Summer 2020

Teaching Information Privacy Law

Joseph A. Tomain
Indiana University Maurer School of Law, jtomain@indiana.edu

Teaching Information Privacy Law

Joseph A. Tomain[†]

Teaching information privacy law is exciting and challenging because of the fast pace of technological and legal development and because "information privacy law" sprawls across a vast array of disparate areas of substantive law that do not automatically connect. This Essay provides one approach to teaching this fascinating, doctrinally diverse, and rapidly moving area of law. Through the framework of ten key course themes, this pedagogical approach seeks to help students find a common thread that connects these various areas of law into a cohesive whole. This framework provides a way to think about not only privacy law, but also law generally.

I. INTRODUCTION

Unlike traditional courses, such as contracts and criminal law, "information privacy law" is not a course that is limited to a single doctrinal silo.[1] The casebook I use covers a wide variety of disparate areas of law from contracts to constitutional law to consumer law and beyond.[2] I use this casebook in two three-credit courses: "Information Privacy Law I" and "Information Privacy Law II."[3] In addition to its vast scope, information privacy law is one of the quickest developing areas of law because of the relentless pace of technological advancement and the new ways in which

[†]Joseph A. Tomain is a Lecturer in Law and Director of the Cybersecurity and Information Privacy Law Program at the Maurer School of Law, Indiana University. He is also a Senior Fellow at Indiana University's Center for Applied Cybersecurity Research. Thank you to the *Washburn Law Journal* for the invitation to present at its Symposium on "The Future of Cyber Speech, Media, and Privacy." Thank you to Susannah Mroz, Joseph P. Tomain, and the fellow symposium participants and attendees for their helpful comments and questions.

1. The nomenclature describing this area of law varies. "Data privacy" is another commonly used term. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 775 (2019).

2. DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW (6th ed. 2018). There are, of course, other casebook choices, such as WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW (2016).

3. Information Privacy Law I is course number B708 and Information Privacy Law II is course number B728 at Maurer School of Law, Indiana University. Maurer School of Law offers other privacy and data law courses, as well. *E.g.*, Health Privacy Law (B536); *and* Seminar in Intellectual Property: Data Law and Policy (L730). Course descriptions are available at https://www.law.indiana.edu/academics/courses/ [https://perma.cc/PZA7-XD7B].

technology is used—ways that disrupt existing notions of privacy and have a substantial impact on society.[4] For one example among many, consider China's development of a "social credit score" system that covers "all aspects of life, judging citizens' behavior and trustworthiness."[5] Also, consider that a similar social credit system in the United States may not be far off.[6]

In light of the diverse doctrinal areas of law that constitute information privacy law and the rapid pace of technological development that, at the very least, requires reconsideration of the adequacy of existing law, there ought to be a way to bring some coherence to this sprawling and fast-moving field of study.[7] To that end, I have identified ten key course themes that provide a framework for students to study information privacy both within a single semester and as a way to connect Information Privacy Law I and II.[8]

These ten themes provide the course framework precisely because people have been thinking and writing about them in the context of information privacy law for some time and continue to do so. For example,

4. Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, SSRN 1, 11 (Jan. 24, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3457563 [https://perma.cc/J546-BUVC] ("privacy law is a constantly evolving area of law").

5. Nicole Kobie, *The complicated truth about China's social credit system*, WIRED (June 7, 2019), https://www.wired.co.uk/article/china-social-credit-system-explained [https://perma.cc/7J6V-37WX].

6. Mike Eglan, *Uh-oh: Silicon Valley is building a Chinese-style social credit system*, FASTCOMPANY (Aug. 26, 2019), https://www.fastcompany.com/90394048/uh-oh-silicon-valley-is-building-a-chinese-style-social-credit-system [https://perma.cc/UM3C-YV4Q] ("[S]uch systems, it turns out, are not unique to China. A parallel system is developing in the United States, in part as the result of Silicon Valley and technology-industry user policies, and in part by surveillance of social media activity by private companies.").

7. Another rapidly developing area of law that incorporates privacy law is "Internet Law" or "Cyberlaw." Part of my inspiration for this Essay is Eric Goldman, *Teaching Cyberlaw*, 52 ST. LOUIS U. L.J. 749 (2008). There is a debate about whether "Cyberlaw" or "Internet Law" is the proper term for such courses because terms like "cyberspace" and "cyberlaw" might obscure legal analysis. *See* JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS, 1, 53–54 (9th ed. 2019) ("This spatial vision of 'cyberspace' cast a long shadow on legal thought, especially when it came to jurisdiction."). There is also a debate regarding whether "Internet Law" or "Cyberlaw" should even be its own field of study. *Compare* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996), *with* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999). Perhaps that same debate could be applied to "information privacy law." *See, e.g.*, Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 310 (1975) ("The question arises, then, whether or not there are *any* rights in the right to privacy cluster which aren't also in some other right cluster. I suspect there aren't any, and that the right to privacy is everywhere overlapped by other rights."). While this "reductionist" debate is beyond the scope of this Essay, it is covered in the Solove & Schwartz casebook and is part of class discussion when I teach Information Privacy Law I. SOLOVE & SCHWARTZ, *supra* note 2, at 55.

8. I am not the first person to suggest that teaching privacy law requires reconsideration of the proper pedagogical approach for this field of study. *See generally* Constance Anastopoulo & Thomas P. Gressette, Jr., *Teaching Privacy in the Age of Octomom: Enhancing Case/Socratic Method with Structured Class Discussion*, 44 VAL. U.L. REV. 391 (2010).

one of the key course themes is the concept of privacy in public spaces.[9] Others have written extensively about this topic.[10] I believe my pedagogical contribution is organizing the study of information privacy law through the framework of these ten themes. Through this framework, students are encouraged to think "horizontally" across the various doctrinal silos covered in information privacy law.[11] By thinking "horizontally," students have a way to find intersections between the various doctrinal fields of law covered in information privacy law and a way to think about law more generally. Anecdotal evidence from former students lends some support to my view that these ten course themes serve that intended purpose.[12] Part II provides a summary of my pedagogical approach and course structure. Part III briefly describes the ten key course themes and provides some vignettes to illustrate a few of them.

II. PEDAGOGICAL APPROACH AND COURSE STRUCTURE

Before addressing the ten key course themes, a brief description of the course structure will provide greater context to this Essay and my pedagogical approach. Information Privacy Law I covers the first four chapters of Solove and Schwartz's casebook. Collectively, these chapters: (1) provide an introduction to this field of study and a brief exploration of "Perspectives on Privacy," (2) examine First Amendment issues and related torts involving "Privacy and the Media," and (3) address Fourth Amendment, Fifth Amendment, and related criminal statutes involving

9. The normative value of a public-private dichotomy as a way to conceptualize privacy and privacy law is subject to debate. *E.g.*, Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 17–24 (2013).

10. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); PRIVACY IN PUBLIC: CONCEPTUAL AND REGULATORY CHALLENGES (Tjerk Timan, Bryce Clayton Newell & Bert-Jaap Koops eds., 2017).

11. *See* Goldman, *supra* note 7, at 752 ("[A] survey of disparate legal doctrines can encourage students to think about client problems 'horizontally' rather than in doctrinal silos. Horizontal cross-doctrinal issue-spotting is an essential skill for lawyers, but law school courses often do not practice that skill.").

12. Three former students provided unsolicited feedback regarding the value of the key course themes in their study of information privacy law. One student wrote in a course evaluation: "I found the notes and questions and current event presentation[s] very helpful both as a reflect[ion] of the key course theme[s] and also a good practice for public speaking." Fall 2019 Course Evaluation, Information Privacy Law I, Maurer School of Law, Indiana University (on file with author). Another student wrote in a course evaluation: "[a]s we covered each case policy, or current event, he made sure to take a minute or two to tie it back to a central course theme." Fall 2019 Course Evaluation, Information Privacy Law I, Maurer School of Law, Indiana University (on file with author). Finally, yet another student wrote in an email: "I cannot read an article about privacy now without thinking about how it applies to key course themes." Email from a former student to author (Jan. 10, 2020) (on file with author).

