THE NOTION AND PRACTICE OF REPUTATION AND PROFESSIONAL IDENTITY IN SOCIAL NETWORKING: FROM K-12 THROUGH LAW SCHOOL

By Roberta (Bobbie) Studwell[*]

Social media users often have regrets about some of the information they post, but find themselves unable to remove information that will damage their reputations when they are seeking employment or in other important contexts. Controlling privacy in one's personal information has become nearly impossible. Digital reputations are now more prevalent than ever before, and although individuals may want to change their online persona, legal and non-legal mechanisms that could be put in place to protect them have been instituted too slowly to catch up with the plethora of issues surrounding the social media scene. Remedies to protect unsuspecting social media users are largely unavailable and new proposals aimed at protecting personally identifiable information that is aggregated by commercial entities may take years to test in the courts or to legislate. This author proposes an educational curriculum and training techniques covering the entire kindergarten through post-graduate spectrum as a starting point for discussion that could help to moderate the amount and types of personal information users place in social media settings without anticipating the consequences.

* Associate Dean for Information Services, Barry University Dwayne O. Andreas School of Law.

I. INTRODUCTION TO SOCIAL NETWORKING AND PRIVACY PARADOXES

It is nearly impossible these days to read about technology in a print or digital publication without hearing some admonishment about keeping a person's online identity safe.[1] It is also equally impossible not to see an article about some poor soul being spoofed on Facebook, Twitter, or on another social media site not knowing that she had been caught in the act when she thought her actions were not being observed by anyone else. Many of these unsuspecting social media users have regrets about some of the information they post, but find themselves unable to remove information that will damage their reputations.[2]

Reputation by its very nature is fragile, and most individuals want autonomy and want to be in control of the information that goes into forming someone else's opinion of them. In the age of digital information, controlling that information is becoming more and more difficult.[3] In her book, the *Value of Privacy*, Beate Rossler sums it up nicely; "The reason the protection of information privacy matters so much to a person is that it is an intrinsic part of

1. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 167 (2012) (discussing ways that networked technologies track everything about us, creating records of where a person goes, what she buys, reads, what she likes, and who her friends are); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 65 (2013) (discussing systems capable of aggregating and analyzing large quantities of information from a variety of sources); *Are Today's Students All That Techno-smart? Maybe Not*, ECAMPUS NEWS, Oct. 2012, at 27 (discussing the fact that mastery of devices does not necessarily translate into understanding); CLAY SHIRKY, COGNITIVE SURPLUS: CREATIVITY AND GENEROSITY IN A CONNECTED AGE (2011); *Syracuse Reinstates Student After Facebook Expulsion*, ECAMPUS NEWS Mar. 2012, at 19, (discussing a Syracuse University reversal of a decision to reinstate a student after he posted what were thought to be racist comments on Facebook); *Experts: Go All in with Facebook Use-or Don't Bother*, ECAMPUS NEWS, Nov./Dec. 2012, at 16 (discussing a Kaplan survey of incoming students indicating students are not exercising caution when using social media tools); *see also* Jan L. Jacobwitz, *The Legal Perils of Social Media: Avoiding Landmines in Cyberspace*, CONSUMER REPORTS, July 2014, at 15–20; Daniel Solove, *The Clementi Suicide, Privacy, and How We are Failing Generation Google*, THE HUFFINGTON POST (Oct. 7, 2010, 11:16 AM), https://web.archive.org/web/20150917132640/http://www.huffingtonpost.com/daniel-j-solove/the-clementi-suicide-priv_b_754075.html (noting that the failure "to educate young people about privacy and the consequences of self-disclosure and revelation of information about others" leads Generation Google to make many blunders out of insensitivity and stupidity and how our culture is not taking privacy seriously enough nor is it teaching young people the lessons other generations learned about privacy consequences).

2. *See* Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307 (2013) (providing empirical research about oversharing on Facebook pages and about ways to potentially avoid posting ill-advised information at all).

3. *See, e.g.*, Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581 (2014); Anisha Mehta, Comment, *Bring Your Own Glass: The Privacy Implications of Google Glass in the Workplace*, 30 JOHN MARSHALL J. INFO. TECH. & PRIVACY L. 607, 609 (2014) (exploring wearable technologies such as Forerunner, Fitbit, Galaxy Gear smart watch, and now Google Glass which raise the levels of unauthorized surveillance); Yana Welinder, *Facing Real-Time Identification in Mobile Apps & Wearable Computers*, 30 SANTA CLARA HIGH TECH. L.J. 89, 91 (2013) (discussing new technologies and implications for facial recognition).

her self-understanding as autonomous individuals (within familiar limits) to have control over her self-presentation, that is, control of how she wants to present or stage herself, to whom she want[s] to do so and in which contexts, control over how she wants to see herself and how she wants to be seen."[4]

The fact of the matter is that information privacy,[5] especially concerning information on the Internet, is nearly impossible to protect in the 21st Century.[6] Every person has an online identity and leaves a digital footprint with every digital action he or she takes, intentionally or not. Those footprints can harm or enhance a person's reputation and freedom.[7] Any form of social networking (Facebook, Twitter, rating sites, blog sites, review sites, article commenting sites) or even sites promoted or hosted by a community, a parent, or a school about a citizen, child, or student can immediately add data to both that person's digital dossier and to their digital legacy, depending on how that information is harvested and used.[8]

Additionally, commercial and business practices affect digital footprints. When information is captured and recompiled with other known personal information about a person to create accumulating data stores, the sheer amount of information increases the odds that a person's reputation will suffer. In *Privacy Law*, Brownlee and Waleski discuss the potentially damaging effects that commercial practices such as behavioral marketing and the collection of personally identifiable information (PII)[9] when a person in unaware that it is being collected, present to that person's privacy preferences.[10] They point out that the popularity of social networking sites (such as Facebook) raises new legal issues regarding consensual marketing and spurs debate on the limits of personal data collection.[11] Companies use behavioral marketing techniques to tempt

Commented [ZF1]: Can you please check the original?

Commented [B2]: Previous editor asked me to change the language of the direct quote. Direct quote used "they" instead of my "she", hence the verb difference. – see attached.

Commented [B3]: Per the footnote comment, Solove used the term digital dossiers in this article instead of the term digital footprint he used in his 2006 book.

4. BEATE ROSSLER, THE VALUE OF PRIVACY 116 (R.D. V. Glasgow trans., 2005).

5. Information privacy is defined in this article as who knows what about a person and how they know it, and who controls the information about a person.

6. *See generally* COHEN, *supra* note 1; *but see* Amanda Hess, *Millennials Aren't Oversharing on Social Media. (So What Are They Hiding?)*, SLATE (Oct. 18, 2013, 8:41 AM), https://web.archive.org/web/20151001184927/http://www.slate.com/blogs/xx_factor/2013/10/18/millennials_on_social_media_young_people_are_incredibly_savvy_about_internet.html (citing a survey that shows Millennials value privacy more than ever on social http networks).

7. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 127–32 (2006); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 47-52 (2011); Benjamin Wittes & Wells C. Bennett, *Databuse and a Trusteeship Model of Consumer Protection in the Big Data Era*, GOVERNANCE STUDIES AT BROOKINGS, June 2014; Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic*, BROOKINGS INST. (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes; COHEN, *supra* note 1, at 21–23, 167–69.

8. Daniel J. Solove, *Information-Age Privacy Concerns Are More Kafkaesque than Orwellian*, CHRON. OF HIGHER EDUC. (Dec. 10, 2004), http://www.chroniclecareers.com/article/Information-Age-Privacy/33608/.

9. "Personally identifiable information" (PII), is a type of information that can be used on its own or aggregated with other information to identify a person or to identify an individual in a certain context.

10. CHARLENE BROWNLEE & BLAZE D. WALESKI, PRIVACY LAW (2012).

11. Edward W. Felten, *Privacy and A/B Experiments*. 13 Colo. Tech. L.J. 193, 196–97 (2015)

consumers into divulging personal information in order to get a product they desire. Companies are also using techniques such as social listening[12] to analyze social media content in order to improve customer service, which if misused could lead a person to think she is being stalked.[13] The technologies used in behavioral marketing algorithms also raise information privacy concerns, but because they run in the background of a personal search, the technologies and the information that they capture are generally invisible to most consumers.[14] In the course of most online searching for products or services, companies monitor a consumer's search terms, information about user interests and tastes, the stories they read, and the websites that they visit. Search terms entered into a search engine reveal PII that many individuals might prefer to be kept confidential such as medical history, religious or political affiliation, sexual orientation, and investment information. As the Internet has expanded, so has the behavioral marketing industry.[15] Businesses view the incentives to monitor online search behavior as additions to their product and corporate bottom lines, but business monitoring produces significant privacy problems and substantial risks to Internet users.[16] Industry practices, in the absence of strong privacy

(discussing ethical consent protocols missing from Facebook's contagion experiment); James Grimmelmann, *The Law and Ethics of Experiments on Social Media Users*. 13 Colo. Tech. L.J. 219, 221–25 (2015) (reviewing the Facebook contagion and OkCupid research projects and the ethical implications of each); Michelle N. Meyer, *Two Cheers for Corporate Experimentation: The A/B Illusion and the Virtues of Data-Driven Innovation.* 13 Colo. Tech. L.J. 273, 298–309 (2015) (discussing consent into human subject research such as the Facebook contagion project).

12. Social listening is the process of monitoring digital media channels such as Twitter or Facebook to key in on what is being said about a company to allow that business to devise a business strategy that might influence online consumers and entice those consumers into buying that business's goods or services. Daniel Newman, *Social Listening Enables Social Business*, FORBES (Aug. 26, 2014, 09:55 AM), http://www.forbes.com/sites/danielnewman/2014/08/26/social-listening-enables-social-business/#2715e4857a0b7b79ae975818 (describing how the original hashtag has evolved into a tool for brand marketers to use to find out what prospects, customers, and competitors are saying about products).

13. Omer Tene & Jules Polonetsky, A *Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 63 (2015).

14. Erica M. Scott, Comment, *Protecting Consumer Data While Allowing the Web to Develop Self-Sustaining Architecture: Is a Trans-Atlantic Browser-Based Opt-In for Behavioral Tracking the Right Solution?*, 26 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 285 (2013); Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL STREET J. (July 30, 2010), http://www.wsj.com/articles/SB10001424052748703940904575395073512989404; James Ball, Julian Borger & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'* GUARDIAN (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Spencer Ackerman & Glenn Greenwald, *How the NSA Is Still Harvesting Your Online Data*, GUARDIAN (June 27, 2013), http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

15. Mike Jaconi, *The 'On-Demand Economy' Is Revolutionizing Consumer Behavior — Here's How*, BUS. INSIDER (July 13, 2014, 4:52 PM), http://www.businessinsider.com/the-on-demand-economy-2014-7#ixzz3VhkibC3o.

16. Cost is a primary incentive. *See generally* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV.

principles, also prevent users from exercising any meaningful control over personal data that is obtained for these marketing purposes.[17]

Almost all information can be traced back to an individual in a variety of ways. Beyond social media sites, students, faculty, and staff using any institution's server systems to post a news piece, blog post, article, or even a short book review about a research resource that the library holds, are immediately identified with that institution by means of personal dataveillance record integration techniques, and the person's footprint automatically increases.[18] The same is true for recent graduates and the alumni of an institution. With each email, blog post, or Tweet to people the graduate has friended, these publicly discoverable footprints will greatly impact both the individual creating the post and the institution.[19] Posts on social media can lead to great reputational harm for that institution if those involved in creating and promulgating the postings are not following some type of social media policy or protocols;[20] a topic which is outside the scope of this article.

Commented [B4]: In response to the footnote comment, I added this phrase from the Clark article.

Although many legal and non-legal mechanisms could be put in place to protect both individuals and business entities, the law has been too slow to catch up with the plethora of issues surrounding the social media scene. The train has simply already left the station.[21] Proposals such as implementing privacy rating schemes, proposals to allow users to delete information that they intended to keep private, and proposals to evaluate impacts of disclosures are being promoted in a variety of privacy forums. Other unique proposals for privacy frameworks in social networking settings include adding privacy-aware ratings and feedback systems or an economic model to explain observed under-supply and under-promotion of privacy as a rational choice by social media site providers.[22] This proposal to better educate and enlighten students about the

849, 860–63 (2014) (discussing the value companies place on a user's data and information use).

17. *The Reform of the EU Data Protection Framework - Building Trust in a Digital and Global World: Before the Committee of the European Parliament on Civil Liberties, Justice, and Home Affairs, European Parliament Room* (Statement of Marc Rotenberg, President, Electronic Privacy Information Center (EPIC)) (2012), https://epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf.

18. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988).

19. Agnieszka McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 889–90 (2013).

20. Jennifer Howard, *Social-Media Skirmishes: More Colleges Are Deciding How—And Whether—To Regulate Faculty Speech*, CHRON. HIGHER ED. (Mar. 9, 2015), http://chronicle.com/article/Social-media-skirmishes-More/228147; *see also* DAVID A. POTTS, CYBERLIBERL: INFORMATION WARFARE IN THE 21ST CENTURY, 139–41 (2011); *cf.* COHEN, *supra* note 1, at 264–65 (making a nuanced argument for policy-making decisions).

21. *See How to Avoid the Data Breach*, NAT'L L.J. (2014) (devoting an entire issue to data breaches and related topics).

22. *See* Esma Aïmeur et al., *Towards a Privacy-Enhanced Social Networking Site*, *in* 5 INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY, AND SECURITY 172 (2010); Cliff Lampe, *The Role of Reputation Systems in Managing Online Communities*, *in* THE REPUTATION SOCIETY: HOW ONLINE OPINIONS ARE RESHAPING THE OFFLINE WORLD 77 (Hassam Masum et al. eds., 2011); Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On The Market For Data Protection In Social Networks*, *in* ECONOMICS OF INFORMATION SECURITY AND PRIVACY 121

potential harms their unintended disclosures might create for them in the future is meant to ensure that students of all age groups put their best foot forward in the digital world. This proposal also leaves room for creating curricular devices, programs, and other mechanisms to educate people about collection of PII that is not yet implemented in new software, devices, or Internet advances.

Schools should present basic information about, train, discuss, practice, and reinforce social media skill sets from a very early age. Elementary education is the best place to start this process in order to ensure that certain simple, best practice steps are followed, reflected on, and practiced. These can include discussing definitions of concepts such as privacy, digital footprints, and databases in the early grades. In later elementary school grades, concepts and ideas about how the misuse of information can harm the unknowing student can be reinforced. Additionally, best practices can be reinforced in high school through discussion and hands-on exercises that illustrate how harms to reputations can occur. A finer parsing of concepts and ideas surrounding privacy should be practiced through a series of well-crafted exercises for new college students. These exercises are important to ensure that students who will enter the work force are skilled in avoiding information improprieties on social media sites. They will also avoid harming their young reputations and those of the businesses they will eventually join.

Discussing hacking, privacy policies on social media sites, reputational harms, and ways of avoiding putting too much information out to the world might better cement students' understanding of informational privacy concerns that could come back to haunt them in the future. Just as many high schools require a driver's education course in order to ensure that students released from their programs are safe on the roads, educational institutions are in the best position to ensure that students avoid as much harm to their reputations as they can or know how to control the information they disclose about themselves.

In universities, adult users should further practice ways that they might eliminate Internet information that could be harmful to their reputation. They can also be taught ways to ensure that harmful information is buried deep in the results of a search engine to which an employer or other prying eyes might gain access. A comprehensive programmatic curriculum surrounding this topic should be created. Such a program and process ensure that by the time students reach the doors of any law school or other professional school, they are aware of the ramifications about how their digital footprint adds to their reputational legacy. Additionally, this curricular outline ensures that they have been thoroughly counselled and constantly reminded about the best ways of continuing to protect their reputations.

The job of educators is taking students as they are and educating them to be knowledgeable, ethical, good citizens. Students should be advised early and often about steps to take to keep their reputations secure and as pristine as possible. Information best practices and policies can be crafted for any setting.

(Tyler Moore et al., 2010).

Elementary schools, high schools, universities, and graduate schools, such as law schools, should devise a comprehensive curriculum and series of policies, training modules, and discussion group guidelines to assist students in ascertaining when they are on track and when they have gone astray in keeping their personal information secure.[23]

After the introduction to the basic ideas behind this proposal, Part II explores the legal scheme currently surrounding social networking. Part III discusses the history of reputational injuries, how an individual acquires a social identity, what potential reputational harms lie waiting for individuals, and how social media users can unwittingly impact their social and professional identity in terms of databuse[24] and the information stores that are collected about them. Part IV explores some of the remedies available to users who are harmed by social media intrusions into their privacy. Part V explores ways that institutions can protect students by informing them about privacy intrusions and by teaching them about the professional implications through a series of best-practice techniques.

II. A BRIEF HISTORY OF PERTINENT ONLINE PRIVACY AND DATA PROTECTION LEGISLATION AS IT RELATES TO SOCIAL MEDIA

Many pieces of pertinent federal legislation relating to social media and online data privacy issues have been introduced into Congress, but few have passed.[25] The measures that have passed tend to be business-friendly statutes that protect information privacy generally, but do not greatly impact business practices. At present, the legal framework of online privacy statutes directly affecting social media sites is primarily based on the two federal laws explained below; the Electronic Communications Privacy Act (ECPA) and the Children's Online Privacy Protection Act (COPPA).[26]

---

23. That process is now just beginning. *See* COMMON SENSE MEDIA, https://www.commonsensemedia.org/educators (last visited Mar. 12, 2015); *see also Digital Compliance and Student Privacy: A Roadmap for Schools*, IKEEPSAFE, http://www.ikeepsafe.org /educators_old/digital-compliance-and-student-privacy-a-roadmap-for-schools/ (last visited Mar. 1, 2015); Goldie Blumenstyk & Jeffrey R. Young, *3 Big Issues We Heard About at SXSWedu*, CHRON. OF HIGHER ED. (Mar. 13, 2015), http://chronicle.com/blogs/wiredcampus/3-big-issues-we-heard-about-at-sxswedu/56063?cid=at&utm_source=at&utm_medium=en for the "Statement of Data Principles" crafted during the South by Southwest Education Conference in March 2013 espousing commitments to "safeguard and only permit minimum and necessary access to student data."

24. Originally coined by Benjamin Wittes, the term refers to data stores of personal information about a person that can potentially lead to abusive practices and potential reputation harmSupra note 7.

25. *See* Fred H. Cate, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, FIRST REPORTS (2003) (discussing the legislation that has been introduced to control the type of information that could be used to cause harm to an individual).

26. 18 U.S.C. § 2510–22 (2012); 15 U.S.C. 6501–06(2012); *see also* Children's Online

A general schema was proposed as early as the 1970s to protect the privacy and integrity of various types of personal information.[27] In 1973, the Department of Health, Education and Welfare Advisory Committee drafted the Code of Fair Information Practices (FIPs).[28] The code was widely adopted internationally. After the Organization for Economic Cooperation and Development revised the general principles from the original HEW code into a broader OECD document, those principles became influential internationally. The FIPs have played a significant role in framing privacy laws in the United States, and led to the passage of the Privacy Act of 1974.[29] Statutory enactments to protect personally identifiable data were proposed by citizen groups and legislators after the FIPs were recognized internationally, however none have passed. Although no regulatory body is formally charged with monitoring online privacy violations, many federal statutes and regulations have been enacted since the 1970s that include provisions protecting information privacy and personal information privacy such as the protection of financial information, protection of drivers' records, and video privacy protection. Most of this patchwork of legislation occurred because of egregious privacy invasions. The driver's privacy legislation occurred after an increase in opponents of abortion rights using public driving license databases to track down and harass abortion providers and patients and the video privacy protections fell in place after Robert Bork's video rental history was published during his Supreme Court nomination hearing.[30] None of these legislative schemes are comprehensive, and regulation and oversight of these enactments is charged to the Consumer Financial Protection Bureau state agencies, and federal law enforcement agencies.[31]

Commented [B5]: Per the first editor review I originally had this as text and they suggested that I make it a footnote. I placed it back here per the footnote editors comment and added a footnote source. Please advise if this needs another change.

In recent years, consumers have unsuccessfully advocated for legislation giving the Federal Trade Commission (FTC) the power to regulate online privacy and to create "do not track"[32] mechanisms.[33] The FTC also recently

---

Privacy Protection Rule, 16 C.F.R. § 312.1–.13 (2015).

27. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMMITTEE, AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND RIGHTS OF CITIZENS (1973).

28. *Id.*

29. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44 (2001).

30. Paul M. Schwartz, *Preemption and Privacy*, YALE L. J. 923, 932–35 (2009). .

31. ROTENBERG, *supra* note 29, at 26; Bryan Knedler & William Welkowitz, *States Continue to Protect Workers' Social Media Privacy in 2014*, BNA SOC. MEDIA L. & POL'Y REP. (Feb. 10, 2015), http://www.bna.com/states-continue-protect-n17179922967/ (highlighting the fact that many bills have been proposed in the years since the ECPA and COPPA were originally passed to deal with information privacy gaps. Many states have taken matters into their own hands by enacting a comprehensive set of social media privacy laws. They include: Arkansas, Colorado, California, Delaware, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont and Washington, with more than 30 other states working on similar bills).

32. "Do not track" is a set of online tools that consumers can use to signal that they do not want to be tracked. Fred B. Campbell, Jr., *The Slow Death of 'Do Not Track'*, N.Y. TIMES (Dec. 26, 2014), http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html?_r=0.

33. Angelica Nizio, Note, *Taking Matters into Its Own Hands: Why Congress Should Pass*

reported on security issues arising out of notice and choice issues tied to the Internet of things (IoT).[34] The Federal Trade Commission Act permits the FTC to identify unfair consumer practices that are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves, but this statute has not been construed to generally permit the FTC to regulate online privacy.[35] Many states, with California at the forefront, are reluctant to wait for the federal government to act and have passed their own privacy legislation.[36] Those laws mandate that personal information such as Social Security numbers, driver's license numbers, credit card numbers and passwords be protected from unauthorized access, destruction, use, modification, or disclosure.[37] California's recent attempt to protect minors on the Internet is the passage of SB 568, entitled "Privacy Rights for California Minors in the Digital World."[38] It contains sections on advertising and marketing certain types of products to teenagers and an eraser law which will allow minors to delete their online presence.[39]

Currently, no comprehensive legislative privacy scheme governs data privacy and social media use and abuse in the United States. Citizens may witness a new era of privacy enforcement and practice in the next few years, however. The Obama Administration proposed a Consumer Privacy Bill Of Rights in 2012 and elaborated on it in the 2015 State of the Union Address.[40] Additional measures highlighted in remarks to the Federal Trade Commission just before the President's January 2015 address included a presidential legislative proposal intended to assist Americans whose personal and financial information has been compromised in a data breach.[41] The proposed guidelines and potential legislative enactments could help to limit the impact on a citizen's

Legislation to Allow the FTC to Regulate Consumer Online Privacy with a "Do Not Track" Mechanism, 14 U. ILL. J.L. TECH. & POL'Y 283, 289–90 (2014).

34. FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https:// www.ftc.gov/system/files/documents/reports/federal-trade-comrnission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

35. 15 U.S.C. § 45(n) (2012).

36. *Map: A Wave of State Student-Data-Privacy Legislation*, EDUCATION WEEK, (May 10, 2015), http://www.edweek.org/ew/section/multimedia/student-data-privacy-map.html; *see also State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES, (February 24, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx; Spencer Kuvin & Chelsea Silvia, *Social Media in the Sunshine: Discovery and Ethics of Social Media - Florida's Right to Privacy Should Change the Analysis*, 25 ST. THOMAS L. REV. 335, 342 (2013).

37. Bruce Radke & Michael Waters, *Selected State Laws Governing the Safeguarding and Disposing of Personal Information*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 487 (2015).

38. *See* 2013 Cal. Legis. Serv. Ch. 336 (S.B. 568) (West).

39. Stephen J. Astringer, Note, *The Endless Bummer: California's Latest Attempt to Protect Children Online Is Far Out(Side) Effective*, 29 NOTRE DAME J.L. ETHICS & PUB. POL'Y 271, 272–73 (2015).

40. *See* Barack Obama, *Remarks by the President in the State of the Union Address*, THE WHITE HOUSE (Jan. 20, 2015), https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015.

41. *See* Barack Obama, *Remarks by the President at the Federal Trade Commission*, THE WHITE HOUSE (Jan. 12, 2015), https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

digital footprint if the legislation that follows the President's proposal stays true to the ideal of protecting online users' privacy expectations.[42] Additionally, a Student Digital Privacy Act[43] was proposed to ensure that data collected about students is used only for educational purposes and to prevent the sale of student data to third parties. If passed, a companion Act, the Student Privacy Protection Act[44] will amend the Family Education Rights and Privacy Act to prevent companies from using data collected about students in schools .[45]

Commented [B6]: Changed based on footnote editors comment.

A. Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA)

The Electronic Communications Privacy Act of 1994 (ECPA) amended the 1968 federal wiretap statute to cover electronic communications.[46] The ECPA and the Stored Communications Act of 1995 (SCA) were written when older technologies such as floppy disks and cassette tapes were more prevalent and were used to store letters, messages, and transcripts of letters. The ECPA was passed to address the privacy of electronic mail at an early stage of the penetration of the Internet into mainstream commerce and everyday life.[47]

The SCA amended the ECPA in order to restrict access to stored communications and transaction records that a business or governmental agency might request.[48] The SCA is known as Title II of the ECPA, and the intent of the Act appears to be to protect email and similar electronic communications such as data transfers between businesses and customers.[49] It expressly does not apply to an electronic communication that is readily accessible to the general public, making it inadequate to control access to information provided on social media sites.[50] Taken together, the ability of either statute to resolve web-based or social media abuse problems is questionable even if both statutes were amended since the statutes deal primarily with the way a message, email, or other communication is intercepted or stored and by whom; not the way that individual privacy is protected.

In the past decade, legislation has been introduced to provide greater transparency and more consumer control over personal information collected during a consumer's online transaction session, but most legislation has not

42. As of January 2016, the Senate and House Bills introduced, S. 547 114th Congress (2015-2016) and H.R. 1053 114th Congress (2015-2016), have not been reported out of committee.
43. As of February 2016, the Senate and House Bills introduced, S.1788 114th Congress (2015-16) and H.R. 2092 114th Congress (2015-2016), have been referred to Senate and House Subcommittees.
44. As of January 2016, the Senate and House Bills introduced, S. 1341 114th Congress (2015-2016) and H.R. 3157 114th Congress (2015-2016), have not been reported out of committee.
45. *Id.*
46. *See* 18 U.S.C. § 2510–22 (2012).
47. ROBERT GELLMAN & PAM DIXON, ONLINE PRIVACY 21 (2011).
48. *See* 18 U.S.C. § 2701–12 (2012).
49. GELLMAN & DIXON, *supra* note 47.
50. 18 U.S.C. § 2511(g)(i) (2012).

successfully made its way out of the committee process largely due to concerns about the impacts a regulatory scheme could have on businesses.[51] Agencies such as the Department of Justice, the Internal Revenue Service, and the Department of Health and Human Services have wrestled for authority over online privacy and confidentiality of PII, at least for the information these agencies collect.[52] The Federal Trade Commission, in particular, is authorized to investigate complaints about business practices impacting privacy and PII and has published guidelines to support industry self-regulation.[53] Only in the past five to eight years have consumers begun to appreciate the extent to which a person's personal information is tracked and used by governmental agencies.[54]

Any new legislative or regulatory schemes face attacks from business stakeholders and conflicts about the types of information that should be protected.[55] Businesses dealing with financial transactions or health information have complied with FTC Privacy rules requiring them to supply notice of how that business will use, share and protect personal information. Nearly every person in the United States now receives privacy notice updates in the mail at least annually reminding them of the practices the businesses use that she deals with for financial and health services. However, legislative mandates to ensure that a person who uses any business site or social media site for purposes other than health and finance is made more aware of how her information disclosures and releases of personal information might be used, shared with other businesses and protected are still only a blip on the horizon.

Amendments to the ECPA have been repeatedly introduced into Congress in nearly every session, however none have been successful.[56] Given the recent push by the Obama Administration to pass a Consumer Privacy Bill of Rights, the timing for an extensive set of changes to ECPA is better than it has ever been for privacy legislation dealing with social media and information privacy to pass within the next year or two.[57]

---

51. *See e.g.*, THE WHITE HOUSE, CONSUMER DATA IN A NETWORKING WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

52. *Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information Is Systematic and Routine*, PRIVACILLA (Mar. 2001), http://www.privacilla.org/releases/Government_Data_Merger.html.

53. GELLMAN & DIXON, *supra* note 47, at 121, 123.

54. *Id.* at 124–26.

55. *See, e.g.*, S. 1158, 114th Cong. (Consumer Privacy Protection Act) (2015-2016); H.R. 2977, 114th Cong. (2015-2016). Both would establish a federal security breach notification law and provide protection for many types of data including social security numbers, financial account information, online usernames and passwords, unique biometric data (including fingerprints), information about a person's physical and mental health, information about a person's geo-location, and access to private digital photographs and videos. The bills would pre-empt weaker state laws while leaving stronger state privacy laws in place. Both are now stalled in committee.

56. *See generally* GELLMAN & DIXON, *supra* note 47, at 21–22.

57. Sanford Reback, *Big Data, Big Policy Changes?: The Obama Administration's Reports May Ultimately Lead to a Major Reform of How the U.S. Protects Privacy*, BLOOMBERG GOVERNMENT: BGOV ANALYSIS (June 25, 2014), http://about.bgov.com/bgov200/content/uploads

B. Children's Online Privacy Protection Act (COPPA)

By the 1990s, the Internet had become a major source for marketing, selling, and distributing products and services. Families began purchasing games and other forms of online entertainment for their children. By 1998, almost 26% of households in the United States had access to the Internet.[58] Families began to understand the potential for marketing and privacy abuses attached to marketers who collected personal information from children when they registered for chat rooms and discussion boards.

In April 2000, the Children's Online Privacy Protection Act (COPPA) was enacted with the intent of protecting the privacy of children under the age of thirteen.[59] Parental consent is required for the collection or use of any personal information about a young child by a commercial website or online services that are directed at children.[60] As a part of its oversight role, the FTC published a series of guidelines and frequently asked questions aimed at educating businesses and website owners about the collection and use of children's information online privacy. These are included in the FTC's COPPA regulations and are generally available on the FTC website.[61]

Commented [B7]: Added this word and added a pinpoint to the footnote per footnote editors comment.

On July 1, 2013, The FTC suggested amendments to revise COPPA to expand the definition of what it means to collect data from children.[62] The latest revisions address changes in the way children access the Internet in general and social media in particular. It has expanded the definition of what is personal information to now include "persistent identifiers" or cookies that can be used to track a child's online activity. The changes also recognize the frequency with which young children access the Internet through mobile devices such as smart phones and tablets. The FTC also placed tighter controls on geolocation information, photos, videos, and audio recordings.[63]

All of these acts taken as a whole protect consumer's interests in their Internet and digital privacy in a limited way. The issues surrounding information privacy, database relationships, big data[64] compilations of consumer

Commented [B8]: Added a definition and source as suggested.

/sites/2/2014/06/GdnSTovayqJbENWOZrOjhg1.pdf.

58. JENNIFER CHESSMAN DAY ET AL., U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003: SPECIAL STUDIES 1 (2005), https://www.census.gov/prod /2005pubs/p23-208.pdf.

59. 15 U.S.C. §§ 6501–06 (2012).

60. *Complying with COPPA: Frequently Asked Questions*, U.S. FED. TRADE COMMISSION, (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

61. *Id.*

62. *Revised Children's Online Privacy Protection Rule Goes into Effect Today*, FED. TRADE COMMISSION (July 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect.

63. *Id.*; *see also* Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) (recognizing that the state constitution protects an individual's reasonable expectation of privacy in cellular phone call location data).

64. "Big data" can be defined as extremely large data sets that may be analyzed by computers to reveal patterns, trends, and associations, especially relating to human behavior and interactions;

information, and social media protections remain largely unanswered in any legislative scheme presented separately or as a whole in the enactments presented above.[65] Even if a person wants to protect their identity and privacy completely, she cannot. A person cannot wipe his digital footprint in order to preserve his digital reputation.[66] When a vast reputational harm occurs, the consequences can affect a person's life for years to come. How can legal problem solvers repair this reputational harm?

III. PROTECTING A PERSON'S DIGITAL REPUTATION IN AN UNREGULATED WORLD

Reputation defines people. Most people value the ability to control the information that goes into forming another person's opinion about her as a colleague, employer, student, or in some other capacity.[67] Distorted or incorrect information about a person that makes its way onto the Internet directly affects her in a variety of ways.[68] The distorted information may cause an unwanted effect on that person's behavior, making her feel as if she is under attack and thereby causing her to pull back from normal activities, shy away from cameras, shun others, and generally modify her normal modes of expression and behavior.[69] She may also try to become anonymous on the Internet, but will likely fail.[70] Additionally, a person who is damaged by distorted information

The Big Data Conundrum: How to Define it?, MIT TECH. REV. (October 3, 2013), https://www.technologyreview.com/s/519851/the-big-data-conundrum-how-to-define-it/.

65. For a discussion of "big data" collection practices *see* Peter DiCola & Marcelo Halpren, *Legal Problems in Data Management: IT & Privacy at the Forefront: "Big Data": Ownership, Copyright, and Protection*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 565 (2015); Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81 (2013); Debbie Feinstein, *The Not-So-Big News About Big Data*, FED. TRADE COMMISSION (June 16, 2015 11:30AM), https://www.ftc.gov/news-events/blogs/competition-matters/2015/06/not-so-big-news-about-big-data.

66. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (proposing taking control over personal information nearly 50 years ago); Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 66, 109–10 (suggesting the concept of "information bankruptcy"); Graeme Wood, *Scrubbed*, N.Y. MAG. (June 16, 2013), http://nymag.com/news/features/online-reputation-management-2013-6/ (discussing the new nearly-$5-billion-a-year business of online reputation management).

67. *See* DAVID ROLPH, REPUTATION, CELEBRITY AND DEFAMATION LAW 6–11 (2008); Michael S. Wagner, *The Convergence of Human and Digital Memory: A Call for Consumer Action*, 5 WAKE FOREST J.L. & POL'Y 443, 463 (2015) (calling for solutions to consumer data exposure and ultimate research and experimentation of that data by businesses).

68. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 160 (2008) (describing the way that "distorted" information that is false and misleading affects other peoples' perception and judgment of the person being pictured); ROLPH, *supra* note 67, at 37 (describing the concept of reputation as being inherently relational); *see* Solove, *The Clementi Suicide*, *supra* note 1.

69. Cass R. Sunstein, *Believing False Rumors*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 91, 102 (Saul Levmore & Martha C. Nussbaum, eds., 2010).

70. Alex Kozinski, *Essay: The Two Faces of Anonymity*, 43 CAP. U. L. REV. 1 (2015).

may become unable to adequately prepare for the world of work,[71] shun intimacy,[72] feel out of control,[73] or appear to be unengaged.[74]

Privacy and reputation are intricately linked.[75] The protection of information privacy matters to many people. Information about a person is an intrinsic part of her self-understanding. Autonomous individuals want control over a type of self-presentation. That self-presentation includes taking control of how to present or stage herself, to whom she wants to appear and in which contexts. That control extends to how a person wants to see herself and how she wants to be seen.[76]

Controlling all of the information about a person has become more difficult as the Internet expands the number of people who will most likely view it and who could mislead others.[77] Unlike paper-based personal information, digital formats permit data to be haphazardly copied, saved, linked, shared, modified, and remixed. Social media sites, unlike paper newsletters or film in a cassette tape transcend the physical and material limitations of images and sounds, texts and film.[78] The context of words and actions shifts in a digital world, making those images and words perpetually visible to a wide audience and therefore making it possible to shame someone or bring about a scandal.[79] Virtual deletion

Commented [B9]: Added a pinpoint cite based on footnote editors comment.

71. MATTHEW CRAWFORD, THE WORLD BEYOND YOUR HEAD: ON BECOMING AN INDIVIDUAL IN AN AGE OF DISTRACTION (2015) (examining how people come to flee from the world or interact with it because of the forces that claim our mental space, leave us distracted and unable to direct our attention to important issues, or permit us to better fit in with the world by acquiring context and tradition).

72. JOSE MARICHAL, FACEBOOK DEMOCRACY: THE ARCHITECTURE OF DISCLOSURE AND THE THREAT TO PUBLIC LIFE 132 (2012); *see also* Karen E.C. Levy, *Intimate Surveillance*. 51 IDAHO L. REV. 679 (2015).

73. *Id*.

74. *Id*.

75. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007); ELIZABETH PRICE FOLEY, LIBERTY FOR ALL: RECLAIMING INDIVIDUAL PRIVACY IN A NEW ERA OF PUBLIC MORALITY (2006); SOLOVE, THE DIGITAL PERSON, *supra* note 7; Michael Zimmer & Anthony Hoffman, *Privacy, Context, and Oversharing: Reputational Challenges in a Web 2.0 World*, *in* THE REPUTATION SOCIETY 175 (Hassan Masum & Mark Tovey eds., 2011); Sunstein, *supra*, note 69.

