, 2016, makes key reforms to 1966 FOIA.

Among its key changes:

- Codifies a "foreseeable harm standard" into FOIA; an agency must release information unless it "reasonably foresees that disclosure would harm an interest protected by an exemption" or "disclosure is prohibited by law";
- Requires launch of a "consolidated online request portal" to allow members of the public to use a single website to file FOIA requests;
- Codifies the DOJ guidance that agencies are to make records and documents available to requesters in an electronic format and to post online records that are requested three or more times;
- Creates a Chief FOIA Officers council of Federal Chief Officers; this council to develop recommendations for increasing compliance and efficiency in responding to FOIA requests;
- Excludes the "deliberative process privilege" from records created 25 years or more before the data on which the records were requested; and
- Requires the Office of Government Information Services to offer mediation services to resolve disputes between requesters and agencies "as a non-exclusive alternative to litigation."

Automatic License Plate Readers

***Gannett Co. v Cty. of Monroe*, 4 N.Y.S.3d 847 (Sup. Ct. 2015)**
Holding that New York's FOIA, the Freedom of Information Law, generally permits individuals to find out whether their license plate data has been collected through law enforcement use of License Plate Readers and stored in state databases. Law enforcement agencies also can seek to refuse release on grounds that it would interference with "a current specific ongoing law enforcement investigation."

Government Privacy and Security Management

Office of Mgmt. & Budget, *Circular No. A-130* (2016)
In its Circular A-130, the OMB sets policy and provides guidance on information technology management for federal executive agencies. Before the Obama Administration issued this update in July 2016, Circular A-130 had last been revised in 2000. This update focused on such areas as cyber-security, information governance, privacy, security, and open data. Perhaps most crucially, Circular A-130 calls for strong data governance by the Federal Government to proactively identify risks to privacy and security and to identify and test practical solutions to risk.

Notable Books

James B. Jacobs, *The Eternal Criminal Record* (2015)
Examines problems with current criminal recordkeeping.

Notable Scholarship: Articles and Other Sources

Erin Murphy, *The Mismatch Between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System*, 87 S. Cal. L. Rev. 633 (2014)
Argues that the adversarial process is ill suited to twenty-first-century evidence—such as location tracking, biometrics, digital forensics, and other database-driven techniques.

FINANCIAL DATA

Notable FCRA Cases

***Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)**
Not all FCRA violations qualify for standing, despite congressional intent for the statute to create a private cause of action. To demonstrate the necessary "injury in fact" from the dissemination of false information, plaintiffs must also show a "concrete harm." The concrete harm need not be "tangible," and a sufficient risk of real harm may qualify, but a "bare procedural violation" is insufficient.

***Sweet v. LinkedIn Corp.*, No. 5:14-cv-04531-PSG, 2015 WL 1744254 (N.D. Cal. Apr. 14, 2015)**
LinkedIn's "References Searches" feature, which allowed employers to find people with whom a prospective employee may have worked, did not qualify as a FCRA "consumer report." The report's contents were entirely derived from self-provided information, which is exempted under the statute. Moreover, the district court found that LinkedIn did not qualify under FCRA as a "consumer reporting agency"; the contested feature was only furthering the user's "information-sharing objectives."

CFPB Rulemaking

CFPB, *Rule for Publishing Financial Rules Online* (Oct. 20, 2014)
Financial institutions subject to the GLBA may publish privacy policies online rather than through an annual hard copy. Consumers may be informed about these online privacy policies in a "regular consumer communication," such as a monthly statement.

Notable CFPB Cases

***In re Dwolla, Inc.*, CFPB No. 2016-CFPB-0007 (Mar. 2, 2016)**
This consent order stemmed from the first CFPB action related to data security. An online payment platform, Dwolla, allows its members to transfer funds to other members. The company advertised that its data-security practices "exceed[ed]" or "surpass[ed] industry security standards." It also claimed that members' "information is securely encrypted and stored." Among other things, the CFPB found that Dwolla did not reasonably protect consumer data, did not encrypt all sensitive information, and did not exceed industry standards. The CFPB alleged that the company engaged in "deceptive acts or practices." Dwolla agreed to a $100,000 civil penalty, to comply with all statutory requirements in the future, and to implement numerous improvements in its data-security practices.

CONSUMER DATA

New Cases: Standing

***Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016)**
Not all FCRA violations qualify for standing, despite congressional intent for the statute to create a private cause of action. To demonstrate the necessary "injury in fact" from the dissemination of false information, plaintiffs must also show a "concrete harm." The concrete harm need not be "tangible," and a sufficient risk of real harm may qualify, but a "bare procedural violation" is insufficient.

***Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012)**
Plaintiffs sufficiently pleaded an injury-in-fact by alleging a sufficient nexus between data breach and theft of their identify. Allegation was that the same sensitive information stored on stolen laptops was used by thieves to open bank accounts in plaintiffs' names.

***Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190 (N.D. Cal. 2014)**
Class action suit alleging LinkedIn accessed user email accounts and sent correspondence without permission. The court found that the social networking site's users had consented to this usage but had not agreed to follow-up emails LinkedIn sent. The parties entered a settlement wherein LinkedIn agreed to pay $13 million in damages and $3.25 million in legal fees.

Notable FTC Cases

***FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)**
Affirmed the FTC's authority to bring actions against companies with inadequate data protection practices. The FTC had pursued a suit against Wyndham, a chain of hospitality suites, alleging a string of data breaches at the company resulted from insufficient security measures. The Third Circuit held that a company's failure to

maintain reasonable and appropriate data security could constitute "unfair practices" under Section 5 of the FTC Act. Additionally, the court concluded that prior FTC guidelines and actions provided fair notice that Wyndham's conduct fell within the agency's statutory authority.

Notable FTC Enforcement Actions

***In re ASUSTeK Comput., Inc.*, FTC No. C-4587 (July 18, 2016)**
ASUSTeK, a Taiwan-based computer hardware maker, sold routers and cloud services, advertising that these products included multiple security features that would protect customers' computers from viruses and other types of unauthorized access. In fact, ASUSTeK's product possessed security weaknesses that exposed and compromised thousands of consumers' personal information. The FTC's order requires the company to establish and maintain a security program that will be subject to independent audits for the next 20 years.

***FTC v. Sitesearch Corp.*, No. CV-14-02750-PHX-NVW (D. Ariz. Dec. 11, 2015)**
The FTC brought an action against data brokers that gathered loan applications that consumers had submitted through payday loan sites. These companies allegedly provided third party scammers with consumers' sensitive personal information, allowing scammers to withdraw money from the consumers' accounts. A settlement now prohibits these companies from providing further sensitive information to third parties and also requires the destruction of previously collected data. The order also includes a $5.7 million suspended judgment against defendants and a $4.1 million default judgment against Sitesearch.

***In re Craig Brittain*, FTC No. C-4564 (Dec. 28, 2015)**
Craig Brittain allegedly operated a "revenge porn" website and deceptively acquired and posted nude images of women. Subsequently, he demanded that the victims pay fees to have the content removed. After the FTC pursued an action against him, Brittain entered into a settlement prohibiting him from publicly sharing any nude content without the express consent of the subjects. The settlement also required the deletion of all previously published content on Brittain's website.

***In re PaymentsMD, LLC*, FTC No. C-4505 (Jan. 27, 2015)**
PaymentsMD provided a billing platform for medical care providers, allowing patients to pay bills online. The FTC alleged that PaymentsMD deceptively collected consumer health information by contacting various health insurance companies, pharmacies, medical offices, and labs without informing consumers. As a result of an FTC order, PaymentsMD must destroy all this collected information; the order also prohibits the company from engaging in similarly deceptive collection and use of consumers' personal information.

***In re RadioShack, Corp.*, 550 B.R. 700 (Bankr. D. Del. 2016)**
RadioShack intended to sell their customer database during bankruptcy proceedings. Referring to *In re Toysmart*, the FTC urged the bankruptcy court to protect consumer data through limiting the sale and use of data to ensure RadioShack's privacy promises were honored. RadioShack subsequently entered into an agreement with state attorney generals that limited the company purchaser's access to RadioShack's customer database. The bankruptcy court ultimately approved the sale.

***In re Nomi Techs., Inc.*, FTC No. C-4538 (Aug. 28, 2015)**
Nomi Technologies allegedly misled consumers through statements published on the company website falsely indicating that consumers could opt-out of in-store mobile device tracking. The FTC order prohibits Nomi from misleading consumers regarding how their data is collected, processed, used, and shared on any type of electronic device. Furthermore, Nomi may not misrepresent the extent to which consumers will receive notification about the company's privacy practices. Strong dissents in this matter from Commissioners Maureen Ollhausen and Joshua Wright.

***FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-00967-JLR (W.D. Wash. Dec. 19, 2014)**
Suit alleging T-Mobile improperly billed customers for unwanted third-party services like horoscopes and celebrity gossip. T-Mobile alleged to have essentially hid these charges from consumers by placing them in extensive phone bills. T-Mobile and the FTC entered a $90 million settlement agreement, including fines in all states and refunds for affected customers.