"Privacy and Law Enforcement."[13] These four chapters offer readers a taste of privacy theory and an introduction to some constitutional and related, subordinate legal considerations involving privacy.[14] While the Solove and Schwartz casebook is an excellent introduction to information privacy law, the casebook, through no fault of the authors, could have been updated the month it was published because of the speedy pace of technological and legal change in privacy law. Thus, each semester, I update the syllabus with recent developments that connect to the casebook's coverage.[15] In the Fall 2019 semester of Information Privacy Law I, my assigned readings included thirty-nine supplemental materials from 2018-2019 alone.[16] These supplements to the casebook included twenty-two news articles and blog

13. Information Privacy Law II covers an even broader array of substantive law: government records, consumer privacy, employment privacy, education privacy, financial privacy, and international privacy.

14. Some understanding of constitutional law may be necessary for a valuable discussion of privacy law. *See* Anastopoulo & Gressette, *supra* note 8, at 401 ("Understanding privacy as a legal concept is not a simple undertaking. Some scholars have proposed teaching the law of personal liberties as a separate Advanced Constitutional Law class, premised on the idea that a student must first have some understanding of constitutional law before undertaking study of privacy.").

15. *Id.* at 394, 409 ("Teaching privacy law exclusively from casebooks is simply insufficient to teach law students how to thoroughly analyze issues at the intersection of privacy and technology. . . . The texts must be supplemented in order to address the impact of technology on privacy.").

16. I include other supplemental materials that pre-date 2018, but do not include a discussion of them here.

posts;[17] twelve cases and briefs;[18] two law review articles;[19] and the written remarks of Alvaro Bedoya from the 2019 U.S. Senator Dennis Chavez

17. Roger McNamee, *A Brief History of How Your Privacy Was Stolen*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/06/03/opinion/google-facebook-data-privacy.html [https://perma.cc/R64H-TCLK]; Zeynep Tufecki, *Think You're Discreet Online? Think Again*, N.Y. TIMES (Apr. 21, 2019), https://www.nytimes.com/2019/04/21/opinion/computational-inference.html [https://perma.cc/YT2M-HK6H]; Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreements*, VICE (July 25, 2019, 10:54 AM), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement [https://perma.cc/C99Z-QX9H]; Eric Goldman, *An Email Inbox Isn't a "Place" for Purposes of Florida Privacy Law–Hall v. Sargeant*, TECH. & MARKETING L. BLOG (Apr. 11, 2019), https://blog.ericgoldman.org/archives/2019/04/an-email-inbox-isnt-a-place-for-purposes-of-florida-privacy-law-hall-v-sargeant.htm [https://perma.cc/M565-NQ22]; Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html [https://perma.cc/UU55-MJBQ]; Geoffrey A. Fowler, *Alexa has been eavesdropping on you this whole time*, WASH. POST (May 6, 2019, 8:00 AM), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/ [https://perma.cc/4AND-44N8]; Megan Wollerton, *Aibo's dark side: Why Illinois bans Sony's robot dog*, CNET (Apr. 1, 2019, 5:00 AM), https://www.cnet.com/news/what-sonys-robot-dog-teaches-us-about-biometric-data-privacy/ [https://perma.cc/LA48-9ZE3]; Rob Dozier, *Big Tech Lobbying Gutted a Bill that Would Ban Recording You Without Consent*, MOTHERBOARD (Apr. 12, 2019, 8:00 AM), https://www.vice.com/en_us/article/ywyzm5/big-tech-lobbying-gutted-a-bill-that-would-ban-recording-you-without-consent [https://perma.cc/2KZK-RB3B]; Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html [https://perma.cc/6XWK-6PAQ]; Sam Biddle, *In Court, Facebook Blames Users for Destroying Their Own Right to Privacy*, INTERCEPT (June 14, 2019, 10:50 AM), https://theintercept.com/2019/06/14/facebook-privacy-policy-court/ [https://perma.cc/XSP9-NA2W]; Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/66EX-PU6A]; George Joseph & Murtaza Hussain, *FBI Tracked an Activist Involved with Black Lives Matter as They Travelled Across the U.S., Documents Show*, INTERCEPT (Mar. 19, 2018, 10:29 AM), https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/ [https://perma.cc/6U3E-84FP]; Sam Biddle, *Hacked Border Surveillance Firms Wants to Profile Drivers, Passengers, and Their "Likely Trip Purpose" in New York City*, INTERCEPT (July 9, 2019, 1:49 PM), https://theintercept.com/2019/07/09/surveillance-perceptics-new-york-city-drivers/ [https://perma.cc/C8N8-SJLK]; Nidhi Prakash, Julia Reinstein & Salvador Hernandez, *Homeland Security Is Investigating Immigration Officials' Secret List Of Journalists, Attorneys, And Activists To Question At The Border*, BUZZFEED NEWS (Mar. 7, 2019, 6:32 PM), https://www.buzzfeednews.com/article/nidhiprakash/0homeland-security-investigating-secret-list-immigration [https://perma.cc/GMY3-GBTR]; Seth Harp, *I'm a Journalist But I Didn't Fully Realize the Terrible Power of U.S. Border Officials Until They Violated My Rights and Privacy*, INTERCEPT (June 22, 2019, 7:00 AM), https://theintercept.com/2019/06/22/cbp-border-searches-journalists/ [https://perma.cc/B2V6-5QMV]; Tom Jackman, *Judge Orders Fairfax Police To Stop Collecting Data From License Plate Readers*, WASH. POST (Apr. 2, 2019), https://www.washingtonpost.com/crime-law/2019/04/02/judge-orders-fairfax-police-stop-collecting-data-license-plate-readers/ [https://perma.cc/CX4J-AKAP]; Andrew Crocker, *To Search Through Millions of License Plates, Police Should Get a Warrant*, ELECTRONIC FRONTIER FOUND. (Mar. 22, 2019), https://www.eff.org/deeplinks/2019/03/search-through-millions-license-plates-police-should-get-warrant [https://perma.cc/GD4F-A3FZ]; Aaron Mak, *Facing Facts*, SLATE (Jan. 25, 2019, 12:49 PM), https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html [https://perma.cc/SFG3-HE3T]; Nicole Karlis, *San Francisco's facial recognition ban still lets corporations spy on you*, SALON (May 21, 2019, 11:00 PM), https://www.salon.com/2019/05/21/san-franciscos-facial-recognition-ban-still-lets-corporations-spy-on-you/ [https://perma.cc/4UG6-VGAK]; James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html

Memorial Lecture in Law & Civil Rights at The University of New Mexico School of Law.[20] Some of these supplemental materials are discussed below, including the concept of sexual privacy and the emergence of "sharenting." Even with these supplemental materials, and just like the content in the casebook, my syllabus itself could be updated during the semester.

One way I seek to keep pace with privacy law issues that arise during the course of the semester is requiring students to do short current event presentations. Students write a short summary and provide a brief presentation on a current event that connects to material we have covered to date. Specifically, students are asked to find a news article from the current calendar year and post the following on our online course platform: (1) a citation and link to the news article; (2) citations to required course readings we have already covered that connect to that current event; and (3) no more than four paragraphs explaining the connection to required course materials and key course themes. Students provide a three-to-five minute in-class presentation the day after posting this content. Not only do these current event assignments help the course material remain current, they also serve as a useful pedagogical tool to help the students engage with the materials and connect the key course themes to material that they discover on their own. The current event presentations also provide a public

---

[https://perma.cc/2ZC4-8NTZ] Catie Edmonson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/F7M5-VLE6]; Janus Rose, *Amazon Says The Face Recognition Tech It Sells to Cops Can Now Detect 'Fear'*, MOTHERBOARD (Aug. 13, 2019, 4:47 PM), https://www.vice.com/en_us/article/7x59z9/the-facial-recognition-system-amazon-sells-to-cops-can-now-detect-fear [https://perma.cc/95T8-JCP5].