76. ROSSLER, *supra* note 4.

77. JULIAN PETLEY, MEDIA AND PUBLIC SHAMING: DRAWING THE BOUNDARIES OF DISCLOSURE 77, 97 (2013).

78. Zimmer & Hoffman, *supra* note 75, 176–77, 181; Woodrow Hartzog, *Social Data*, 74 OHIO ST. L. J. 995, 998 (2013); Richard Warner & Robert H. Sloan, *Self, Privacy, and Power: Is It All Over?*, 17 TUL. J. TECH. & INTELL. PROP. 61, 67 (discussing the ideal of creating a multi-faceted self in the online world).

79. Hanne Detel, *Disclosure and Public Shaming in the Age of New Visibility*, *in* MEDIA AND PUBLIC SHAMING: DRAWING THE BOUNDARIES OF DISCLOSURE 77, 79 (Julian Petley ed., 2013); *see* Allison C. Shields, *Managing Your Reputation in an Online World*, LAW PRACTICE MAGAZINE, (2014), http://www.americanbar.org/publications/law_practice_magazine/2014/july-august /simple-steps.html (noting that lawyers need to be aware that other's online activities may affect their reputations); *see also* Neil Richards, *The Electronic Panopticon*, CHRON. OF HIGHER ED., (Mar. 16, 2015), http://chronicle.com/article/The-Electronic-Panopticon/228419/ (noting that sensitive data about our mental activities need special protections); Kathleen Brennan Hicks, Note,

of information a person releases and later regrets or that might harm her is not a possibility in many or most cases because the websites hosting a person's social portrayal of her secrets and personal images are controlled by a license.[80]

Commented [B10]: Added the phrase directly used in the source per footnote editors comment.

Potential harms to a person include disclosure of information that a person wishes to keep secret such as sexual orientation or disclosure of a chronic disease. Additionally, pictures that are posted to a social media site in jest such as those portraying a person who is obviously drunk, especially if multiple photos of a drunk person are posted at various points in time, could impact their ability to land the job of their dreams. Other potential harms include cyberstalking, financial loss, loss of friends, loss of business partners, loss of a potential spouse, and even the trust of a parent.

Although a breach of privacy may not matter to a teenager, intrusions or distortions of personal information that reveal secrets will matter later in life. If a person is interested in protecting small pieces of personal information that could affect her future reputation if those pieces are compiled with other information about her, then starting at a very early age, a person should have ways to control information privacy invasions. Harms that could accrue from those invasions should be explained early on to a young person who is most at risk. If the information cannot be regulated or prohibited, other ways of protecting a person's personal information, such as permitting them to remove harmful personal facts, information about juvenile offenses or other criminal information, or to remove photographs and the harmful iterations of a photo that have occurred after it was posted, must become more readily available.[81]

While the harm that accrues from a single transaction, post, or tweet made online is likely negligible, consider the cradle-to-grave scenario that follows the average person's life span.[82] When one regrettable transaction becomes ten, twenty, or hundreds, and a person is not tracking her privacy or security settings, actively taking steps to reduce her online footprint, or following best practices

---

The Right To Say, "I Didn't Write That": Creating a Cause of Action to Combat False Attribution of Authorship on the Internet, 22 J. INTELL. PROP. L. 375 (2015).

80. Jeffery Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, *in* CONSTITUTION 3.0 : FREEDOM AND TECHNOLOGICAL CHANGE 69, 78 (Jeffrey Rosen & Benjamin Wittes eds., 2011); Ryan Calo, *Quantifying Harm Structure: Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361–63 (2014) (listing current case law in the area of what counts as personal information).

81. Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007); DAVID H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY 273 (2010); DANIEL J. SOLVE, UNDERSTANDING PRIVACY 160 (2008) (describing the way that "distorted" information that is false and misleading affects other peoples' perception and judgement of the person being pictured); John B. Thompson, *The New Visibility*, 22 THEORY, CULTURE, AND SOCIETY 31 (2005); Michael L. Rustad and Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*. 28 HARV. J.L. & TECH. 349, 352, 379–80 (2015).

82. *See* Lilian Edwards & Edina Harbinja, *Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World*, 32 CARDOZO ARTS & ENT. L.J. 83 (2013) (discussing the protection of digital "assets" after death and the difficulties involved).

in an online environment, her reputation could be compromised.[83] Consumer harm and impact on businesses are often raised as key issues in in the United States for not passing comprehensive legislation controlling privacy over personal information. Reputational harm is more relevant to individuals, and potentially damaging data stores can affect reputation now and far into the future.[84]

These data stores of personal information about a person that can potentially lead to abusive practices and potential reputational harm can be called *databuse*.[85] After a birth record is produced, a digital "dossier" begins to be collected about a person's health, school history, online preferences, and much more; ending with a county death record.[86] Add to these permanent records the information that children who start to use the web at an early age begin to produce, and the potential privacy harm begins to increase exponentially.[87]

Once these existing data stores of personal information are expanded by future technologies unimagined by any person, the harm to reputation may become difficult to contain.[88] For example, a mobile phone's geolocation capability permits personalized location information to be delivered to a business wanting to provide a person with the latest services and goods in the store she is currently visiting.[89] This technology and the smartphone itself were not anticipated twenty years ago. If even a few of the new disruptive technologies anticipated today, such as totally automatic cars or refrigerators designed to remind you that you need milk are networked together any time soon, then much more information could be unwittingly added to these dossiers of personal information.[90] Consider for example the self-driving automobile that

83. *See* Robin Feldman, *Coming to the Community*, *in* IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY, 84 (Austin Sarat, et al. eds., 2012) (providing an overview of the topic and a discussion about reconceptualizing the entire social media and public/private and property/tort law issues surrounding most of these potential harms); *see also* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 270–73 (2014) (setting out a series of privacy survey indicators of online users lack of awareness).

84. *See* for example ROLPH, *supra* note 67, at 37.

85. Wittes, supra note 7.

86. SOLOVE, THE DIGITAL PERSON, *supra* note 7, at 127–39.

87. *See* Feldman's notion of creating a right of "identity cohesion" which differs from privacy rights in that they are rights 'personal' to a human being, but not rights to monetize or trade away. Feldman, *supra* note 82.

88. *See* Danielle Young, Comment, *Now You See It, Now You Don't...Or Do You?: Snapchat's Deceptive Promotion Of Vanishing Messages Violates Federal Trade Commission Regulations*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 827, 828 (2014) (describing how Snapchat's vanishing messages features contribute to inadvertent reputation damage).

89. David Shepardson, *Report: Cars Are Vulnerable to Wireless Hacking*, DETROIT NEWS (Feb. 8, 2015 10:18 p.m. EST), http://www.detroitnews.com/story/business/autos/2015/02/08 /report-cars-vulnerable-wireless-hacking/23094215/.

90. Paul Nunes & Larry Downes, *The Five Most Disruptive Innovations at CES 2015*, FORBES/TECH (Jan. 09, 2015, 1:27 PM), http://www.forbes.com/sites/bigbangdisruption/2015/01 /09/the-five-most-disruptive-innovations-at-ces-2015/.

could, at the same time it is making its way down the road, send images of what the driver is watching or doing.[91] Consider as well the possibility of NEST[92] household products, that talk to each other to keep a house warm or lights actively working in the house, which could relay personal facts about the state of disarray of a house or household. The Internet of Things[93] is also certain to contribute to the bloat of personal information that companies mine when a person uses a computer-based storage device ranging from a FitBit[94] to a refrigerator tied to Amazon as their source for restocking a staple food item.

Commented [B11]: Added a definition and source as suggested in the comment.

In *Divining a Digital Future*, Paul Dourish and Genevieve Bell talk about one of the first smart-location technologies called Active Badge, which was implemented in a variety of university and research settings between 1989 and 1992.[95] Active Badge was a tracking system that pinpointed its wearer's location and permitted the receptionist to forward phone calls.[96] It also raised an unanticipated firestorm of alarm over user's privacy concerns such as the way data about a person was logged, how management might ultimately misuse information about employee movements, concerns about a secret logging system running in the background unknown to most employees, and the lack of freedom in choosing to remain anonymous that employees had in choosing not to wear a badge at all on certain days. Conceptual models of the potential privacy invasions were lacking when Active Badge was introduced. Even today, conversations about privacy concerns that a new technology might generate often appear to take place as an aside in the business setting.[97] The complicated concerns about breach of trust, secrecy, risk, danger, lies, control, security, identity, morality, and power that a newer technology might unleash are often not even considered.[98] Reputation should be added to this list. Active Badge illustrated the fact that social, informational, and reputational practices all must be comprehended, discussed, and addressed as new technologies are released. These concerns must become an ingrained part of the testing phase of new

91. Orly Ravid, *Don't Sue Me, I Was Just Lawfully Texting & Drunk When My Autonomous Car Crashed into You*, 44 SW. L. REV. 175 (2014).

92. The NEST is a newer computer application that works with most computer operating systems to turn a phone into an on-off switch for a thermostat, NEST Cam or Dropcam. It permits a person to see live video previews of all home-mounted cameras on one computer screen, to allow a person to peek into any room, and notify the NEST that a person is home or away.

93. The Internet of Things is a network of physical objects or things that include software and sensors which connect to each other and allow those objects to collect and exchange data.

94. A FitBit is a wearable fitness device that can be strapped to an arm or wrist which sends personalized fitness information about the user to a remote database. Laura P. Paton, Sarah E. Wetmore, Clinton T. Magill, *How Wearable Fitness Devices Could Impact Personal Injury Litigation In South Carolina*, 27 S.C. LAW. 44 (2016).

95. PAUL DOURISH & GENEVIEVE BELL, DIVINING A DIGITAL FUTURE: MESS AND MYTHOLOGY IN UBIQUITOUS ECOMPUTING 137–39 (2011) [hereinafter DIVINING].

96. *Id.* at 137.

97. *Id.*

98. *Id.* at 139.

technologies so that they can be managed instead of handled through litigation or legislation after an information privacy breach occurs.[99]

Since an easy technological or legislative solution does not appear to be readily available, a person needs to ensure the security of her personal information through educated critical evaluation processes. When Tweeting, geolocation devices, and wearable technologies become the latest technologies that a person must have, she also needs to ask if the technology or system is secure from hacking, prying eyes, and the unintended release of personal information. Critical among the questions she must ask is whether or not her reputation will be damaged in some unexpected way and how she can explore her options before making that purchase or signing that licensing agreement.

Scholars in the area of reputational privacy disagree about the ways digital reputations should be protected.[100] Some argue that privacy-enhancing social norms will develop in order to protect users, while others indicate that the key is to create contextual information norms that can protect people and groups from harm.[101] One argues that an action for libel is sufficient, since being subject to an action for libel creates a chilling effect on conversations that may curb future false statements.[102] Another scholar suggests mandating that social networking sites adhere to a new regulatory regime that will provide specific privacy protections is needed in the areas of competition policy, privacy, and consumer protection.[103] A new regulatory regime could focus on prohibiting anticompetitive conduct among social networking sites.[104] Professor Tushnet suggests that constitutional first amendment protections for libel and slander on a social media site might be subject to different content-based and content-neutral rules applied to those causes of action when dealing with the press or in broadcasting since the dissemination mode casts a broader net.[105]

---

99. Biovanni Iachello and Jason Hong, END-USER PRIVACY IN HUMAN-COMPUTER INTERACTION, 100-–01 (2007).

100. *See* Feldman, *supra* note 82 (discussing the legal issues involved in promoting some type of legal privacy regime as opposed to reconceptualizing the entire social media public/private and property/tort law discussions surrounding most of these discussions); *see also* DENNIS D HIRSCH, *In Search of the Holy Grail: Achieving Global Privacy Rules through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029 (2013).

101. *Compare* Ruben Rodrigues, *Privacy in Social Networks: Norms, Markets, and Natural Monopoly*, THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 238 (Saul Levmore & Martha C. Nussbaum eds., 2010) [hereinafter THE OFFENSIVE INTERNET] *with* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2009).

102. *See* Sunstein, *supra* note 69, at 91.

103. Mark MacCarthy, *Is Internet Exceptionalism Dead?*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 221–22 (Bernin Szoka & Adam Marcus eds., 2006)

104. *Id* at 248. The competitive conduct here refers to the competition for users based on the social networking site's privacy policy. A social network monopoly can be created when users only use one social networking site. When that happens, users are at the mercy of that one social networking site's privacy policy.

105. Mark Tushnet, *Internet Exceptionalism: An Overview from General Constitutional Law*, 56 WM. & MARY L. REV. 1637, 1663–64 (2015).