***In re Snapchat, Inc.*, FTC No. C-4501 (Dec. 23, 2014)**
Mobile app Snapchat allows users to share photos and videos that will automatically be deleted after several seconds. In 2014, Snapchat suffered data breaches involving usernames and passwords. The FTC brought a suit against the company, alleging Snapchat users were deceived by a privacy policy that promised less protection than actually provided. In their settlement with the FTC, Snapchat agreed to strengthen privacy and security measures, to provide users with an accurate description of these measures, and to be monitored by an independent privacy professional for 20 years.

***In re GMR Transcription Servs.*, FTC No. C-4482 (Aug. 14, 2014)**
Settlement involved allegations that a medical transcription company outsourced services to a third party without adequately checking that it could implement reasonable security measures.

***In re Accretive Health, Inc.*, FTC No. C-4432 (Feb. 5, 2014)**
A company providing medical billing and revenue management services to hospitals put consumers' personal information at risk by, among other things, transporting laptops with sensitive data in a way that made them vulnerable to theft. The FTC also said the company gave access to personal information to employees who didn't need it to do their jobs.

Children's Online Privacy Protection Act (COPPA)

FTC COPPA Cases

Video Privacy Protection Act (VPPA)

Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (codified as amended at 18 U.S.C. § 2710)
Permitting a videotape service provider to obtain the consumer's informed, written consent through the Internet. Such consent is valid for a period of up to two years or until consent is withdrawn.

VPPA: Leading Cases

***Austin-Spearman v. AMC Network Entm't, LLC*, 98 F. Supp. 3d 662 (S.D.N.Y. 2015)**
AMC Networks allegedly violated the VPPA by sharing user's video-streaming history collected from their website with a social network. The court ruled that these claims were sufficient to constitute an injury-in-fact, required for Article III standing. However, the plaintiff failed to establish that she was a registered user or had any other relationship with the website; the court consequently held she was not a "consumer" protected by the VPPA.

***Eichenberger v. ESPN, Inc*, No. C14–463 TSZ, 2015 WL 7252985 (W.D. Wash. May 7, 2015)**
Class action suit against ESPN alleging that the network's Roku streaming app improperly shared consumer's PII, such as streaming behavior, with third parties. The information given to third parties combined unique Roku serial number with information previously collected about that consumer. The unique serial number of a Roku device was held not to constitute PII under the VPPA.

***Locklear v. Dow Jones & Co.*, 101 F. Supp. 3d 1312 (N.D. Ga. 2015), *abrogated by Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015)**
Another court reached a similar conclusion to the *Eichenberger* decision, holding that a device's unique serial number was not PII under the VPPA.

***Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015)**
The Cartoon Network offered free mobile app services that allowed consumers to stream freely available content. A consumer alleged that the company violated the VPPA by disclosing mobile device identification numbers and records about the viewed content with data-analytics companies. The court held that an individual who uses a free mobile app to view freely available content does not qualify as a "subscriber" and consequently is not a "consumer" under the VPPA.

***Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482 (1st Cir. 2016)**
Newspaper publisher Gannett Satellite offered a mobile app and allegedly disclosed personal information to third-party data-analytics companies, including the unique identifier number of consumers' mobile devices, GPS locations, and content viewed through the app. While the Eleventh Circuit agreed with the district court that this type of information qualifies as PII under the VPPA, it reversed the lower court's dismissal on the grounds that the complaint adequately alleged that the plaintiff was a "consumer" for purposes of the VPPA.

Telephone Consumer Protection Act (TCPA)

***Palm Beach Golf Center-Boca, Inc. v. John G. Sarris, D.D.S., P.A.*, 781 F.3d 1245 (11th Cir. 2015)**
Eleventh Circuit ruled transmission of junk faxes conferred Article III standing, even if the faxes in question were unseen by recipients. The court contended that rendering a plaintiff's fax machine unavailable for a period of time constituted an injury-in-fact.

FCC Enforcement

The FCC has increased its enforcement of privacy matters and has handed out large fines. Collaborating with other agencies, the FCC has collected more than $365 million through its settlements, including punitive fines and refunds to consumers.

FCC, *Privacy Guidelines for ISPs* (2016)
Privacy guidelines issued for ISPs, providing three separate categories for using and sharing information. The guidelines also provide ISP customers with increased transparency and power regarding their personal information.

***In re Cellco P'ship*, FCC No. EB-TCD-14-00017601 (Mar. 7, 2016)**
Verizon Wireless had previously added unique identifier headers, or "supercookies," into customer's mobile Internet traffic without notification or consent. According to an FCC suit, these supercookies were employed from 2012 to 2014. A settlement between the parties included a $1.35 million fine and required the adoption a three-year compliance plan. Verizon agreed to notify consumers about tracking and targeting practices, and the company now needs consumer consent in order to share supercookie information with third parties.