18. State v. VanBuren, 214 A.3d 791 (Vt. 2019); Manigault-Johnson v. Google, LLC, No. 2:18-CV-1032-BHH, 2019 WL 3006646 (D.S.C. Mar. 31, 2019); Carpenter v. United States, 138 S. Ct. 2206 (2018); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018); United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018); United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018); United States v. Touset, 890 F.3d 1227 (11th Cir. 2018); United States v. Yang, No. 2:16-CR-231-RFB, 2018 WL 576827 (D. Nev. Jan. 25, 2018); Neal v. Fairfax Cty. Police Dept., No. CL-2015-5902, 2019 WL 1438078 (Va. Cir. Ct. Apr. 1, 2019) (order granting injunction); Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant and Reversal, United States v. Williams, 942 F.3d 1187 (10th Cir. 2019) (No. 18-1299); Brief of Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Indiana in Support of Appellant, Seo v. State, 112 N.E.3d 1082 (Ind. 2019) (No. 18S-CR-595); State's Response to Brief of Amicus Curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Liberties Union of Indiana, Seo v. State, 112 N.E.3d 1082 (Ind. 2019) (No. 18S-CR-595).

19. Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019); Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019).

20. Alvaro Bedoya, Remarks at U.S. Senator Dennis Chavez Memorial Lecture in Law & Civil Rights at The University of New Mexico School of Law, Privacy and Civil Rights in the Age of Facebook, ICE, and the NSA, (Apr. 4, 2019). Shahid Buttar, *Alvaro Bedoya Highlights the Critical Connection between Civil Liberties and Civil Rights*, ELECTRONIC FRONTIER FOUND. (Apr. 25, 2019), https://www.eff.org/deeplinks/2019/04/dennis-chavez-memorial-lecture-alavaro-bedoya-highlights-critical-connection [https://perma.cc/5587-UE3C].

speaking opportunity and thus some practice developing a key lawyering skill.

When laying a foundation for the information privacy law courses, I add a supplemental framework that I borrowed from Lawrence Lessig. In making the case that studying "cyberlaw" is a worthwhile endeavor, and not simply a modern-day example of the "Law of the Horse," Lessig identified four modalities that regulate human behavior. Those four modalities are: (1) law, (2) social norms, (3) markets, and (4) architecture.[21] Introducing these four modalities that regulate human behavior is probably helpful for any study of law because it highlights that law is only one potential modality that can be used (alone or in conjunction with the other modalities) to guide human behavior. It may be easy to lose sight of this truism when immersed in a three-year law school curriculum. Highlighting these four modalities is particularly relevant when studying information privacy because of the ways that technology continually disrupts existing understandings of privacy and because existing legal doctrine sometimes precludes recourse through the law when privacy interests are harmed. "Sharenting" is one example, discussed more below, where existing law precludes legal remedy for privacy invasions caused by parents posting images and videos of their children online.[22] To be sure, privacy as a concept must be distinguished from privacy as a right.[23] There are times when privacy is desired, but the law does not (and sometimes should not) provide privacy rights.[24] One example, discussed more below, might be an individual who attended a Phish concert and had his reaction to a song become a viral meme overnight. Offering this supplemental framework allows students to better situate the study of law as one mere (albeit essential) component of how social systems can set boundaries for human behavior.

---

21. Lessig, *supra* note 7, at 507–508.

22. *See* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839 (2017) (advocating for a public health model approach where parents are educated on "sharenting" harms because First Amendment law and legal protection for parental authority over children are likely to preclude legal rights of children against their parents for privacy harms resulting from oversharing photos and content online). Sharenting is discussed below in the section on Autonomy and Consent.

23. SOLOVE & SCHWARTZ, *supra* note 2, at 41 ("At the outset, it is important to distinguish between the concept of privacy and the right of privacy.").

24. *E.g.*, New York Times Co. v. United States, 403 U.S. 713 (1971) (the "Pentagon Papers" case where the Supreme Court held that the government could not impose a prior restraint on further publication of the Pentagon Papers); Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555 (1980) (the First Amendment protects a presumptive right of public access to criminal trials); Bartnicki v. Vopper, 532 U.S. 514 (2001) (the First Amendment protected publication of an illegally recorded telephone conversation because the radio station did not participate in the underlying illegal recording and the content of the call was a matter of public concern); FCC v. AT&T Inc., 562 U.S. 397, 401 (2011) (Freedom of Information Act exemption 7(c) that allows government agencies to withhold law enforcement records that "could reasonably be expected to constitute an unwarranted invasion of personal privacy" does not apply to corporations).

III. TEN KEY COURSE THEMES

The ten key course themes and Lessig's four modalities are set forth on the first day of both Information Privacy Law I and II. After identifying and providing a brief description of the ten key course themes, this section provides vignettes of three themes to provide a glimpse of how they underlie and connect course readings. Some themes include two closely related and somewhat overlapping concepts. The ten key course themes are:

- **Surveillance.** Surveillance is a field of study in its own right.[25] In the not too-distant-past, surveillance was largely conceptualized as government action.[26] Today, however, it seems nearly impossible to think of surveillance without also thinking about how private actors engage in surveillance behavior.[27] The title and content of Shoshana Zuboff's 2019 book, "The Age of Surveillance Capitalism," make this point clear.[28] This *Washburn Law Journal* symposium edition also includes an important and underexplored issue of surveillance by a specific type of private actor in Erin Carroll's *News as Surveillance*.[29]
- **Aggregation.** In the age of Big Data, one cannot escape the concept of aggregation when studying information privacy law. Relatively early case law involved claims of privacy violations because of data aggregation.[30] In 2018, Vermont passed the nation's first law regulating data brokers.[31] In large part, Vermont passed the law to address the risks of harm created by widespread data aggregation.[32] Although concerns about privacy harms from data aggregation have been amplified in the age of Big Data, they are not new concerns.[33]

---

25. *E.g.*, DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW (2007).

26. The online Merriam-Webster dictionary defines "surveillance" as "close watch kept over someone or something (as by a detective)." *Surveillance*, MERRIAM-WEBSTER DICTIONARY, available at https://www.merriam-webster.com/dictionary/surveillance [https://perma.cc/D3T9-458W] (last visited Mar. 25, 2020).

27. To be sure, concerns about surveillance by private actors have existed for some time now. *E.g.*, Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) ("First, we must recognize that surveillance transcends the public/private divide.").

28. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

29. Erin C. Carroll, *News as Surveillance*, 59 WASHBURN L.J. – (2020).

30. *E.g.*, In re Google, Inc. Privacy Policy Litig., 2013 WL 6248499, *3 (N.D. Cal. Dec. 3, 2013) (plaintiffs' claims were based in part on allegations that "they purchased an Android phone before March 1 and that after implementing the new policy Google aggregated their personal information without consent or compensation.").

31. VT. STAT. ANN. tit. 9 § 2447 (2020).

32. *Report to the General Assembly of the Data Broker Working Group Issued Pursuant to Act 66 of 2017*, OFF. ATT'Y GEN., 1, 7 (Dec. 15, 2017), https://ago.vermont.gov/wp-content/uploads/2018/02/2017-12-15-Data-Broker-Working-Group-Report.pdf [https://perma.cc/9ZGZ-YDMW].

33. For example, in 1971, Arthur Miller raised concerns about a "comprehensive womb-to-tomb dossier on every individual and transmitting it to a wide range of data users over a national network." ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA, BANKS, AND DOSSIERS 39 (University of Michigan Press 1971). The Fair Credit Reporting Act of 1970 also addressed concerns

- **Public "versus" Private.** I include the scare quotes because "versus" does not fully capture this theme. Sometimes public and private actors (or spaces) cannot be neatly divided.[34] Sometimes the word "and" might be a better descriptor, such as when describing Amazon's subsidiary, Ring, partnering with law enforcement.[35] Ultimately, however, "versus" seems like a useful starting place for the conversation. This theme is divided into two sub-themes:
  - **Public "versus" Private Actors.** Debate regarding the appropriate legal regulation of an actor based on its classification as public or private is by no means limited to privacy law.[36] This debate is particularly salient in privacy law for at least two reasons. First, public and private actors often work together in ways that cause privacy harms.[37] Second, the power that private actors possess to create privacy harms often exceeds the power of state actors.[38]
  - **Public "versus" Private Spaces.** This sub-theme is discussed below in the contexts of a viral meme and face recognition technology.
- **Power.** Power is a closely related concept to the public "versus" private theme. I often introduce the public "versus" private theme and then introduce the concept of power by raising the question: Is our main concern the designation of the actor or the power of that actor, regardless of whether it a public or private actor? For example, both Facebook and the United States government wield immense power over individuals. Are we not concerned about Facebook's power over individuals simply because it is a private actor? If we are concerned about the power of private actors, what

---

of data aggregation by consumer reporting agencies. The Congressional Findings and Statement of Purpose section states that consumer reporting agencies have "grave responsibilities" with respect to a "consumer's right to privacy." 15 U.S.C. § 1681(a)(4) (2020).