Different strategies for dealing with information privacy and reputation can be implemented based on the effect on reputation at specific points in the information collection and aggregation process and will involve a combination of technology, policy, and the law.[106] The end result of these strategies may be greater monetary costs.[107] Even if social media sites' privacy settings or some new privacy protocols, policies, or legislation can assuage most privacy concerns by limiting corporate access to private personal information, consumers are still unlikely to truly understand their privacy options, potential tort remedies, and first amendment rights[108] The structures and systems noted in the next section exemplify some of the approaches legislators, companies, and authors have proposed which, for the most part, have not succeeded in informing a person about how to control the information she releases to social media or commercial websites about her.[109] An alternate proposal, noted below, may provide the best working solution, at least for the near future.

Commented [B12]: Added phrasing from the source to clarify.

IV. REMEDIES CURRENTLY IN PLACE AND NEWER PROPOSALS AIMED AT PROTECTING OUR DIGITAL FUTURES

Existing legal doctrines such as contract law, constitutional law, and the privacy torts in particular seek to protect reputation by providing remedies – almost exclusively financial. Yet injuries to reputation are not exclusive to a person's bottom line. In many ways, reputation is a quintessential public good incentivizing people to perform altruistic or other good acts to remain true to their pristine persona, and punishing them for a lack of cooperation or bad acts when undesirable reputational qualities arise. For that reason alone, a variety of remedies should be available.[110] Remedies are, for the most part, unavailable to persons who are injured by defamatory comments or by virtue of their own harmful behavior on social media sites and in other online venues. Defamation law as a remedy for privacy violations is inadequate to remedy social media

106. Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1737 (2008); David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 328 (2010).

107. PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION at 59 (2002); *see also* HIRSCH, *supra* note 100, at 1032.

108. A topic too broad to be explored here, but for an overview *see generally* THE OFFENSIVE INTERNET, *supra* note 100, and Daniel Solove's articles (cited throughout); *see also* Joel R. Reidenberg, et al. *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding* 30 BERKELEY TECH. L.J. 39, 41 (2015); Paul F. Kirgis, et al., *"Whimsy Little Contracts" With Unexpected Consequences: An Empirical Analysis Of Consumer Understanding Of Arbitration Agreement*, 75 MD. L. REV. 1 (2015) (explaining empirical data collected about consumer's understanding of arbitration contracts and their acceptance of them without understanding their procedural rights).

109. *See* BROWNLEE & WALESKI, *supra* note 10; GRETCHEN MCCORD, WHAT YOU NEED TO KNOW ABOUT PRIVACY LAW: A GUIDE FOR LIBRARIANS AND EDUCATORS (2013).

110. David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. CIV. RTS.-CIV. LIBERTY L. REV. 261, 262 (2010).

abuses. Because the concept of reputation remains relatively unexamined in defamation law, it is rarely, if ever, raised as a cause of action.[111] Courts and most privacy tort law scholars tend to make assumptions about the meaning of reputation and find that they are unable or unwilling to define it.[112]

Since the publication of the seminal Warren and Brandeis article, "The Right to Privacy,"[113] in 1890,[114] followed by the birth of Prosser's privacy torts in 1960,[115] a variety of legal systems, regulatory schemes, and other remedies have been proposed to protect both individual privacy and information privacy.[116] Since individual notions of privacy that are tied into notions of reputation are defined uniquely and differently by all of us, the courts have been reluctant to define and enforce most reputational privacy protections. Most claims of violation are raised either under a constitutional or a tort claim.[117] Few constitutional claims succeed.[118] Because tort law is a matter of state law, remedies differ. Without a showing of actual harm, emotional distress, mental anguish, or some similar complaint, most remedies remain unavailable to most plaintiffs.[119] Courts often deny recovery by placing a number of substantial barriers to recovery in the way. Plaintiffs are often forced to prove that the defendant intended to invade another's privacy, that the defendant's conduct was highly offensive to a reasonable person, or that the plaintiff's information was sufficiently private in order to recover.[120] These substantial barriers to legal remedies for privacy violations have been difficult to surmount for offline activities, and are harder to overcome for online activities."[121]

Commented [B13]: Added a pinpoint cite to clarify section of source used.

111. *See* ROLPH, *supra* note 67, at 3–6 (explaining the difficulty most authors, including Prosser and Keeton have had in defining 'reputation' to include in discussions of tort relief).

112. *Id.* at 3.

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

114. The article proposed the structure of a clearly articulated law, but set certain limitations on the form of the cause of action. The law could not prevent someone from disclosing information about someone if that person had already made the information public in some way. More protections accrued from this first articulation, including the modern articulations of "personally identifiable information" anonymity", and the Fair Information Practices Principles, *see* MCCORD, *supra* note 109, at 7–13.

115. RESTATEMENT (SECOND) OF TORTS RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D, 652E, 652C (1976).

116. For a history of information privacy law and its origins *see* DANIEL J. SOLOVE, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 1-1 (Kristen J. Mathews ed., 2006) [hereinafter PROSKAUER ON PRIVACY].

117. MCCORD, *supra* note 109, at 45.

118. *See* DOUG LINDER, *The Right to Privacy: Is It Protected by the Constitution?*, EXPLORING CONSTITUTIONAL CONFLICTS (2015), http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

119. MCCORD, *supra* note 109, at 47.

120. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1828–31 (2010).

121. GELLMAN & DIXON, *supra* note 47, at 13.

The privacy torts,[122] other common law protections, constitutional law protections, a variety of legislative and regulatory schemes,[123] and other remedies applicable to information and data protection harms are already available to a plaintiff, so when privacy advocates call for special private data legislation for Internet users to redress any problems that arise those cries often go unanswered. However, these protections fail to protect users' private data because most people do not easily know when their data privacy has been breached until it is too late.[124] As various remedies have been tested in the courts to resolve the information privacy conundrum, plaintiffs often find themselves lacking the requisite standing or justifications to trigger relief.[125] Legislation is slow to catch up with all but the most egregious privacy intrusions such as the driving records and video rentals records privacy legislation mentioned earlier.[126]

An overarching scheme to protect personal information must be proposed that provides a cause of action and extends some form of relief beyond the common law and constitutional remedies that already exist. A variety of somewhat novel proposals are ready to be tested in the courts and through legislative initiatives. The proposal to permit a person to erase or suppress old information or a tainted set of personal data , or reputation-damaging content would allow a person who discovers she has been defamed or is made aware of embarrassing things she has done in the past has not been supported as a cause of action in any court to date.[127] The President's proposed legislation noted in his 2015 State of the Union address might create a code of big data ethics that will stem the death of privacy by governing information flows of personal information, but that legislation awaits congressional enactment.[128] The proposal to build Privacy by Design into new software products and services to limit privacy intrusions could be a viable option, but would require industry buy-in and some type of regulatory scheme.[129] A proposal to *curb the collection of*

Commented [B14]: Made several textual changes to clarify based on footnote editors comments.

122. PROSKAUER ON PRIVACY, *supra* note 116, at 1-13 to 1-46.

123. Covered briefly in Part II of this paper.

124. Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now Is The Time?*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 18 (2009).

125. Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, PENN L.: LEGAL SCHOLARSHIP REPOSITORY, Sept. 2015, at 1 (2015), http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2588&context=faculty_scholarship.

126. Cate, *supra* note 25.

127. Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 455 (2014); Miquel Peguera, The Shaky Ground of the Right to Be Delisted (Aug. 14, 2015), http://works.bepress.com/miquel_peguera/1; Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 258-59 (2012).

128. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 408–26 (2014). As of January 2016, the Senate and House Bills introduced, S.547, 114th Congress (2016) and H.R.1053, 114th Congress (2016), have not been reported out of committee.

129. Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1335–43 (2013)); *see* Aaron Massey, *Getting to October: Why Understanding Technology Is Essential For Privacy Law*, 51 IDAHO L. REV. 695, 697–698 (2015) (arguing that the current PbD policy initiatives do not provide enough specific guidance to be practical); Michael Birnhack, Eran Toch & Irit Hadar.

"social intelligence", defined as the collection of digital data about social relationships could provide a mechanism for limiting the reputational harms associated with hastily posted information, its metadata, and geolocation information available from social media sites.[130] The use of "de-identification" techniques to separate a person's identity and her information stores could be a part of the President's proposal, but it is unclear until the legislation makes its way through Congress.[131]

Many of these newer proposals for privacy protections revolve around notions that controlling the effects of technology should not be left exclusively in the hands of legislators or judges, whose rulings are often rushed to meet the urgency of the case at hand.[132] Businesses and industry have also proposed schemes such as Value Sensitive Design, which is a theoretical approach aimed at controlling the intrusive capabilities of technologies by embedding ethics and human values in the design and manufacture of those technologies.[133] The theory is still untested for the most part.

Ideally, a set of industry practices and codes of commercial conduct with teeth could provide the best solution, but will need legislative or judicial assistance to succeed.[134] The basic commercial codes of conduct and industry practices must at a minimum address transparency in data collection practices and limit the amount of information collected about a person.[135] The enforcement of those codes and practices could be strengthened if the FTC is specifically authorized to include online privacy practices of social media sites and if a proposal to create a Privacy Policy Office is effectuated.[136] The FTC has already recommended that it be allowed to require that data brokers be more transparent by revealing their information collection practices.[137] Additionally,

---

Privacy Mindset, Technological Mindset, 55 JURIMETRICS J. 55 (2014) for arguments against "privacy by design" proposals.

130. Laura Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061, 1070 (2015).

131. Yianni Lagos, *Taking the Personal Out of Data: Making Sense of De-Identification*, 48 IND. L. REV. 187, 190, 190 n. 23 (2014). As of January 2016, the Senate and House Bills introduced, S.547, 114th Congress (2016) and H.R.1053, 114th Congress (2016), have not been reported out of committee.

132. Alexandra Rengel, *Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights*, 8 INTERCULTURAL HUM. RTS. L. REV. 177, 225 (2013).

133. *Id.*

134. *See* Rodrigues, *supra* note 101, at 247–48; *see also* HIRSCH, *supra* note 100, at 1031.

135. Jugpreet Mann, Comment, *Small Steps for Congress, Huge Steps for Online Privacy*, 37 HASTINGS COMM. & ENT. L.J. 365, 387–89 (2015).

136. *Id.*

137. FED. TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at viii (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

the President's Consumer Privacy Bill of Rights initiative may provide the timing and impetus to see that these codes and practices become a reality.[138]

A variety of approaches to information privacy protection in the United States have been proposed that, for the most part, have failed to fully inform individuals about the best ways to protect themselves from unintended releases of private information. Given the pace of current technological change, society cannot wait any longer for a resolution. Although consumer education might resolve some information privacy protection issues, most consumers are unwilling to read the entirety of a click-through license or a privacy policy online. A more robust privacy education scheme is needed.[139] Students and young people must become aware of the reputational harms that lie ahead and implement best practices in their everyday online behavior.[140]

Commented [B15]: Added clarifying text here and in the footnote.

A fully formed educational curriculum can play a vital role in preventing harm to young reputations. Friedman concludes that privacy education is needed since the average person contradicts her expectation and demand for privacy and anonymity when she is also perfectly willing to invade the privacy of other people.[141] A robust educational dialogue beginning at an early age can unearth these contradictory attitudes and sway the average person to be cognizant about her desire to disclose the secrets of another while at the same time wanting to preserver her own privacy. An educational curriculum that is well planned and implemented from elementary school forward will likely persuade a person to, at the very least, moderate the amounts of personal information she places on social media sites that might harm her reputation.

V. SOCIAL MEDIA SKILL SETS AND BEST PRACTICES

Social media skill sets are important and need to be developed and implemented at a very early age. Young parents are introducing toddlers to digital technologies very early; even before a toddler walks. This early introduction signals a pattern of digital use and databuse that is likely to develop before these youngsters enter school. Since it is likely that the digital dossier of these individuals will develop very early in life, the concepts of privacy protections should be introduced in the early grades. Moving forward into junior high and senior high school, the educational ideas of privacy laid out in the early grades can be refined, discussed, and practiced, and understanding could be heightened as a variety of projects or assignments bring the point home. As a

138. *Supra*, note 40.

139. *See* LAWRENCE M. FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 260–62 (2007) (discussing how an analogy to the drive for sex education in the 1960s can be made to the need for privacy education now. The point of his book is that "the average person likes his privacy, expects privacy, demands privacy, along with a certain degree of anonymity"); *see also* SOLOVE, *supra* note 68, at 203–04 (exploring some of what we can do to protect students and young people from themselves).

140. Astringer, *supra* note 39, at 297 (advocating for an expansion and upgrade of Internet education requirements for young adults to include social media).

141. FRIEDMAN, *supra* note 139, at 260–62.

student decides to enter college or junior college or a trade school, she should be encouraged to continue to develop knowledge of privacy principles and should be encouraged to develop policies for classes in which she participates.