***In re AT&T Servs., Inc.*, FCC No. EB-TCD-14-00016243 (Apr. 8, 2015)**
AT&T's overseas workers stole personal information from 280,000 customers. In a settlement with the FCC, AT&T agreed to pay a $25 million fine for violating their statutory duty under the Communications Act to reasonably secure and protect their customer data. The FCC noted this failure also constituted "an unjust and unreasonable practice in violation of the Communications Act."

***In re TerraCom, Inc.*, FCC No. EB-TCD-13-00009175 (July 9, 2015)**
TerraCom and YourTel exposed consumers' sensitive information to unauthorized individuals when its data storage vendors utilized servers without any encryption or password protection. As a result, the FCC issued an order to the companies that set out a $3.5 million penalty. The companies were also required to implement a comprehensive information security program, a data breach response plan, enhanced employee training, and regular privacy risk assessments. The FCC's order mandated that the two parties designate a certified privacy professional at a senior corporate manager level and to provide compliance reports with the FCC.

***In re Cox Commc'ns, Inc.*, FCC No. EB-IHD-14-00017829 (Nov. 5, 2015)**
FCC data security enforcement action against a cable provider following a data breach and subsequent allegations of unreasonable data security practices. The FCC also alleged that Cox failed to notify law enforcement authorities of the security breaches in a timely fashion. Cox entered into a consent decree that included a $595,000 civil penalty and required enhanced security practices including oversight of vendors, privacy risk assessments, a written compliance program, training of employees, and notification issued to affected consumers.

Electronic Communications Privacy Act (ECPA)

***Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836 (N.D. Cal. 2014)**
A suit alleging Facebook violated ECPA by scanning users' private messages for targeted advertising purposes. The court held that consumers of Facebook's website neither expressly nor implicitly consented to the alleged interception of their private messages. Facebook's disclosure that it may use information about users for data analysis was not specific enough to constitute valid consent, nor did it provide adequate notice regarding the private communications text-scanning.

***Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033 (N.D. Cal. 2014)**
Consumers brought a class action alleging that Apple knowingly and intentionally violated ECPA when intercepting and storing text messages sent by current owners of Apple devices to former users, rendering the delivery impossible. The district court held that the plaintiffs' claims failed to allege that Apple accessed messages while in storage and thus did not constitute a proper claim under ECPA. However, Apple's conduct violated the Wiretap Act. Court also noted that the software license agreement failed to adequately notify consumers that Apple's message interception would make the delivery impossible.

***In re Carrier IQ, Inc.*, No. 12-md-02330-EMC, 2016 WL 4474366 (N.D. Cal. Aug. 25, 2016)**
Judge granted preliminary approval to a $9 million class action settlement following a federal court's rejection in *In re Carrier IQ, Inc.*, 78 F. Supp.3d 1051 (N.D. Cal. 2015), of smart phone manufacturers' claims that the plaintiffs lacked standing under the Wiretap Act. Plaintiffs had alleged that their phones' performance had been degrad-

ed by the error-logging software that collected information about the substance of phone usage, including websites visited and text message contents. The court held plaintiffs had also sufficiently alleged a Wiretap Act claim.

Notable New Books

Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (2015)
Comparing U.S. privacy and data security laws and enforcement strategies with those of Europe, finding certain trends towards convergence as well as a distinctive U.S. model of compliance.

Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (2016)
Comprehensive examination of the FTC and its modern role as an inventive regulator in the U.S. privacy marketplace. Valuable analysis of the FTC's history—in the area of privacy and beyond—to explain its current role and predict where it will go in the future.

Notable New Articles

Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 Geo. Wash. L. Rev. 2230 (2015)
Arguing that the FTC's statutory authority permits the agency to reach a broader scope of privacy and data security issues than it currently pursues.

DATA SECURITY

Notable Cases: FTC

***FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)**
Affirming FTC's authority to bring cases against companies with inadequate data protection practices. A company's failure to maintain reasonable and appropriate data security could constitute unfair competition under the FTC's Section 5 authority. FTC Act and prior FTC guidelines and actions were sufficient notice that Wyndham's conduct fell within statutory authority.

Notable FTC Enforcement Actions

***In re ASUSTeK Comput. Inc.*, FTC No. C-4587 (July 18, 2016)**
Pioneering Internet of Things enforcement action by the FTC. Company alleged to misrepresent its router security features. Among other things, the complaint alleged that ASUSTeK encouraged customers to set up accounts on its private cloud network with weak security presets and authentication bypass vulnerabilities. Company also allegedly failed to provide consumers timely notification of vulnerabilities after receiving customer complaints.