34. *E.g.*, Richards, *supra* note 27.

35. Lauren Goode & Louise Matsakis, *Amazon Doubles Down on Ring Partnerships with Law Enforcement*, WIRED (Jan. 7, 2020, 8:02 PM), https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/ [https://perma.cc/D6BQ-7XWM].

36. *E.g.*, Danielle C. Jefferis, *Constitutionally Unaccountable: Privatized Immigration Detention*, 95 IND. L.J. 145 (2020) (constitutional protections should apply in the context of civil detentions by for-profit private actors, in large part, to protect dignity of detainees); Marsh v. Alabama, 326 U.S. 501 (1946) (constitutional claims can be made against a company-owned town); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 505 (1985) ("I suggest that it is time to begin rethinking state action. It is time to again ask why infringements of the most basic values—speech, privacy, and equality—should be tolerated just because the violator is a private entity rather than the government.").

37. Richards, *supra* note 27. *See also* Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1369 (2003) ("Privatization is now virtually a national obsession. Hardly any domestic policy issue remains untouched by disputes over the scope of private participation in government . . . .").

38. *See, e.g.*, Shoshana Zuboff, *The Secrets of Surveillance Capitalism*, FRANKFURTER ALLGEMEINE (May 3, 2016, 1:23 PM), https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html [https://perma.cc/TMK8-MCT3] ("[T]he real truth is that the surveillance capabilities being developed by surveillance capitalists are the envy of every state security agency.").

does this mean for the constraints of current constitutional interpretation as applied to private actors, as well as the political will to regulate powerful private actors through legislative action?[39] To be clear, the purpose of this course theme is not to suggest that we simply impose equivalent constitutional obligations on private actors in toto.[40] Instead, the purpose is help students avoid a "major blind spot [of] contemporary libertarianism, which is rightly concerned with government overreach but bizarrely tolerant of mistreatment or abuse committed by so-called private actors."[41]

- **Human Dignity/Inviolate Personality.** This theme is discussed in more detail below in the context of sexual privacy. That said, no introductory conversation about privacy law can begin without referencing Samuel Warren and Louis Brandeis's seminal law review article where they advocated for a right to privacy primarily to protect the "inviolate personality."[42]
- **Autonomy/Consent.** This theme is discussed in more detail below in the context of "sharenting." As a starting point, however, the scholarly discussion of "autonomy" is fraught with uncertainty as to exactly what this term means.[43] Further, courts and commentators agree that the concept of "consent" is problematic, at least when one considers the legal fiction of consent in contract law.[44] Nonetheless,

---

39. For a discussion of general apathy or aversion to regulating private power in the United States, *see generally* TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (Columbia Global Reports 2018). For interesting research and analysis by a psychology professor on how increases in power change human behavior and perspective, *see* DACHER KELTNER, THE POWER PARADOX: HOW WE GAIN AND LOSE INFLUENCE (Penguin 2017). For an excellent song that echoes this theme, listen to, "Killing Fields" by The Last Internationale, TLImusic, *The Last Internationale – Killing Fields (Live at New Monkey Studios)*, YOUTUBE (Jan. 9, 2017) https://www.youtube.com/watch?v=XZ4pK4fZ6mo [https://perma.cc/NM63-ZWKD] ("Power is power, love. No matter who's on top.").

40. *See* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1194 (2018) ("[I]t is unhelpful to impose a rigid distinction between public and private power to understand digital speech today. This is not a claim that infrastructure owners should be treated as state actors."); *see also* Prager Univ. v. Google LLC, 951 F.3d 991 (9th Cir. 2020) ("YouTube does not perform a public function by inviting public discourse on its property. . . . To characterize YouTube as a public forum would be a paradigm shift.").

41. WU, *supra* note 39, at 41.

42. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

43. *E.g.*, Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 876 (1994) ("Autonomy, however, is a protean concept, which means different things to different people, and occasionally appears to change its meaning in the course of a single argument."); Jed Rubenfeld, *The Riddle of Rape-by-Deception and the Myth of Sexual Autonomy*, 122 YALE L.J. 1372, 1417 (2013) ("Autonomy is a big and loaded concept, with multiple possible meanings across a variety of contexts."); James Grimmelmann, *Speech Engines*, 98 MINN. L. REV. 868, 896 n.151 (2014) ("Autonomy is a contested concept with multiple overlapping meanings."). For a discussion of autonomy and privacy, *see* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1116–24 (2002).

44. *See, e.g.*, In re Facebook, Inc. Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019) (current law requires courts "to pretend that users actually read Facebook's contractual language before clicking their acceptance, even though we all know virtually none of them did. Constrained by this fiction, the Court must analyze the relevant contractual language to assess whether the users 'agreed' to allow Facebook to disseminate their sensitive information . . . ."); Joshua A.T. Fairfield, *The Search Interest in Contract*, 92 IOWA L. REV. 1237, 1262 (2007) ("As things stand,

taken together, these closely related concepts serve a useful role in framing how one might think about information privacy law. Indeed, consent is a major component of the European Union's General Data Protection Law,[45] as well as a cornerstone of the Fair Information Practice Principles ("FIPPs") set forth in a foundational 1973 report.[46]

- **Obscurity.** Woodrow Hartzog and others have written about this concept in both legal scholarship and the popular press.[47] In short, the concept of obscurity might better explain some instances where people desire (or previously had) "privacy." For example, when the Court of Justice of the European Union applied the EU's "right to be forgotten" in 2014, it required Google to delist a newspaper article from its search results that appeared when one would search for "Costeja González," but it did not require the newspaper to remove that article from its online website.[48] Thus, that news article was not completely forgotten or removed from the internet but was made much more obscure because it did not populate in Google search results for "Costeja González."
- **Purposes of Privacy: Individual and Collective.** Perhaps the first reaction one might have when thinking about privacy is to view it as an individual interest. This immediate reaction is not wrong, but it is far from the whole story. Privacy has played and continues to play an essential role in furthering collective ends, particularly in the context of a democracy. Publication of the Federalist Papers under the pseudonym "Publius" is a classic example of privacy serving a collective end. The United States Supreme Court has also acknowledged the value of privacy for collective ends. In 1958, the Court recognized a First Amendment right to associational privacy when it denied the state of Alabama access to the NAACP's membership list.[49] In 1995, the Court recognized a qualified right to anonymous speech in the context of political speech when it held unconstitutional an Ohio Election Code provision prohibiting the

---

therefore, courts and statutes have stretched the legal fiction of negotiated consent beyond the breaking point of reason or experience."). *See generally* R. George Wright, *Clicking Through Consent*, 64 WAYNE L. REV. 315 (2019).

45. Council Regulation, 2016/679, art. 7, 2016 O.J. (L 119) (EU) ("Conditions for Consent").

46. *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens*, U.S. DEPT. HEALTH, EDUC. & WELFARE (1973). The FIPPs form the basis for the recently approved Draft Restatement of Data Privacy. Solove & Schwartz, *supra* note 4, at 7 ("The primary contribution of the *Principles* is to attempt to revitalize the application of the Fair Information Practice Principles (FIPPs) in U.S. privacy law.").

47. *E.g.*, Woodrow Hartzog, *The Case for Online Obscurity*, 101 CAL. L. REV. 1 (2013); Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html [https://perma.cc/KT6B-BRSB]; David Hoffman, Paul Bruening & Sophia Carter, *The Right to Obscurity: How We Can Implement the Google Spain Decision*, 17 N.C. J.L. & TECH. 437 (2016).

48. *Report of Cases*, EUR-LEX *(May 13, 2014),* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN *[https://perma.cc/5ZBR-GRNK].*

49. NAACP v. Ala. ex rel. Patterson, 357 U.S. 449 (1958).

distribution of anonymous campaign literature.[50] Commentators have written about the critical role that anonymity provides in a democracy.[51] The use of face recognition technology raises new questions and concerns for democracy.[52] Expressly identifying that privacy has both individual and collective purposes is helpful in framing the scope of an information privacy law course.