Although much of this article is aimed at protecting the reputational interests of students as they make their way through our required educational system, undergraduate and law school curriculums should also be developed, and proposals have been included below. The idea of proposing a curriculum for the university and graduate-level programs may seem farfetched, but universities now welcome ideas for new proposals as a part of core curriculum or outside the classroom curricular models.[142] Going well beyond the idea of having a student develop privacy practices for classes in which she participates, she might also be a vital part of assisting others in the university setting increase their understanding about how to keep data safe. This can be accomplished if she becomes a member of a student advocacy group or a student body leader. As she enters her first internship experience in her final undergraduate year, she might even be encouraged to provide feedback about privacy principles to companies, legislators, or other employees based on the comprehensive knowledge she has acquired as a result of her K-16 education about the topic. Ideas about setting policies, creating guidelines, developing schemes for monitoring, and developing either authorization schemes for privacy protection have been included in the ideas set out here.

A. K–12 Curriculum Ideas

A K-12 curriculum should take a "building blocks" approach. Ideas should be developed and reinforced, vocabularies introduced and practiced, and concepts could be illustrated through a series of capstone exercises as students prepare to leave high school.

As a part of the K-8 curriculum terminology and concepts can be introduced and refined.[143] Students entering elementary school are already learning new words and their meanings. Adding a set of privacy terms and definitions to a vocabulary lesson is explored below:

(1) Introduce the word privacy, related terms and their definitions[144] as early as kindergarten.

Commented [B16]: Changed to the numbering followed by letters as you suggested.

142. *See, e.g.*, *Curriculum Proposal System*, OR. ST. UNIV., https://secure.oregonstate.edu /ap/cps/proposals (last visited Nov. 2, 2015) (available for student input); *What Is the OCC?*, UNIV. OF PITTSBURGH, http://www.studentaffairs.pitt.edu/occwhatisit (last visited Nov. 2, 2015) (explaining an Outside the Classroom Curriculum idea being vetted at the University of Pittsburgh).

143. *See, e.g.*, IKEEPSAFE, IKEEPSAFE PRIVACY K-12 CURRICULUM MATRIX (2015), http://ikeepsafe.org/wp-content/uploads/2015/08/PDF_iKeepSafe-Privacy-K-12-Curriculum-Matrix_8.05.2015.pdf (including lesson ideas and learning objectives, but which does not include practice and role playing ideas).

144. While appropriate definitions other than those found online, in the dictionary, or in a thesaurus, may be difficult to locate, younger students will greatly benefit by role playing or by learning about real life examples of what is "private" and what is "public."

(2) Grades 1-3 - Reinforce the terms and definitions and introduce scenarios that include ways of protecting information in online settings.

(3) Grades 4-6 - Reinforce the notion and concepts of privacy by tying related concepts such as personal information, knowledge, dignity, freedom, reputation, and disclosure.

(4) Grades 7-8 – Practice terms and concepts by reinforcing the notion of privacy as a socialization process. Implement a series of exercises such as the following:

(a) Inventory personal information you have released to businesses and others. Create a log of what was supplied and where it is safeguarded on personal computers.

(b) Research the laws that apply to keeping that information secure.

(c) Learn the steps that businesses must perform to do a risk and root cause analysis when a breach of data occurs.

(d) Learn how to encrypt a laptop and other devices.

(e) Develop a list and process for knowing when passwords, links to websites, and other access points providing routine paths to data are secure.

(f) Create a list of ways to stay connected but to only share personal information with trusted friends.

(g) Learn how to use Facebook and other social media sites' privacy settings and ways to create personal prompts to regularly change privacy settings and review new user information provided by the site about those settings.

(5) Grades 9-12 provide the perfect opportunity to promote ways to practice and discuss safe modes for protecting personal information and other data.

(a) Have students who follow each other's accounts become comfortable with reporting others' behaviors.[145]

(b) Discuss harms that accrue when violent online behavior is tolerated.

(c) Discuss methods for dealing with a future employer's requests for Facebook or social media passwords.

(d) Explore procedures for raising personal information intrusion claims through a regularly accessed online entity.

145. David Geer, *Posting a Threat: Recognizing and Responding to Threats of Violence Made Via Social Media*, UNIV. BUS. MAG. (Nov. 2012), http://www.universitybusiness.com /article/posting-threat (noting that the best way to discover potential violence and threats is to make students who follow each other's accounts comfortable with reporting threats and behaviors).

(e) Assign students an exercise in which they craft a base line consumer bill of privacy rights.

(f) Assign students an exercise in which they detail best practices and a process for self-regulating their online behavior using pictures or through storytelling.

A variety of exercises and other ideas developed for the early elementary grades for protecting privacy generally are available at the iKeepSafe.org website. It also explores the concept of building and online reputation, but only generally. Other privacy ideas and concepts are explored more expansively in a twenty-eight page curriculum guide.[146] Other curricular ideas are presented by the Common Sense Education website which focuses primarily on digital citizenship and offers two curriculum lessons on privacy concepts.[147]

B. Undergraduate Curriculum Ideas

Undergraduates are ready to tackle more difficult analysis and conceptualization of concepts. This proposal could accommodate course types ranging from the fine arts to the pure sciences. It could also be presented as a series of curricular models outside the classroom, as a series of TED Talks, Massive Online Open Courses (MOOCs), or be required in certain core areas of speciality such as education, general studies, business, and communication studies where the concepts and ideas surrounding ethical practices should be explored. At this stage of their education, students could provide the colleges and universities they attend with pertinent data about their searching techniques, personal information disclosures, and other information about their online experiences and about techniques they use in protecting their personal data. They could also make relevant recommendations for necessary policy changes to university policies concerning safe use of social media sites. Much of that information could be presented and data could be collected during key times in the undergraduate life-cycle.

1. Pre-Admission Materials

In pre-admission packets or in online venues before matriculation, universities should provide materials such as University Computer Usage Policies, Codes of Conduct, selected sets of privacy articles, a short book on the topic such as the self-published, *Online Privacy: How To Remain Anonymous & Protect Yourself While Enjoying A Private Digital Life On The Internet* by Brendon Ward, checklists of best practices for protecting personal information online, and sets of exercises aimed at encouraging safe online digital practices.

Commented [LT17]: Would you be open to bolding these sub-headings to make them stand out more?

Commented [B18]: Agreed. Please check for consistency since I may have missed a few.

146. *K-12 Digital Citizenship Curriculum*, COMMON SENSE EDUC., https://www.commonsensemedia.org/educators/curriculum (last visited Nov. 4, 2015).

147. *Id.*

2. Undergraduate Orientation

Orientation is often the only time that students will meet together with others in their cohort group. This a time that exploration of students' current knowledge of privacy principles can be assessed and enhanced. Pre- and post-tests to gather information could be created and administered either online or in a variety of orientation venues. As a part of orientation activities, students could meet in small groups to discuss materials noted above that should be included in pre-admission packets. With a good facilitator, discussion is often a valuable way to discover what privacy means to each student in the group. Students are also more likely to explore and defend their ideas about ways to increase privacy protections in a small group setting. Often the exchange of ideas brings new tools and concepts to light that students may not have encountered as high school students which some will incorporate or explore as a way of keeping information safe, confidential, and secure.

3. Discussion of Privacy and Practice in Targeted Colleges within the University or in Outside the Classroom Curricular Settings

Students who are involved in business, marketing, communication, journalism, political science, and curriculums crafted around public policy concerns will be interested in exploring privacy principles with their students before they enter workplace settings or in professional club settings on campus. A series of TED Talks about privacy subjects could be produced by individuals in the groups or by key administrators who are aware of gaps in privacy knowledge which they have gleaned from the students' pre- and post-tests. Students who are especially knowledgeable or interested in information privacy could be encouraged to produce short MOOCs or lessons about a topic of interest. These short lessons could also become a part of a lesson plan for a marketing, communication, journalism or other course and could be contributed to a class Wiki or documented through some other technology tool which could track a set of topics over a period of time for those professors who might be interested in experiential learning experiences in their classroom. As a part of a series of TED Talks, students could illustrated the dos and don'ts for maintaining privacy settings on social media sites or other information that could put students at risk for being expelled.[148] Professors could make a series of current articles available that illustrate best practices and then break their class into discussion groups that explore the ramifications for not revising social media settings, during which students could provide personal experiences and insights.[149] For those professors and outside groups that agree that students learn a topic well

148. *See What You Put Out There Can Hurt You*, ECAMPUS NEWS, March, 2012, at 14 (discussing how Syracuse reinstated a student after his Facebook expulsion).

149. *See, e.g.*, Caitlin McGarry, *FaceBook Changes the Way it Tracks and Serves You Ads*, PC WORLD, (June 12, 2014), http://www.pcworld.com/article/2362629/facebook-changes-the-way-it-tracks-and-serves-you-ads.html (discussing control over your website experience); Ian Sherr & Seth Rosenblatt, *That Privacy Notice You're Posting to Facebook? It Won't Work*, CNET/TECH CULTURE, (December 2, 2014, 4:00 AM), http://www.cnet.com/news/that-privacy-notice-youre-posting-to-facebook-it-wont-work/.

when they are challenged to teach it, those educators could challenge students to create a variety of hands-on exercises about search engine privacy which could be presented as a series of short quizzes. Once the results of those exercises are known to the entire class they could then discuss the results to determine the level of students' awareness about the search engines to avoid because they are notorious for collecting their personally identifiable data. They could also determine which website privacy policies could be models for other websites to investigate.[150] This could then lead students to create models of best practices and procedures to introduce into workplaces, gaming websites, commercial website, or other appropriate venues.

Students could also be encouraged to have discussions about the types of privacy groups that are interested in protecting PII. Students could visit and present information about the Electronic Privacy Information Center, the American Civil Liberties Union, and the Electronic Frontier Foundation websites. Then the class as a whole could discuss each privacy group's goals for helping consumers keep personal information secure. These presentations could be followed by having students research and present findings about which privacy groups have called for greater privacy protections for search engine information.

A series of TED Talks could key in on collection, retention, and disclosure rationales behind information policies. Students could locate published privacy policies on websites provided by entities such as Facebook, LinkedIn, Google, etc.[151]

Another class exercise could be created that requires a group to search for federal laws that provide uniform privacy protections for personal data submitted to financial and health-related search engines. Follow up research papers could be a part of a for-credit course.[152]

Another exercise might involve having students search for corporate policies or for IP address tracking features used by online entities.[153] Once they are located these policies or features could be discussed and dissected.

4. Locational Privacy & New Social Media Channels

Marketers promote locational software services by offering discounts and coupons to individuals who "check in" to their location.[154] The Pew Internet

150. Linda Rosencrance, *Survey Finds Solid Opposition to Release of Google Data to Feds*, COMPUTER WORLD, (Jan. 24, 2006), http://www.computerworld.com/s/article/107993/Survey_finds_solid_opposition_to_release_of_Google_data_to_feds?taxonomy (discussing a 2006 survey of Google users which revealed that 89% think their search terms are kept private).

151. Facebook, Google, and other privacy policy changes since 2006, have been widely discussed. *See* articles in PC WORLD and CNET for examples too exhaustive to include here.

152. *See, e.g.*, 45 C.F.R. § 164.514(b)(2)(i)(O) (2014).

153. Some federal regulations treat IP addresses as "individually identifiable" information for specific purposes, but such treatment is not comprehensive and corporate policies vary widely.

154. Ryan Goodrich, *Location-Based Services: Definition & Examples*, BUS. NEWS DAILY, (Oct. 30, 2013, 5:34 PM), http://www.businessnewsdaily.com/5386-location-based-services.html.

and American Life Project found that 8% of U.S. adults ages 18-29 use location-based services such as Foursquare or Gowalla significantly more than online adults in any other age group.[155] To make students aware of the potential information accumulation effects these uses have, a series of exercises could center on the topics that follow:

Commented [B19]: Article check showed these changes were needed.

(1) Locational privacy is now a hot topic.[156] Have students search for recent cases from their home states.

(2) Have a group search for both federal and state locational privacy law legislative proposals since 2003 and report back on the intent of the proposals.

(3) Have groups present information about locational privacy protections offered in the Electronic Communications Privacy Act.[157]

(4) Have a discussion about individuals moving about in public space, and their expectation that their movements will be largely anonymous.

(5) Discuss the potential ramifications of running Foursquare, Facebook Places, and Google Maps on phones knowing that this use of information will result in targeted advertising and could be used for other purposes. Discuss some of those other unauthorized uses and how they could put user information at risk.[158]

5. Social Media Security Discussion and Exercise

Social media site present some of the most security challenges to students who are unaware of potential pitfalls and traps. A TED Talk or MOOC could begin to explore these typical social media site security problems by asking students to add to a list such as the one that follows:

(1) Hacking; what it is, and how to avoid being hacked.