***In re Snapchat, Inc.*, FTC No. C-4501 (Dec. 23, 2014)**
Alleging misrepresentations regarding irretrievability of messages sent via mobile app. Complaint alleges that Snapchat privacy promises were deceptive because of behavior of third-party developers using Snapchat's own API. Snapchat also made deceptive promises regarding analytics tracking.

***In re Oracle Corp.*, FTC No. C-4571 (Mar. 28, 2015)**
Complaint alleged that Oracle knew of security vulnerabilities in older Java versions, but in update removed only the most recent version of the software. Oracle agreed to refrain from misrepresenting the security of its software. Oracle further agreed to notify consumers of risks associated with older Java versions present on computers and to provide notice of the settlement on its website.

Notable CFPB Enforcement Actions

***In re Dwolla, Inc.*, CFPB No. 2016-CFPB-0007 (Mar. 2, 2016)**
CFPB's first data security action. Misrepresentation alleged regarding security of online payment system. Dwolla claimed that customer transactions would be "safe" and "secure" in compliance with standards set by the trade group Payment Card Industry Security Standards Counsel, but its practices fell below those standards. Inadequate or unreasonable practices alleged related to adopting and implementing data-security policies, assessing foreseeable security risks, ensuring employee security training, using encryption technology, and practicing secure software development. Pursuant to deceptive acts and practices authority, the CFPB ordered Dwolla to refrain from misrepresenting the security of its online payment system; enact data security measures and policies to correct the above deficiencies; and pay $100,000 civil money penalty.

Notable FCC Enforcement

***In re AT&T Servs., Inc.*, FCC No. EB-TCD-14-00016243 (Apr. 8, 2015)**
In its largest data security action, the FTC entered a $25 million settlement with AT&T to resolve investigation into data breaches at AT&T's call centers in Mexico, Colombia, and the Philippines. These breaches resulted from employees' unauthorized use of customers' information, jeopardizing the confidentiality of almost 280,000 customers' personal information. In addition to the financial penalty, FCC ordered AT&T to appoint a compliance officer; develop and implement a compliance plan that included risk assessment, review, and training; and provide notice to affected customers.

***In re Cox Commc'ns, Inc.*, FCC No. EB-IHD-14-00017829 (Nov. 5, 2015)**
Cox entered into a consent decree following a 2014 data breach and subsequent FCC allegations of unreasonable data security practices. Unlike enforcement practices typically mandated by the FTC, the FCC consent order required specific security practices rather than general "reasonable" security maintenance. $595,000 civil penalty assessed. FCC's first data security action against a cable provider and first action regarding a hacking incident.

***In re TerraCom, Inc.*, FCC No. EB-TCD-13-00009175 (July 9, 2015)**
TerraCom and Yourtel entered into a consent decree following FCC allegations that they failed to protect the sensitive information of customers applying for their Lifeline phone services. Specifically, they allegedly stored customer data on online servers without password protection or encryption, leading to a data breach. The companies jointly agreed to pay a $3.5 million civil penalty; appoint a compliance officer and develop a compliance plan; implement an information security program; and other measures.

Notable Treatises

***Cybersecurity: A Practical Guide to the Law of Cyber Risk* (Edward R. McNicholas & Vivek K. Mohan eds., 2016)**
Succinct yet thorough treatise on cybersecurity law.

EDUCATION PRIVACY

New Federal Laws

Every Student Succeeds Act (ESSA), Pub. L. No. 114-95, 129 Stat. 1802 (codified as amended in scattered sections of 20 U.S.C.) (2015)

Primary Function: Governs law for K-12 public education policy and replaces No Child Left Behind Act. The law requires grantees to possess knowledge of FERPA's responsibilities.

Homeless Students: ESSA mandates that homeless students' living situations not be listed in directories; instead, this information is considered a part of the student's educational record and thus protected by FERPA.

Congressional Findings: Congress included a section on the importance of protecting student privacy, calling for recipients of funding to ensure PII is held in strict confidence.

New Fourth Amendment Cases

***G.C. v. Owensboro Public Schs.*, 711 F.3d 623 (6th Cir. 2013)**
School officials lacked reasonable grounds to search a student's cell phone. The student had a history of depression and marijuana-usage, and he violated school policy regarding cell phone usage in the classroom. These combined factors were deemed insufficient to justify a cell phone search by school officials.

Notable Scholarship: Articles and Other Sources

Katherine P. McGrath, Note, *Developing a First Amendment Framework for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Protection Act*, 49 U.C. Davis L. Rev. 1149 (2016)
Note examining California's SOPIPA in light of the Supreme Court's *Sorrell v. IMS Health, Inc.* decision about the freedom of commercial speech, hypothesizing that SOPIPA would not survive a First Amendment challenge. The article suggests a number of changes to help SOPIPA better conform to the Supreme Court's views on commercial speech.