- **Proper Legal Classification of Privacy.** In short, there does not seem to be a singular answer to this question. In 1890, Warren and Brandeis explained why contract law, property law, and intellectual property law, for a few examples, were insufficient to protect the scope of what privacy seeks to cover.[53] Today, it seems difficult to exclude property law as playing some role in the privacy law discussion because the "fuel" of the "information economy" is data, often times personal, "private" data.[54] But, just as in 1890, property law alone remains an inadequate classification to capture all of the interests that "privacy" seeks to address. To add to the mix, commentators who are labeled as "reductionists" contend that privacy as a concept might not be necessary (or may even be detrimental) because other doctrinal areas of law taken together can suffice.[55] Identifying the classification question may help students think more broadly about the interests that privacy law seeks to address and more creatively about legal pathways to protecting those interests.
- **Courts "versus" Legislatures "versus" Administrative Agencies.** Finally, like at least some other key course themes, this one clearly transcends the topic of privacy. Assuming some type of government regulation is in play, the question of the proper branch (or branches) of government to set the rules is a prominent one in the context of privacy law because of how quickly new issues emerge. Others have previously recognized this point.[56] Also, like the public

50. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

51. *E.g.*, Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 746 (1987) ("The processing of personal data is not unique to a particular society. . . . For a democratic society, however, the risks are high: labeling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control threaten the very fabric of democracy."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999); Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861 (2014); *see* Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH 106 (2019).

52. *The Guardian View on Facial Recognition: A Danger to Democracy*, GUARDIAN (June 9, 2019, 1:30 PM), https://www.theguardian.com/commentisfree/2019/jun/09/the-guardian-view-on-facial-recognition-a-danger-to-democracy [https://perma.cc/8Z84-SMXD]; Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1614 (2017) ("[F]acial recognition impinges on several concepts that were critical to the Framers in crafting the Constitution, including . . . the preservation of a democracy.").

53. Warren & Brandeis, *supra* note 42, at 211–12.

54. Solove & Schwartz, *supra* note 4, at 4.

55. *See* SOLOVE & SCHWARTZ, *supra* note 2, at 55.

56. Anastopoulo & Gressette, *supra* note 8, at 412–14.

> "versus" private theme, the "versus" term does not provide the full picture because often there is interaction between different branches of government.[57] The early development of privacy law provides a useful comparison to highlight this theme. In the years shortly after Warren and Brandeis called for recognizing a right to privacy, the highest courts in two states confronted the question of whether to recognize a common law right of misappropriation. In 1902, the Court of Appeals of New York rejected this request because it viewed the creation of such a right to be within the province of the legislature.[58] Three years later, the Georgia Supreme Court reached the opposite conclusion.[59] It reasoned that a "right to privacy in matters purely private is . . . derived from natural law."[60] Thus, these two judicial decisions cleanly set up the fundamental question of lawmaking in a common law system. Moreover, within one year after the Court of Appeals of New York declined to create a common law misappropriation right, the New York legislature did just that, thereby illustrating the interaction between courts and legislatures.[61] Solove and Schwartz introduce these two cases early in the casebook,[62] as well as a 1998 Minnesota Supreme Court case in which the majority recognized three invasion of privacy claims for the first time in Minnesota, but the dissent criticized the majority for overstepping the limits of judicial authority.[63]

Once one begins to view the required materials through this lens, it is almost impossible not to see these themes. As one former student wrote unsolicited in an email to me: "I cannot read an article about privacy now without thinking about how it applies to key course themes."[64] The purpose of this essay, however, is not to engage in a tedious march through each of these themes and all of the places they appear. That task could not be fully

---

57. Perhaps even more so than public "versus" private, the term "versus" does not completely and accurately capture this theme. There are often times where judicial opinions state that the relief sought is outside the jurisdiction of the court and that the legislature is the proper entity from which the party should seek relief. But other times, it is not a question of which branch of government should regulate privacy, but an interaction between two or more branches of government. Peter Swire makes this very point, which Solove & Schwartz include along with other views in a Note & Question titled "The Courts vs. Congress." SOLOVE & SCHWARTZ, *supra* note 2, at 318–19.

58. Roberson v. Rochester Folding Box Co., 64 N.E. 442, 443 (1902) (While the legislature could create this right, "[t]he courts . . . being without authority to legislate, are required to decide cases upon principle, and so are necessarily embarrassed by precedents created by an extreme, and, therefore, unjustifiable application of an old principle.").

59. Pavesich v. New England Life Ins. Co., 50 S.E. 68, 80–81 (1905).

60. *Id.* at 70.

61. N.Y. Laws Ch. 132 §§ 1-2 (1903). The original version of the act is available in LEGISLATIVE DRAFTING COMMISSION, LAWS OF THE STATE OF NEW YORK PASSED AT THE SESSIONS OF THE LEGISLATURE 1, 308 (1903), https://babel.hathitrust.org/cgi/pt?id=nyp.33433090742549&view=1up&seq=320 [https://perma.cc/7RK7-3RJY]. Today, the law is N.Y. CIV. RIGHTS LAW §§ 50-51 (2019).

62. SOLOVE & SCHWARTZ, *supra* note 2, at 25–26.

63. *Id.* at 29–31 (case excerpt of Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (1998)).

64. Email from a former student to author, *supra* note 12.

accomplished over the course of two semesters, let alone one essay. Instead, the purpose of this Essay is to highlight a few of the themes, illustrate how they connect and overlap with one another, and hopefully make a small contribution to the pedagogical and normative literature on information privacy law. To that end, the remainder of this essay offers vignettes to illustrate the themes of autonomy/consent, human dignity/inviolate personality, and public "versus" private spaces.

A. Autonomy/Consent and Sharenting

When I teach first-year Contracts, one of the key points I emphasize to students on their first day comes from the preface of the casebook: "No study of law is adequate if it loses sight of the fact that law operates first and last, *for*, *upon*, and *through* individual human beings."[65] A fundamental part of being human is autonomy. Although the value of autonomy as an integral part of being human cannot be overstated, the concept of autonomy in legal and philosophical scholarship cannot be uniformly explained and is often debated.[66] At least at a rudimentary level, however, autonomy conveys the idea that one is free (or largely free) to make her own decisions. Moreover, autonomy is a critical part of being human from a very early age.[67] And, through autonomous decision-making, one can consent to foregoing some of this freedom. Perhaps the amorphous concept of autonomy is sometimes overlooked or taken for granted in the grand scope of a three-year legal education where more concrete goals are understandably emphasized (or are at least front-of-mind for students), like learning bar-tested rules of law and developing practical lawyering skills in clinics. One way I seek to bring the concepts of autonomy and consent to the forefront in a privacy law context is through the example of a relatively new phenomenon and neologism: "sharenting."

"Sharenting" is a "term used to describe the ways many parents share details about their children's lives online."[68] This sharing can begin before birth by posting sonogram images.[69] Most of the time, posting images and

65. CHARLES L. KNAPP, NATHAN M. CRYSTAL, & HARRY PRINCE, PROBLEMS IN CONTRACT LAW, xxiv (Wolters Kluwer 9th ed. 2019) (emphasis in original). This sentence has been in every edition of the casebook dating back to the first edition in 1976. *Id.* at xxiii–xxiv.

66. *See supra* note 43 and accompanying text.

67. *See generally* Marilena Côté-Lecaldare, Mireille Joussemet & Sarah Dufour, *How to Support Toddlers' Autonomy: A Qualitative Study With Child Care Educators,* EARLY EDUC. & DEV., 27, 822–40 (2016), https://www.tandfonline.com/doi/full/10.1080/10409289.2016.1148482 [https://perma.cc/K8ES-ZE6L].

68. Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 842 (2017).

69. Anya Kamenetz, *The Problem with 'Sharenting'*, N.Y. TIMES (June 5, 2019), https://www.nytimes.com/2019/06/05/opinion/children-internet-privacy.html [https://perma.cc/8WQR-2UZ7].

details about children online is simply because a loving parent wants to share this joy with family and friends. Sometimes, however, an added layer of complexity arises when parents "sharent" for profit by turning their children into so-called "kidfluencers."[70] In any case, autonomy and consent concerns arise even when the intent of the sharing derives from a place of love. Sharenting raises challenging questions that directly connect to autonomy and consent because it may involve a conflict of interest between parents' free speech rights and traditional parental authority rights on the one hand, and a child's privacy interests on the other.