(2) Discuss what to do after a Facebook or Google account gets hacked.[159]

(3) Identity Theft; what it is and how to avoid it.

(4) Discuss how people close to a person – a mother, boss, or significant other - would react and fear for a person if they read what she typed into

155. Kathryn Zickuhr & Aaron Smith, *4% of Online Americans Use Location Based Services*, PEW RES. CTR. (November 4, 2010), http://pewinternet.org/Reports/2010/Location-based-services/Overview.aspx.

156. *See Locational Privacy*, EPIC (last visited Nov. 7, 2015), https://epic.org/privacy/location_privacy/#Case_Law for frequently updated information on case law in the EPIC organization's Locational Privacy forum section.

157. 18 U.S.C. §§ 2701–712 (2012).

158. *See* Andrew J. Blumberg & Peter Eckersley, *On Locational Privacy, and How to Avoid Losing It Forever*, ELECTRONIC FRONTIER FOUND., (August 2009), https://www.eff.org/files/eff-locational-privacy.pdf (discussing information useful in starting the conversation).

159. Mat Honan, *What to Do After You've Been Hacked*, WIRED MAGAZINE, (Mar. 15, 2013, 6:00 AM), http://www.wired.com/2013/03/what-to-do-after-youve-been-hacked/.

computers. Never type anything into a computer that a mother might read which would cause her to become alarmed.

(5) The dangers of running malicious programs, especially ones that ask for access to students' profile information.

(6) Compromising friends' personal information when students are hacked.

(7) Risks of using Facebook Apps that could put student personal information and friends' personal information at risk.

6. Discussion and Rule Setting to Prevent Security Breaches

Professors could use discussion boards or outside-of-class electronic tools to create a set of rules for a class to use throughout the semester which students could be encouraged to add to or modify or comment on as the semester ensues. The discussion could include creating rules about how to avoid putting sensitive information into a profile such as social security numbers and bank account information or how to limit the personal information such as credit cards, addresses and phone numbers that they store on a website. Other rules could be crafted around the following topics:

(1) Using social media site applications sparingly and refusing requests to gain access to sensitive student profile information.

(2) Ways to run anti-virus and anti-spyware software at all times, ways to check for free alternatives recommended by the university, and ways to regularly update this software.

(3) Setting computers to scan for malicious intrusions at least weekly.

(4) Checking software before installing it to ensure it is the software purchased or desired in order to avoid potential malware attacks.

(5) Avoiding clicking on links in email and other online solicitations from social media sites unless students know who sent them.

(6) Using a strong password and avoiding using the same password for multiple sites, and investing in a secured vault for password storage such as McAfee's Safe Key Vault in order to remember those passwords.

(7) Ways to avoid permitting access to a personal password and ignoring requests from websites asking for a password in order to locate a person's friends.

(8) Logging out of a public computer after using it.

(9) Changing all passwords at least every six months and using a storage mechanism or commercial software to store them.

(10) Declining to share a computer, phone, PDA, etc. unless separate profiles with separate passwords are created in order to avoid having someone post an embarrassing or misleading statement under a person's name.

7. Preventing Security Intrusions

Students could also create a set of good security practices which could follow some of the protocols that are generally accepted based on the author's research into a series of privacy group recommendations and website best practices protocols:

Browser link protection practices

(1) Experiment with and review the privacy controls in browsers other than the ones students regularly use. For example, compare controls in Firefox or Chrome to those in Internet Explorer.[160]

(2) Explore cost versus benefit of blocking ads in order to avoid dangerous links and viruses.

(3) Create an exercise on checking the authenticity of URLs.[161]

8. Facebook Precautions

Since Facebook is currently one of the most used social media sites, a student's likelihood of having her personal information discovered greatly increases. A separate discussion of precautions is necessary in at least one required class, TED Talk, or in some other training venue.

(1) Discuss ways to keep personal information[162] placed on Facebook to a minimum.

(2) Discuss safe uses of Facebook friend lists.[163]

(3) Discuss the use of outside applications provided by Facebook.

Policy Exercises to Use in Various Classes

Social media sites' privacy policies should be clear and should permit users to easily understand their obligations. However, social media sites' privacy policies and terms of use often require users to switch between the two to understand the details and the definitions of the privacy agreement.[164] This can lead to misunderstandings and frustration. For example, the military, which had banned the use of social networks in 2009, reconfigured its Internet grid,

160. Some browsers prevent cross-site linking. Cross-site linking permits a hacker to insert dangerous code into seemingly non-malicious looking URLs.

161. Seth Rosenblatt, *How To Check If a Web Site Is Safe*, CNET (Aug. 26, 2011 4:18 PM), http://www.cnet.com/how-to/how-to-check-if-a-web-site-is-safe/.

162. An information-heavy profile may put a user at risk for identity theft. Users who include birthday, address, and phone number information are making themselves vulnerable. Pictures should also be discussed since certain digital cameras encode information about images.

163. Personal settings that are not restricted to "friends only" may create unintended consequences. Have students discuss creating several different friends lists, and assigning different permissions to each so that most casual friends are restricted to just basic information.

164. *See, e.g.*, LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 121–36 (2012); *see also* Oliver Smith, *Facebook Terms and Conditions: Why You Don't Own Your Online Life*, THE TELEGRAPH (Jan. 4, 2013, 1:20PM GMT), http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html.

NIPRNET (Non-classified Internet Protocol Router Network) – the largest private network in the world – to provide soldiers access to YouTube, Facebook, Myspace, Twitter, and Google apps along with a strong social network policy statement.[165]

(1) Have students explore definitions of terms such as privacy, profile, third party applications, and others on at least two social media sites and share their findings with the class.

(2) Have students explore geo-location based explanations and policies for the use of a user's personal information on at least two social media sites and share their findings with the class.

C. Best Practices in Law Schools – Classroom Discussions

Legal ethics and professional responsibility have received great attention in recent bar and law school articles, local presses, blogs, and websites such as the American Bar Journal and the ALM website which issues regular updates on technology and privacy issues. Symposia about legal malpractice and ethics of information privacy have been presented by the Berkeley Technology Law Journal (BTLJ) and by the Loyola Consumer Law Review in 2015. Additionally, the Privacy Law Blog pressed by the Proskauer Rose LLP group could be consulted weekly for regular information updates concerning a variety of privacy issues, including information privacy. The Law School and its constituents from a variety of law school departments such as the Library, Career Services, IT and more are called on to join their colleagues in the classroom in educating students concerning ways to form a positive, professional identity both online and offline. Although much of that identity has been formed around non-professional relationships up to the point of entry into law school, after law school orientation, this group of online professionals often counsels students concerning professional demeanor while attending law school, ethical violations that must be reported to the local bar, the best ways to network and form professional relationships and much more. Discussions about forming that professional legal identity when using social media and other websites can explore best practices, engaging in safe, ethical habits online, and on practices on working towards changing a former less than professional image on social media sites by lowering Google hits on poor behavior and raising hits on good, professional images. These discussions will engage students in the types of higher levels of analytical thinking that those of us in law school educational settings aspire to promote. The best settings for these discussions include the classroom, clinics, career services events, library training programs, and technology training programs focusing on improving a person's online image. The process can start with law school orientation.

165. *Id.*

1. Law School Orientation Training Sessions

A variety of discussion sessions about privacy and personal information can take place during a school's orientation program. Although time is often limited during orientation at most schools, the 1Ls who make up a new cohort group are motivated to learn about professionalism issues and information privacy is something to which each person can easily relate. Those discussions could include, but are not limited to, the topics that follow:

(1) Social media policies,

(2) Opt-in and opt-out policies for social media sites, and

(3) Facebook profile settings.

Discussions in small groups could explore:

(1) Facebook's privacy controls and settings and how they could affect a law student's reputation.

(2) Ways that users can opt-out *before* sharing private information of their own or about their contacts through an exploration of a variety of live social media sites.

(3) Examples of profile settings on a Facebook page that are "too broad" versus those that will protect most privacy intrusions.

(4) Facebook's default settings and how they might disseminate all of a user's profile changes to all of a user's contacts.

(5) A review of the "my privacy" section of any social media site.

(6) A variety of social media sites' opts-out systems which, for the most part, assume consent in the absence of an affirmative act by the user.[166]

(7) A review of TRUSTe[167] and other privacy certifications and their validity.[168]

166. *See generally* Scott R Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014); *see also id.* at 140 (discussing new technologies that are lacking notification and consent protocols).

167. TRUSTe is a data privacy management company which works with businesses on attaining privacy compliance across business information collection practices and data use channels.

168. Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 295–99 (2012) (discussing TRUSTe certification and erroneous privacy practices).

2. Law School Classroom Discussions and Interactive Exercises; 1L to 3L

Contracts or contract drafting and negotiation courses could include hypotheticals about Terms of Service (TOS) agreements and privacy policies.[169] Questions could be raised about:

(1) Whether contracts with social media sites must build in a user's ability to close an account completely.

(2) If a social media provider merely "deactivates" an account and retains all of that user's information, does a cause of action exist?[170]

(3) How privacy policies in the TOS are spelled out on a social media site. If a user wants to protect profile information such as users' names, profile pictures, friends' lists, fan pages, and more, can that user be protected from third party applications desiring access?[171]

Other discussions and hypotheticals could center on the differences between contracts and other types of enforcement mechanisms. For example:

(1) If a party proceeds with a transaction after viewing the terms of the online contract, they are assumed to have consented. What other options besides assent exist in electronic contexts?

(2) Is encrypted information an automatic signal to a website provider that a person is intentionally desiring to keep her information confidential?[172] Most often, encryption is not mentioned in most user contracts nor is it encouraged.

(3) Is the "do not track" option selected in a consumer's browser enough notice in and of itself as a matter of contract law that a person's data should not be used or shared with data brokers?[173]

Torts classes or upper level specialized seminars dealing with the privacy torts could include hypotheticals about needed changes to the privacy torts as they related to "spaceless" infringements taking place in the online world. These could include:

---

169. Most social media privacy policies are fluid, and may be altered by the Web site, nearly at will. Although changes will be posted on the site, rarely do sites specify how long these changes will be posted or where they are posted.

170. *See, e.g.*, Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 929–33 (2013) (discussing privacy lurches).

171. *See* G. S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 167–171 (2012–2013).

172. *See* Carly Fabian, *iPhone's Encryptions Protect Privacy*, UNIV. WIRE [CARLSBAD], published in the UCD ADVOCATE, Univ. of Colo. Denver, Denver Colo., (Nov. 12, 2014).

173. Joshua A.T. Fairfield, '*Do Not Track' As Contract,* 14 VAND J. ENT. & TECH. L. 545, 582-83 (2012).

(1) Is public disclosure doctrine applicable to the online world and especially to social media sites?[174]

(2) How should intrusion be defined in web-based spaces?

(3) What constitutes public disclosure of information on the Internet?

(4) Is the privacy tort of publicity relevant to social media sites?

Professional Responsibility and ethics classes or discussions about ethics can explore a variety of privacy questions from various contextual perspectives. Some examples follow.

(1) Facial recognition technology[175] allows a person to be identified, normally to gain access to a secure system of some type. A Professional Responsibility class could discuss the uses of this technology to locate other personal data about an individual by asking questions such as:

(a) Could social media sites like Facebook be mined by the government for facial recognition purposes?

(b) What does the use of facial recognition technology mean for privacy and civil rights?[176]

(2) Internet protocol addresses (IP addresses) are assigned to a device in order to allow devices to communicate with each other. In many cases, those addresses are static and identifiable. Questions that could be raised in class about privacy invasions of static IP addresses include:

(a) Are IP addresses personally identifiable information[177] that businesses should be allowed to link to an individual user?[178]

(b) What best practices should websites use to ensure that IP data is regularly deleted?

(3) Newer technology tools such as Spotify and even Windows 10 software have appeared online recently that are raising new privacy concerns.[179]

---

174. *See* Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J. L. & TECH. 1, 27 (2007) (discussion of a more coherent factor-based approach).

175. Generally, an image of a person must be stored in a computerized system of some type in order for the image being verified via a video source. Privacy advocates argue that this leads to further digital data stores about an individual.

176. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012).

177. *See* Tene, *supra* note 11.

178. Frederick Lah, Note, *Are IP Addresses "Personally Identifiable Information?* 4 ISJLP 681, 693 (2008) (explaining that search engines track IP addresses to account for or prevent "click fraud," a false accrual of clicks on advertisements such as those found on Google, and about which Google defends its retention of search queries and associated IP addresses); *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept Of Personally* Identifiable *Information*, 86 N.Y.U. L. REV. 1814 (2011) (discussing PII as a central concept in determining privacy harms).