Jules Polonetsky & Omer Tene, *The Ethics of Student Privacy: Building Trust for Ed Tech*, 21 Int'l R. Info. Ethics 25 (2014)
Analyzing challenges in the Ed Tech industry, noting the widespread skepticism that apps like InBloom have faced. The authors propose a "solution toolkit" involving transparency and parental access to data. The article also contends that lengthy privacy notices for products may be off-putting and counter-productive for users.

Jules Polonetsky & Omer Tene, *Who is Reading Whom Now: Privacy in Education From Books to MOOCs*, 17 Vand. J. Ent. & Tech. L. 927 (2015)
Focusing on the broad landscape of Ed Tech and arguing for an analytic separation of the privacy issues and education standardization debate surrounding Ed Tech.

EMPLOYMENT PRIVACY

New NLRB Cases

***Landry's Inc.*, 362 N.L.R.B. No. 69 (2015)**
NLRB held that a policy was lawful, where it urged employees not to post anything that could result in morale problems, but did not explicitly prohibit employees from posting information related to the job or co-workers.

***Boch Imports, Inc.*, 362 N.L.R.B. No. 83 (2015), *aff'd, Boch Imports, Inc. v. NLRB*, 826 F.3d 558 (1st Cir. 2016)**
NLRB found a social media policy violative of Section 8 of the NLRA, which required employees to self-identify when posting comments about the employer, the employer's business, or policy issues.

***Chipotle Services LLC*, NLRB No. 04-CA-147314 (2016)**
In this NLRB action, an administrative law judge concluded that some aspects but not all of Chipotle's social media policy violated Section 8 of the NLRA. A provision prohibiting the disclosure of "confidential information" was violative because the policy did not define "confidential"—a term the NLRB found "vague and subject to interpretation." A provision prohibiting "disparaging" statements was violative because it was overbroad. But the ALJ upheld a provision against "harassing or discriminatory" statements.

Americans with Disabilities Act (ADA)

EEOC, *Living with HIV Infection: Your Legal Rights in the Workplace Under the ADA* (2015)
The EEOC issued this guidance document to address the protections required under the ADA for applicants and employees with HIV infection. Generally, persons with HIV infection are allowed to keep their condition private. If persons disclose their condition, employers have an obligation to keep the medical information confidential, "even from co-workers."

New Employer Access to Employee Social Media Account Laws

Connecticut, An Act Concerning Employee Online Privacy (S.B. 426) (2015)
Prohibits employers from requesting or requiring employees or applicants to provide access to personal online accounts or to invite the employer to join an online network.

Delaware, Employee/Applicant Protection for Social Media Act (H.B. 109) (2015)
Restricts employers from requiring or requesting access to an employee's or applicant's personal social media profile or account.

Maine (H.B. 640) (2015)
Prohibits employers from requiring or coercing employees or applicants to provide passwords to access personal online accounts, provide account information, or add the employer to an account.

Montana (H.B. 343) (2015)
Prohibits employers from requesting employees or applicants to provide passwords or user names to social media accounts.

Nebraska, Workplace Privacy Act (L.B. 821) (2016)
Prohibits employers from accessing personal Internet accounts of applicants or employees. Prohibits employers from taking adverse action against an employee or failing to hire an applicant for not providing personal Internet account information.

Oregon (S.B. 185) (2015)
Prohibits employers from requiring employees or applicants "to establish or maintain a personal social media account," or to allow the employer to use the account for advertising.

Tennessee, Employee Online Privacy Act (S.B. 1808) (2015)
Prohibits employers from requiring employees or applicants to disclose passwords to social media accounts. The Act also prohibits forcing employees or applicants to add the employer as a contact or access the social media account in the employer's presence.

Virginia (H.B. 2081) (2015)
Prohibits employers from "requiring, requesting, or causing" employees or applicants to provide usernames and passwords to social media accounts. The Act also bars employers from requiring employees to change privacy settings or add any other person to the social media account's contacts.

West Virginia, Internet Privacy Protection Act (H.B. 4364) (2016)
Prohibits employers from requiring employees or applicants to disclose user names, passwords, or any other means of access to personal online accounts.

INTERNATIONAL PRIVACY LAW

ECHR Cases

***Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* 931/13 Eur. Ct. H.R. (2015)**
Publisher Satakunnan Markkinapörssi Oy printed Finnish individuals' publicly-available tax-related data. The publisher collaborated with service provider Satamedia Oy to send out tax information via text message upon an individual's request. Extensive publication of personal, publicly-available tax information constituted a violation of Article 8, especially in light of Article 10's protection of a free press. The ECJ also found that these text messages had low public interest value.