A recent *New York Times* video interview compilation of conversations between children and their respective parents nicely illustrates the value of autonomy to children.[71] Seven-year-old Lucy Petrzela and her mother discussed the mother posting a photograph of Lucy on social media without Lucy's consent. Lucy's mother said, "If I'd asked you about the picture would you be okay if I posted it?" Lucy replied "yes." To which her mother responded, "Oh, really. So it's actually about the asking, not about the picture itself?" Lucy seemed to agree. This anecdotal example shows the importance of autonomy and the closely related concept of consent to human beings, even at a young age. Moreover, it does so in the context of a new information privacy issue where one can debate whether the law can or ought to interfere with parents' speech rights and traditional parental authority for the purpose of protecting a child's autonomy. More broadly, this example helps establish that autonomy and consent are fundamental considerations as we confront privacy disruptions caused by technological development. Even if neither legal scholars nor philosophers will ever reach a consensus on precisely what autonomy means, it is a concept that underlies our legal system in large part and plays a significant role in determining when privacy as a concept should also be privacy as a right.

B. Human Dignity/Inviolate Personality and Sexual Privacy

Another key course theme closely related to autonomy and consent is human dignity and the inviolate personality. Like autonomy, the concept of human dignity in law is also fraught with uncertainty and rich in legal

70. Sapna Maheshwari, *Online and Making Thousands, at Age 4: Meet the Kidfluencers*, N.Y. TIMES (Mar. 1, 2019), https://www.nytimes.com/2019/03/01/business/media/social-media-influencers-kids.html [https://perma.cc/7F8F-TL9J].

71. Zoya Garg, Elmer Gomez, & Luciana Yael Petrzela, *If You Didn't 'Sharent,' Did You Even Parent?*, N.Y. TIMES (Aug. 7, 2019), https://www.nytimes.com/2019/09/19/learning/film-club-if-you-didnt-sharent-did-you-even-parent.html [https://perma.cc/D3FJ-FQLN].

commentary.[72] "In this sense, dignity [and autonomy] share[] many of the frustrating traits of privacy."[73] Also like autonomy, however, the concept of human dignity is foundational to our legal system and at a base level means something to all of us.

The phrase "inviolate personality" is forever tied to privacy law because it is the key phrase in Warren and Brandeis's seminal 1890 article, and it is the key reason why they advocated for a right to privacy. Other areas of law, such as contracts and property, were inadequate to protect intangible privacy interests.[74]

The emerging concept of sexual privacy law provides a powerful way to integrate the related concepts of human dignity and inviolate personality into the course.[75] In a 2019 article, Danielle Citron defined "sexual privacy" as "the behaviors, expectations, and choices that manage access to and information about the human body, sex, sexuality, gender, and intimate activities."[76] Sexual privacy immediately evokes notions of human dignity and inviolate personality in an almost tautological way. As Citron wrote, sexual privacy is "foundational to human dignity."[77] Moreover, Citron's article provides a way to show explicitly the overlap between key course themes because she notes that sexual privacy is a "cornerstone for sexual autonomy and consent."[78]

Not only is sexual privacy a concept foundational to human dignity, it provides an excellent way to show students the connection between theory and practice through the example of the development of statutory law regulating non-consensual pornography. In 2016, *The New Yorker* described attorney Carrie Goldberg as a "pioneer" with a "practice specializing in sexual privacy, a new field of law that has emerged, in large part, to confront some of the grosser indulgences of the Internet."[79] One of those relatively early gross indulgences of the internet was "revenge porn,"

72. Edward J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, 1997 UTAH L. REV. 963, 964 (1997) ("The quest for human dignity in modern society is a noble but elusive goal. Difficult to define, difficult to realize, personally or socially, dignity nevertheless remains a defining trait of human character, and a preeminent ideal of western society."); John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 676 (2008) ("Across all disciplines, human dignity is an underexplored topic. Perhaps the most telling thing that can be said is that 'dignity can mean many things,' and that there is no universally agreed-upon definition. And yet, it must mean something.").

73. Castiglione, *supra* note 72, at 676 n.94.

74. Warren & Brandeis, *supra* note 42.

75. *See* Danielle Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

76. *Id.* at 1873.

77. *Id.*

78. *Id.*

79. Margaret Talbot, *The Attorney Fighting Revenge Porn*, NEW YORKER (Nov. 28, 2016), https://www.newyorker.com/magazine/2016/12/05/the-attorney-fighting-revenge-porn [https://perma.cc/FS5A-A6YQ].

which is more accurately described as "non-consensual pornography" because people post these images and videos for reasons other than just revenge.[80] Initially, the legal system seemed to lack a way to provide either civil remedies or criminal penalties for such behavior, partly because existing law did not seem to cover this conduct and partly because of First Amendment concerns.[81] Creative lawyers were sometimes able to turn to copyright law by relying on the takedown procedures provided by the Digital Millennium Copyright Act to have images and videos removed from online platforms.[82] While a helpful legal move in the absence of alternatives, copyright law was an inadequate proxy to protect against the privacy harms caused by non-consensual pornography.

Today, forty-six states, the District of Columbia, and one territory have enacted non-consensual pornography laws.[83] This impressive development of law to meet a new threat created by technological change is the result of practitioners, academics, and others working together to effect legislative change. Practitioner Carrie Goldberg and academics Danielle Citron and Mary Anne Franks (among others) lead the way to educate legislatures about the need for and constitutionality of non-consensual pornography laws. Through this collaborative process between practitioners and academics, the law changed. Thus, not only does the issue of non-consensual pornography illustrate legal protection for dignitary interests, it provides students a concrete example of why understanding legal theory plays an important role in the practice of law.

While great strides in combatting non-consensual pornography have been made in a relatively short time, the problem is by no means solved because non-consensual pornography still occurs. Unfortunately, non-consensual pornography is not the only sexual privacy harm that technological change has wrought. The rise of deep fakes is but one recent

---

80. The Illinois Supreme Court provided two reasons why the term "revenge porn" is misleading:

> First, "revenge" connotes personal vengeance. However, perpetrators may be motivated by a desire for profit, notoriety, entertainment, or for no specific reason at all. The only common factor is that they act without the consent of the person depicted. Second, "porn" misleadingly suggests that visual depictions of nudity or sexual activity are inherently pornographic.

People v. Austin, 2019 IL 123910, ¶18 (2019).

81. *See, e.g.*, Andrew Koppleman, *Revenge Pornography and First Amendment Exceptions*, 65 EMORY L.J. 661 (2016) (noting that the Court's existing categorical First Amendment jurisprudence seems to preclude regulation of non-consensual pornography, but that the text of the First Amendment itself does not require such a conclusion); State v. VanBuren, 214 A.3d 791, 815 (Vt. 2019) (Skoglund, J., dissenting) (Vermont's "revenge porn" law violates the First Amendment).

82. Talbot, *supra* note 79; 17 U.S.C. § 512(c)(3) (2020).

83. *46 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER C.R. INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/Z8KT-X2JG] (last visited Mar. 25, 2020).

example.[84] Some argue for legislation that specifically responds to deep fake pornography.[85] Perhaps that is necessary. But, as Citron notes, we must also think broadly about sexual privacy because new ways of malevolent online conduct will continue to create sexual privacy harms. Citron suggests that sexual privacy should be thought of holistically, that we should see the "constellation of sexual-privacy invasions as a single problem."[86] She situates sexual privacy among other areas where the law has provided heightened privacy protections, such as health and financial information, because "[i]n the hierarchy of privacy values, it is among the most significant to individuals, groups, and society."[87]

Thus, key course theme of human dignity and inviolate personality in the context of sexual privacy does much more work than simply provide a lesson on non-consensual pornography. It demonstrates the value of collaboration between practitioners and academics in addressing new privacy harms and shows how rethinking and expanding existing categories of privacy can help provide structural norms as we continue to face new privacy challenges. These lessons are particularly valuable to the study of information privacy law precisely because students who pursue professional careers in this field will probably have more opportunities to shape the law in ways that they might not in other, more static or entrenched areas of law.

One relatively recent development where existing law seems inadequate to protect dignitary interests is the use of smart home devices as "digital tools of domestic abuse."[88] Echoing concerns from early days of non-consensual pornography, "[l]egal recourse may be limited" when individuals use access to smart home devices to engage in domestic abuse because abusers exercise their power over these devices "in ways that often fall outside existing criminal laws."[89] Perhaps students can find takeaways from the development of non-consensual pornography law to provide

84. Broadly defined, "deep fakes" include "the full range of hyper-realistic digital falsification of images, video, and audio." Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1757 (2019). Deep fake pornography is only one type of problematic deep fakes. *See generally id.*; Edvinas Meskys et al., *Regulating Deep Fakes: Legal and Ethical Considerations*, 15 *J. INTELL. PROP. L. & PRAC.* 24 (Jan. 2020), https://academic.oup.com/jiplp/article/15/1/24/5709090 [https://perma.cc/4PS7-SE38] (providing a taxonomy of deep fakes).

85. Rebecca A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, 88 FORDHAM L. REV. 887 (2019); Douglas Harris, *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, 17 DUKE L. & TECH. REV. 99 (2019).

86. Citron, *supra* note 75, at 1945.

87. *Id.* at 1881. This point also connects to the key course theme that the purposes of privacy are both individual and collective.

88. Bowles, *supra* note 17. To the extent that Citron's definition of sexual privacy covers "intimate activities," the use of digital tools of domestic abuse is at least adjacent to sexual privacy, if not within its scope.

89. *Id.*

solutions in this domestic abuse context, such as collaboration between academics and practitioners to help change the law in beneficial ways. Perhaps they can think about sexual privacy from a larger perspective such that the use of "digital tools of domestic abuse" falls within the "constellation of sexual-privacy invasions" and is part of a "single problem." Perhaps the concepts of human dignity and inviolate personality are the connecting theoretical root between non-consensual pornography, deep fake pornography, the use of digital tools of domestic abuse, and more.

C. Public "Versus" Private Spaces: Viral Memes and Face Recognition Technology

This theme is broken down into two sub-themes: public "versus" private spaces and public "versus" private actors. The public "versus" private actor theme is one that exists throughout law, and privacy law is no exception, especially because public and private actors often work together in ways that create privacy harms. This section focuses on the public "versus" private spaces sub-theme.

A foundational underpinning of privacy as a concept and a right is that it is contextual, not binary.[90] A seminal Fourth Amendment United States Supreme Court decision shows how the law has adopted this contextual approach to privacy, *Katz v. United States*.[91] While using a public phone booth partly made of glass, the Court stated that Katz maintained a reasonable expectation of privacy from the "uninvited ear," even if not the "intruding eye."[92] More recently, the Court confirmed its commitment to a contextual approach to privacy in its Fourth Amendment jurisprudence when it carved out an exception to the third-party doctrine.[93] *Katz* seems like an easy example of privacy's contextual nature. (Perhaps one could

90. *E.g.*, Sanders v. Am. Broad. Companies, 978 P.2d 67, 72 (Cal. 1999) (privacy is "not a binary, all-or-nothing characteristic"); *In re* Facebook, Inc. Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 782 (N.D. Cal. 2019) ("The problem with Facebook's argument is that it treats privacy as an all-or-nothing proposition – either you retain a full privacy interest by not sharing information with anyone, or you have no privacy interest whatsoever by virtue of sharing it even in a limited fashion."); *see* Solove, *supra* note 43 ("what privacy is differs in different contexts"). *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

91. 389 U.S. 347 (1967).

92. Katz v. United States, 389 U.S. 347, 352 (1967).

93. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018). In the 1970s, the Court found no Fourth Amendment violation when the government obtained information from third parties that the defendant ostensibly voluntarily shared with that third party. United States v. Miller, 425 U.S. 435, 446 (1976) (no reasonable expectation of privacy in bank records); Smith v. Maryland, 442 U.S. 735, 735 (1979) (no reasonable expectation of privacy in numbers dialed on a telephone). In *Carpenter*, however, the Court held individuals maintain a reasonable expectation of privacy in historic cell-site location information ("CSLI"), even though that information has been "disclosed" to a third party, the cellular service provider. *Carpenter*, 138 S. Ct. at 2223. The Court carved out this exception because of the extensive information derived from CSLI. *Id.* at 2216 ("cell phone location information is detailed, encyclopedic, and effortlessly compiled").

reasonably argue that it represents a binary example of privacy by framing it as a difference between hearing and seeing.) In any case, this example helps set the table for more complex issues when it comes to privacy expectations in public, such as the use of face recognition technology.

Of course, not every understandable desire for privacy is or ought to be protected as a legal right. Like many legal questions, where to draw the lines is an ongoing conversation. A case that helps flesh out this line-drawing in the context of legal protection for privacy interests in public is the 1953 California Supreme Court decision, *Gill v. Hearst Publishing Company*.[94] In *Gill*, a husband and wife were photographed without their consent while "seated in an affectionate pose at their place of business, a confectionery and ice cream concession in the Farmers' Market in Los Angeles."[95] The photograph was published in at least two magazines in connection with articles involving the topic of love. The husband and wife sued the publishers for unspecified invasion of privacy claims, but the allegations indicate that one of the claims was for public disclosure of private facts.[96] The court held that mere use of the photograph in connection with an otherwise innocuous news article was non-actionable as a matter of law.[97]

The court reasoned that plaintiffs could not establish the required "private" fact element. "[T]he photograph did not disclose anything which until then had been private, but rather only extended knowledge of the

---

94. 253 P.2d 441 (Cal. 1953).

95. Gill v. Hearst Publ'g Co., 253 P.2d 441, 442 (Cal. 1953).

96. According to the Restatement (Second) of Torts:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public.

RESTATEMENT (SECOND) OF TORTS: PUBLICITY GIVEN TO PRIVATE LIFE § 652D (AM. LAW INST. 1977).

97. Although the use of the photograph alone did not give rise to a public disclosure of private facts claim, the Court did allow for the possibility of a claim that the photograph in connection with the content of one of the magazine articles was capable of a false light invasion of privacy claim. The plaintiff alleged that use of the photograph in connection with an article in *Ladies Home Journal* depicted them "in such a manner as to indicate said plaintiffs are loose, dissolute and immoral persons engaged in the so-called 'wrong kind of love.'" Gill v. Curtis Publ'g Co., 239 P.2d 630, 632 (1952). The court held that plaintiffs should have been granted leave to amend their complaint to state a false light claim for this reason. *Hearst Publ'g Co.*, 253 P.2d at 445. The court did not expressly use the term "false light," but that is the gist of the claim allowed to proceed. According to the Restatement (Second) of Torts:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
> (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
> (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

RESTATEMENT (SECOND) OF TORTS: PUBLICITY PLACING A PERSON IN FALSE LIGHT § 652E (AM. LAW INST. 1977).

particular incident to a somewhat larger public than had actually witnessed it at the time of occurrence."[98] But, in this reasoning by the *Gill* majority lies the crux of the line-drawing debate.

The *Gill* dissent seized upon the expanded scope of publication as precisely the reason why publication of the photograph may give rise to a public disclosure of private facts claim. Justice Carter wrote:

> By plaintiffs doing what they did in view of a tiny fraction of the public, does not mean that they consented to observation by the millions of readers of the defendant's magazine. In effect, the majority holding means that anything any one does outside of his own home is with consent to the publication thereof, because, under those circumstances he waives his right of privacy even though there is no news value in the event.[99]

While Justice Carter's 1953 *Gill* dissent may arguably seem antiquated in the age of selfies, Snapchat, and Instagram, that does mean it has no value in today's privacy law conversations. The opposite may be true. Perhaps Justice Carter's concerns about extended publication have more salience today than in 1953. The differential line drawing in *Gill* between the majority and the dissent may be instructive in the context of two recent examples that raise significantly different levels of concern: a viral meme of a concert attendee and the use of face recognition technology by both public and private actors.

On December 30, 2016, Nicholas Peter Orr attended a Phish concert at Madison Square Garden in New York City. A live webcast of the concert was available. During one of the songs, the camera focused on Orr's exuberant reaction to the climactic ending of a song. His reaction went viral[100] and became a meme.[101] Orr attended Phish's concert the following night, also at Madison Square Garden, and other fans recognized him from the prior night's viral video. The online publication *Live for Live Music* interviewed Orr. His reaction to this experience helps students explore key course themes, including privacy in public spaces, consent, and obscurity.[102]

---

98. Hearst Publ'g Co., 253 P.2d at 444.

99. *Id.* at 232–33 (Carter, J., dissenting).