European Court of Justice (ECJ)

Case C-362/14, *Maximillian Schrems v. Data Prot. Comm'r* 2015 E.C.R. (Sept. 23, 2015)
In this landmark case, the ECJ ruled, first, that national authorities must be able to independently investigate the Safe Harbor agreement and to decide on the adequacy of mechanisms in place before transfers of personal information to third countries. Second, the Court considered the adequacy of the Safe Harbor agreement itself. It held that it did not provide an adequate level of protection because EU citizens' data were exposed to the mass surveillance programs of U.S. intelligence agencies without limitations and redress.

Case C-230/14, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Judgment (Oct. 1, 2015)
This case involved Weltimmo, a Slovakian company that ran a Hungarian-language real estate website. The ECJ examined which national data protection law applied to a business operating in more than one EU state. According to the EU Directive, a key factor in determining the applicability of a member state's laws to an entity is whether the company operates a "relevant establishment" in said state. The ECJ held that Weltimmo had an establishment in Hungary for these reasons: (1) website language;

(2) location of advertised property; (3) existence of a representative in Hungary in charge of collecting debts and judicial and administrative proceedings on behalf of Weltimmo; and (4) existence of a business address and bank account in Hungary.

The General Data Protection Regulation (GDPR)

European Commission, Regulation 2016/670 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (May 4, 2016)

After years of discussion and negotiations, the EU adopted the General Data Protection Regulation (GDPR) in April 2016. This new regime will replace the EU Data Protection Directive 95/46 and take effect in May 2018. Unlike the Directive, which required the enactment of harmonizing legislation in Member States, the GDPR will be directly applicable in all Member States. It takes effect in May 2018.

The GDPR includes high penalties for violations, a new and narrower definition of "consent," a requirement for most businesses with more than 250 employees to have a privacy officer, data breach notification requirements, and a "right to erasure." The proposed regulation also contains protections against decisions based exclusively on "automated processing" and safeguards for sensitive data.

Directly Binding in Member States: Unlike the Directive, the GDPR does not require implementation in national law; it will be directly applicable to all member states of the EU. As the Recitals state: "Consistent and homogenous application of the rules for the protection of personal data should be ensured throughout the Union."

National Law-Making and Areas of Exclusion. Although generally directly binding, the GDPR does allow for certain kinds of national law-making. These include national laws that further specify obligations in areas covered under the GDPR, such as "the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in a controller." There are also exceptions and national law-making power for freedom of expression and information, national identification numbers, and employee data. Moreover, the GDPR permits "a margin of manoeuvre" for Member States to specify certain kinds of rules, such as those for sensitive data and regarding the conditions under which data processing will be lawful. Finally, the Regulation does not apply to "activities which fall outside the scope of Union law, such as activities concerning national security." It also does not apply to activities by a natural person "in the course of a purely personal or household activity."

Invalidation of the U.S.-EU Safe Harbor Arrangement

Invalidity of Safe Harbor: The Shrems *decision*

In 2015, in its *Shrems* decision, the ECJ invalided the 15-year-old, widely-used EU-U.S. Safe Harbor Framework, which provided a mechanism for data transfers between the EU and U.S. Austrian privacy-rights activist Max Schrems sued Facebook Ireland, arguing that his data protection rights were violated when Facebook transferred his personal information to U.S. servers and thus exposing it to the NSA's mass surveillance program. The ECJ held that U.S. surveillance policies did not meet EU privacy rights standards. As a result, the EU invalidated the Safe Harbor for failing to guarantee an adequate level of protection for the personal data of EU citizens.

The EU-U.S. Privacy Shield

The U.S. government and European Commission were already negotiating a new framework for data transfers at the time of ECJ's *Schrems* decision, which invalidated the Safe Harbor agreement. On July 12, 2016 the Commission issued its implementing decision, which found the Privacy Shield to ensure an adequate level of protection for personal data transferred from the EU to self-certified organizations in the U.S. pursuant to it.

Principles of the Privacy Shield

The Privacy Shield seeks to impose strong obligations on U.S. companies to protect the personal data of EU citizens, and to establish robust monitoring and enforcement by the Department of Commerce and the FTC. Furthermore, it provides for stronger individual rights for EU citizens including:

1. ***Notice***
   Participating companies must provide individuals with a variety of different information including: (1) type of data collected, (2) purpose of collection, (3) circumstances of onward transfer, (4) third-party identities, (5) rights of the individuals, (6) redress channels for the individuals.
2. ***Choice***
   The Privacy Shield gives individuals a right to opt out of their information being disclosed to a third party, or used for a purpose that is materially different than the purpose for which it was originally collected or subsequently authorized by the individual. Opt-out mechanisms must be "clear, conspicuous, and readily available."
3. ***Accountability for Onward Transfer***
   Organizations are liable for compliance with the Notice and Choice Principles when transferring information to a third party acting as a controller. To do so, organization must enter into a contract with the third party controller.

4. *Security*
   Companies must take reasonable and appropriate measures to protect personal information, taking into account the risks involved in the processing and the nature of the personal information.
5. *Data Integrity and Purpose Limitation*
   Companies possess a duty to ensure that personal data held and processed by the organization is "reliable for its intended use, accurate, complete, and current."
6. *Access*
   Individuals are to have access to personal information about them and be able to correct, amend, or delete that information when it is inaccurate, or has been processed in violation of the Principles. Companies are to reply to individual complaints within 45 days.
7. *Recourse, Enforcement, and Liability*
   The Privacy Shield provides the right to file privacy complaints directly with participating companies. The agreement requires independent recourse mechanisms that must be free of charge to individuals.

Other Aspects of the Privacy Shield

Transparency and Safeguards. The U.S. issued written confirmation to the EU Commission that access of public authorities for law enforcement and national security purposes to EU citizens' information will be subject to "clear limitations, safeguards, and oversight." There will be an annual joint review of the Privacy Shield, including the issue of national security access, which will be conducted by the European Commission and U.S. Department of Commerce. The U.S. has also created a new Ombudsperson, separate from U.S. intelligence services, who will handle individual complaints from EU citizens.

Compliance Review by Companies. Participation in the Privacy Shield framework requires an annual compliance review by companies. Companies exiting the Privacy Shield agreement must still comply with its requirements with respect to the data obtained and processed under the Privacy Shield.

Enforcement. The Privacy Shield heightens enforcement mechanisms beyond those of the Safe Harbor agreement. The Department of Commerce and the FTC are given an oversight role under it. Individuals may also bring complaints under it to a national Data Protection Authority.

U.S.-Swiss Safe Harbor Framework (2009)

The U.S.-Swiss Safe Harbor continues to exist after the invalidation of the U.S.-EU Swiss Harbor. The U.S. Department of Commerce continues to maintain its online U.S.-Swiss Safe Harbor List. The Swiss Data Protection Commission has criticized reliance, however, on the U.S.-Swiss Safe Harbor and called for use of contractual safeguards for Swiss-U.S. data transfers. The Swiss Data Protection Commission also advocated adoption of a regulation analogous to the EU-U.S. Privacy Shield between the U.S. and Switzerland.

New Developments: Canada

Digital Privacy Act, S.C. 2015, c. 32 (Can.)
Amending PIPEDA to established breach notification requirements and heightened requirements for valid consent. The amendments also increase penalties for violations of PIPEDA.

New Developments: Japan

In September 2015, an extensive amendment to the Act on Personal Information was enacted. The amendment to APPI will enter into force on a date set by cabinet order and occurs before September 2017. This Amendment places new restrictions on data transfers to foreign countries. It permits transfers to third parties in foreign countries only when there is prior consent; a transfer to a country with protections equivalent to that of Japan; or the transfer is to a third party with an internal protection system that meets standards set by the Japanese Personal Information Protection Commission. The amended APPI contains additional details regarding the law's definition of personal information. Finally, it contains a new definition of sensitive personal information, which will require prior consent before organizations can collect it.

New Developments: Russia

Localization Law, Federal Law No. 242-FZ
A new law requires that the personal data of Russian citizens be stored within Russia. The deadline for compliance was September 1, 2015.

FTC Enforcement of the APEC Cross-Border Privacy Rules System

***In re Very Incognito Techs., Inc.*, FTC No. 162 3034 (May 4, 2016)**
On May 4, 2016, the FTC approved its first APEC order, settling a case with Very Incognito Technologies, Inc. ("Vipvape"), a vaporizers manufacturer. Vipvape falsely alleged on its website that it was a certified company under APEC's Cross Border Privacy Rules framework. The settlement prohibits Vipvape from misrepresenting its participation, membership, or certification in any government or self-regulatory privacy or security program.

Notable Scholarship: Treatises and Books

Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (2014)
Magisterial treatise on the development of and current status of information privacy law in all Asian states

Andrew B. Serwin, *Information Security and Privacy: A Guide to International Law and Compliance* (2016)
Up-to-date treatise examining EU privacy law and that of individual countries worldwide.

Articles and Other Sources

Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU*, 49 U.C Davis L. Rev. 1017 (2016)
Discussion of significant role of Google in developing the "right to be forgotten" (RTBF) in the EU. Google plays this role by deciding individual RTBF requests made to it.