100. Ming Lee Newcomb, *The Internet Is Loving This Kid From the Phish Stream [Watch],* LIVE FOR LIVE MUSIC (Dec. 30, 2016), https://liveforlivemusic.com/news/internet-loving-kid-phish-stream/ [https://perma.cc/FHN7-7FQH].

101. One of the first results for a Google search of "phish kid meme" is Matthew McMahon, *Phish Melts Newbie's Face Off 12/19/16*, YOUTUBE (Dec. 30, 2016), https://www.youtube.com/watch?v=gyaucgkUyPU [https://perma.cc/FM4R-PBU8].

102. Kendall Deflin, *Meet The Phish Fan Whose Reaction To "Harry Hood" Went Viral*, LIVE FOR LIVE MUSIC (Jan. 4, 2017), https://liveforlivemusic.com/features/meet-the-phish-fan-whos-reaction-harry-hood-went-viral/ [https://perma.cc/EN3C-VMB6].

Several fans who recognized Orr from the viral video took his photograph. Orr's reaction to being photographed varied depending on how the photograph happened. If the would-be photographer introduced herself and asked for a photo, his reaction was positive or at least neutral: "I have met a LOT of very cool, fun, and nice people because of it also. I really didn't mind chatting and taking pictures with the people who came up and were friendly and making sure I was cool with it."[103] On the other hand, if the photographer was surreptitious or did not personally interact with Orr, he felt differently: "I noticed a lot of people staring from a distance and some people trying to take sneaky photos, which isn't an incredibly comfortable experience."[104] Orr also expressed a sentiment that helps illustrate the concept and value of obscurity to individuals: "having a bunch of people recognize you at a show is also quite alarming; I'm very used to being anonymous."[105] Orr's reaction harkens back to a main impetus for Warren and Brandeis's advocacy for a right to privacy in 1890, the development of the "instantaneous photographs."[106] As Mark Twain said (or at least is often attributed as saying), history does not repeat, but it rhymes.[107]

Does *Gill* help us think through Orr's experience? Perhaps the *Gill* dissent supports a potential claim by Orr for public disclosure of a private fact because the viral meme (or the webcast itself) extended the publication of Orr's experience far beyond the tiny fraction of people who could have seen him in Madison Square Garden that night. On the other hand, perhaps the position of the *Gill* majority remains the normatively desirable legal outcome. Even if Orr understandably had a desire for some privacy or obscurity in a public space, it is not one that the law does or ought to protect. At the very least, however, we can connect the differential line-drawing between the *Gill* majority and dissent to this contemporary scenario and others.

A more problematic contemporary issue involving privacy in public spaces is the use of face recognition technology. Remarkably, Warren and Brandeis seemed almost prescient when they wrote the following in 1890: "If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial

103. *Id.*
104. *Id.*
105. *Id.*
106. Warren & Brandeis, *supra* note 42, at 231.
107. Brian Adams, *History Doesn't Repeat, But It Often Rhymes*, HUFFPOST (Jan. 19, 2017), at https://www.huffingtonpost.com.au/brian-adams/history-doesnt-repeat-but-it-often-rhymes_a_21657884/ [https://perma.cc/3NYZ-78S8].

expression."[108] Both private and government actors use face recognition technology.[109] Moreover, some claim that technology does more than merely identify an individual. So-called "facial characterization" technology purportedly reads facial expressions.[110] The regulation of face recognition technology is not non-existent, but it is far from adequate.[111] Illinois regulates the use of face recognition technology and other biometric processes by private actors.[112] Some cities have banned the use of face recognition technology by law enforcement.[113] At the time of writing, two United States Senators introduced a bill to put a moratorium on law enforcement use of face recognition technology without a warrant until it can be better understood and regulated.[114]

Underlying the widespread and largely unregulated use of face recognition technology is a threshold question: does one's mere presence in a public space preclude legal regulation of face recognition technology? Because privacy is contextual, including under the Court's existing Fourth Amendment jurisprudence, that answer should be "no." Where to draw the lines, of course, is a more complicated question.

---

108. Warren & Brandeis, *supra* note 42, at 206.

109. *E.g.,* Tom Chivers, *Facial Recognition . . . Coming to a Supermarket Near You*, GUARDIAN (Aug. 4, 2019), https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties [https://perma.cc/9J78-S7FE]; Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/C72J-L5J6]; Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. TIMES (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html [https://perma.cc/2DTV-BNE4].

110. *E.g.*, Alex Emmons, *Microsoft Pitches Technology That Can Read Facial Expressions at Political Rallies*, INTERCEPT (Aug. 4, 2016), https://theintercept.com/2016/08/04/microsoft-pitches-technology-that-can-read-facial-expressions-at-political-rallies/ [https://perma.cc/2VED-CNMW]; Tom Simonite, *Amazon Says It Can Detect Fear on Your Face. You Scared?*, WIRED (Aug. 18, 2019), https://www.wired.com/story/amazon-detect-fear-face-you-scared/ [https://perma.cc/6RZ9-4K5Q].

111. Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEORGETOWN L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/5GUT-ACY9]; Katitza Rodriguez, *Activists Worldwide Face Off Against Face Recognition: 2019 Year in Review*, EFF (Dec. 30, 2019), https://www.eff.org/deeplinks/2019/12/activists-worldwide-face-against-face-recognition-2019-year-review [https://perma.cc/S9XB-LSG8].

112. Illinois Biometric Invasion of Privacy Act, 740 ILCS 14/1, et seq. (2016).

113. *E.g.*, Matthew Guariglia, *Victory! Berkeley City Council Unanimously Votes to Ban Face Recognition*, EFF (Oct. 16, 2019), https://www.eff.org/deeplinks/2019/10/victory-berkeley-city-council-unanimously-votes-ban-face-recognition [https://perma.cc/S34P-77TN] (noting that the cities of Berkeley, Oakland, and San Francisco in California, as well as Sommerville, Massachusetts have banned law enforcement use of face recognition technology). *But see*, Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point*., N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html [https://perma.cc/W6XF-HSRE] (arguing that face recognition bans are "wrong way to fight against modern surveillance [because] [f]ocusing on one particular identification method misconstrues the nature of the surveillance society we're in the process of building.").

114. S. 3284 "Ethical Use of Facial Recognition Act," 116th Congress (2019–2020), available at: https://www.congress.gov/bill/116th-congress/senate-bill/3284/text [https://perma.cc/7SF5-RBPE].

Perhaps Nicholas Orr should have no legal recourse against the meme maker or strangers taking photos of him at a distance, even though one could understand his desire that it not happen and admit that he has lost some obscurity. The use of face recognition technology, however, is not functionally identical to merely being photographed in public.[115] Perhaps the use of face recognition should be regulated because of its effects on one's autonomy, dignity, and democracy and because of the power it bestows on users of the technology, even though one's face is in public. By using key course themes, cases like *Gill*, and insights from Warren and Brandeis regarding privacy rights in "facial expressions," we can begin the process of line drawing privacy rights when one is in public spaces.

IV. CONCLUSION

This essay provides one way to teach information privacy, not the only way. I hope these ten key course themes, supplemented by Lessig's four modalities that regulate human behavior, give students helpful tools to think about existing, unresolved privacy issues and new ones that will inevitably arise as technological development marches on. Moreover, I hope they provide students a way to think about law generally because many, if not all, of these themes play a role in areas of law beyond privacy.[116]

115. Early "cyberlaw" debates about the regulation of "cyberspace" influence my approach to conversations like this one in privacy law because they both involve complex questions of whether existing law is sufficient to address societal changes wrought by technological development and use. *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); *see also* David G. Post, *Against "Against Cyberanarchy"*, 17 BERKELEY TECH. L.J. 1365 (2002) (differentiating between cyberspace "exceptionalists" and "unexceptionalists" based on disagreements regarding whether "cyberspace" is functionally identical to the offline world).

116. *See also*, Goldman, *supra* note 7, at 750 ("From a pedagogical standpoint, specialty courses like Cyberlaw may reinforce basic legal principles for students and provide new insights into these principles, helping students deepen their understanding of the law."). Information privacy law provides a similar educational opportunity.