179. *See* Ed Silverstein, *Privacy Concerns Arise With Windows 10 Release,*

Pinterest,[180] FourSquare[181] and SnapChat[182] social media websites were not even imagined several years ago, but each raises significant privacy and litigation concerns. Twitter has come under some fire from privacy advocates about use of a user's profile and other information.[183] Questions about ethical practices could include:

(a) What are some of the typical ways that social media companies could give the wrong impression to consumers about privacy of consumer information?

(b) Compare the privacy policies of social media sites regularly accessed and report back on potential privacy concerns.

(c) Do some of these consumer practices violate the FTC FIPs?

(4) E-discovery is another area of in the realm of social media worth discussing and probing with students in a Professional Responsibility class.[184] Some of the questions that could be presented about navigating a variety of social media privacy legal risks include:

(a) Can social media be included in a discovery (e-discovery) request in the litigation context?

(b) If so, are there rules as to how far someone can reach in your social media history?

(c) Can attorneys tell their clients to deactivate all social media?

LEGALTECHNEWS (August 3, 2015), http://www.legaltechnews.com/id=1202733750584/Privacy-Concerns-Arise-With-Windows-10-Release?slreturn=20150830203849.

180. *Ignoring Pinterest in 2012 Could Make Colleges Look 'Old and Stodgy'*, ECAMPUS NEWS, May, 2012, at 25; *see also* John B. Kennedy, *Current Trends In Litigation Involving The Use Of Social Media*, 1 ASPATORE 2014, 2014 WL 5465788 (advising readers that "social media now affect all phases of litigation as the various media transform how lawyers handle cases. Lawyers scour all areas of social media to find information posted by parties about their case. A search for contradictory interests and activities through the pictures posted on Pinterest can give ammunition for cross-examination and support or erode a witness's or party's credibility")."

181. Foursquare learns what you like and leads you to places you'll love. Find great recommendations based on your tastes, your ratings for similar places, and the friends and experts you trust most. However, the privacy policy on this site is proactive about the privacy advice it provides to its users. FOURSQUARE, https://foursquare.com/about (last visited, Jan. 24, 2016).

182. *See* Ryan G. Ganzenmuller, *Snap and Destroy: Preservation Issues for Ephemeral Communications*, 62 BUFF. L. REV. 1239, 1250–52 (2014) (for a discussion of SnapChat and its privacy policies).

183. The FTC took action against Twitter in June 2010 for misleading consumers about the security, privacy, and confidentiality of nonpublic consumer information. *See Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program*, U.S. FED. TRADE COMMISSION (June 24, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal.

184. *See* Agnieszka McPeak, *Avoiding Misrepresentation in Informal Social Media Discovery*, 17 SMU SCI. & TECH. L. REV. 581, 595 (2014) (discussing an attorney's duty to avoid misrepresentation in attempts to access private social media content); Dera J. Nevin and Marc Jenkins, *Information, Knowledge, and the Pursuit of Privacy*. 38 AM. J. TRIAL ADVOC. 485, 492–501 (2015) (discussing ways for in house counsel to deal with a variety of discovery requests).

(5) Other more traditional ethics discussions could include a variety of questions ranging from client solicitation to client confidentiality. A recent article discusses potential ethical issues that are of particular interest to intellectual property attorneys.[185] It could be mined for a series of questions to present in class such as those that follow:

(a) Are the ethics rules concerning social media use interpreted similarly in all jurisdictions?[186]

(b) Under Rule 4.2 may opposing counsel send a friend request to the opposing party since an attorney can specifically ask for the party's consent to access all social media sites and compel the discovery if there is resistance?[187]

(c) What requirements in the Model Rules are triggered by new technologies? Under Model Rule 1.1 what does an attorney need to know about information privacy in order to provide competent representation to a client?

(d) In the age of new technologies, what does it mean to provide competent representation to a client in terms of keeping information private?[188]

(e) Should an attorney use social media to advertise to clients?[189]

(f) Social media provides a great opportunity for an attorney to learn more about potential jurors. Not only can an attorney get a broader picture of the person they are considering in voir dire, but also they can double- check the veracity of the potential juror's responses. Is it an ethical violation to investigate potential jurors in this way?[190]

---

185. Cynthia Laury Dahl, *Making 'Friends' with the #Ethics Rules: Avoiding Pitfalls in Professional Social Media Use"*, 43 AIPLA Q. J. 155, 156-57 (2015).

186. *Id.* at 157–58 (discussing the great differences that exist between state Bars).

187. *Id.* at 174 (noting that under the Model Rules, it is a violation).

188. KAREN ELTIS, COURTS, LITIGANTS, AND THE DIGITAL AGE: LAW, ETHICS AND PRACTICE 91 (2012) (discussing judicial ethics and the use of social media); James Podgers, *Lawyers Struggle To Reconcile New Technology With Traditional Ethics Rules*, ABA J. (Nov 01, 2014) http://www.abajournal.com/magazine/article/the_fundamentals_lawyers_struggle_to_ reconcile_new_technology_with_traditio/ (originally appearing in the ABA JOURNAL November 2014 with this headline: *The Fundamentals: Lawyers Struggle To Reconcile New Technology With Traditional Ethics Rules)*; Glen M. Vogel, *A Review of the International Bar Association, LexisNexis Technology Studies, and the American Bar Association's Commission on Ethics 20/20: the Legal Profession's Response To the Issues Associated With the Generational Gap In Using Technology and Internet Social Media*, 38 J. LEGAL PROF. 95, 120 (2013); Robert Keeling, et al., *Neither Friend Nor Follower: Ethical Boundaries On the Lawyer's Use of Social Media*, 24 CORNELL J.L. & PUB. POL'Y 145, 171–81 (2014).

189. *See The Law of Social Advertising*, *in* ROBERT MCHALE, NAVIGATING SOCIAL MEDIA LEGAL RISKS (2012) [hereinafter NAVIGATING SOCIAL MEDIA LEGAL RISKS]; Elizabeth Colvin, *The Dangers Of Using Social Media In The Legal Profession: An Ethical Examination In Professional Responsibility*, 92 U. DET. MERCY L. REV. 1, *3* (2015) [hereinafter *Colvin*].

190. *Supra* note 180, at 178–79 (noting that the answer will differ from jurisdiction to jurisdiction).

> (g) Although it might not be well received at first, could "reverse mentoring" in the law firm setting provide a solution to closing the technology gap?[191]
>
> (h) Is an attorney obligated to inform clients about the risks to confidentiality when using social media?[192]
>
> (i) Are attorneys required to attain a state of heightened awareness in the moments before sending or exploring messages on social media?[193]
>
> (j) Just as attorneys use social media to elicit business, elected judges especially might use social media as a component of their public campaigns. In addition, several states and the ABA have recognized a public interest in having judges connected to the communities they serve. But judges' impartiality is paramount to the administration of a fair trial and even the appearance of impropriety violates the Model Code of Judicial Conduct. Should judges be allowed to connect to/friend/follow or be followed by the attorneys that advocate before them without violating rules protecting the impartiality of the court?[194]

Commercial law or business association courses could also explore privacy concepts in areas of credit card tracking, corporate advertising, and employee privacy. These same concepts and discussions would also be relevant to labor and employment law specialty seminars.

Privacy principles relating to credit card tracking include concepts of how financial and business entities use personally identifiable information. The class could research the Credit Card Accountability Act and information privacy could be discussed.[195] Consumer privacy best practices could also be discussed in both commercial law and bankruptcy courses. Social media privacy risks under the Fair Credit Reporting Act in employment and other consumer transactions could be explored.[196]

As a typical business organizations course covers the topic of fiduciary obligations to shareholders, behavioral advertising and its potential consumer privacy pitfalls could be explored since this is an area in which the FTC is

---

191. *See* Andrews, *supra* note 164, at 122.

192. Colvin, *supra* note 189, at 18.

193. *See* Jan L. Jacobowitz, *Lawyers Beware: You Are What You Post--The Case for Integrating Cultural Competence, Legal Ethics, and Social Media*, 17 SMU SCI. & TECH. L. REV. 541, 576 (2014) (describing the heightened senses an attorney must bring to bear before posting to social media).

194. *See* Benjamin P. Cooper, *Judges and Social Media: Disclosure as Disinfectant*, 17 SMU SCI. & TECH. L. REV. 521, 533–36 (2014) (arguing for two bright line rules).

195. Laura E. Gomez-Martin, *Smartphone Usage and the Need for Consumer Privacy Laws*, 12 U. PITT. J. TECH. L. & POL'Y 1, 15 (2012); Brett Frischmann, moderator; Lorrie Cranor, Ryan Harkins, and Helen Nissenbaum, panelists, *Panel I: Disclosure and Notice Practices in Private Data Collection*, 32 CARDOZO ARTS & ENT. L.J. 784, 791 (2014) (discussing a variety of notice practices including credit card notices).

196. NAVIGATING SOCIAL MEDIA LEGAL RISKS, *supra* note 189, at 56–61.

showing interest.[197] Another discussion could take about differences in International business sectors transactions and privacy principles and an exploration of whose law applies.[198]

Employment and labor law topics such as sensor-based employee monitoring could be explored along with notions of employee consent.[199] Additionally, students could explore the legality of using friend requests in the pre-employment setting to obtain information about an applicant could be explored.[200] In the labor law seminar, special considerations about the use of social media accounts in government settings could be discussed.[201] An examination of new products being used in the workplace to prevent unauthorized data access and misuse of employee data by authorized users could also be explored.[202] A seminar could also explore policy approaches to using social media in the workplace and an employer's obligations in terms of monitoring, regulating, and disciplining employees about privacy abuses.[203]

A family law class could explore the notions of who will gain access to a person's information once she can no longer access it due to death or frailty of some other kind.[204] This could be an especially important time to drive home points about whether or not loved ones, family, or someone else may view material a person has posted on her sites and the potential property lawsuits that could develop over those digital assets.[205]

---

197. *See* FED. TRADE COMMISSION, SELF-REGULATOR PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), https://www.ftc.gov/sites/default/files/documents/reports /federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/ p085400behavadreport.pdf (which sets out a number of relevant enforcement actions); *see also* H.R. 5777, 111th Cong. (2010); *and see Boucher-Stearns Staff Discussion Draft: A Bill to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to that Individual*, H. COMM. ON ENERGY & COMMERCE (May 3, 2010), http://www.vjolt.net/vol16/issue1/v16i1_1-Klinefelter.pdf.

198. HIRSCH, *supra* note 100, at 1040–49; Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment Of The Second Wave Of Global Privacy Laws*, 74 OHIO ST. L. J. 1217, 1221–28 (2013).

199. Scott R. Peppet, *Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 114 (2014).

200. NAVIGATING SOCIAL MEDIA LEGAL RISKS, *supra* note 189, at 55.

201. *Id.* at 83.

202. John, K. Waters, *Storage Framework Safeguards Privacy and Runs With E-Discovery*, LEGALTECHNEWS (Apr. 8, 2015), http://www.legaltechnews.com/id=1202722833851/Storage-Framework-Safeguards-Privacy-and-Runs-With-EDiscovery. See the section in the article about states' prohibition of employers collecting PII from their employees; and *see* Jackie Ford, *What Clinton's Email Troubles Can Teach Employers*, THE NAT'L L.J. (Apr. 13, 2015) http://www.nationallawjournal.com/id=1202723266630/What-Clintons-Email-Troubles-Can-Teach-Employers?slreturn=20150419131652.

203. Lauren R. Younkins, Note, *#Ihatemyboss: Rethinking The NLRB's Approach To Social Media Policies*, 8 BROOK. J. CORP. FIN. & COM. L. 222 (2013); NAVIGATING SOCIAL MEDIA LEGAL RISKS, *supra* note 189, at 67–85.

204. Jason B. Jones, *Who Will Log You out When You're Gone,*" CHRON. HIGHER ED. (Dec. 1, 2014), http://chronicle.com/blogs/profhacker/who-will-log-you-out-when-youre-gone/58591.

205. Storm Tropea, Comment, *Social Media Is Permanent, You Are Not: Evaluating the Digital Property Dilemma in Florida Probate*, 39 NOVA L. REV. 91 (2014).

3. Best Practices in Law Schools – Skills and Simulation Courses, Clinical Training

With their emphasis on offering real life training to inculcate life-long skill sets, clinical environments are excellent venues for exploring some of the privacy information issues that will in the legal workforce. A variety of questions in each work setting could be explored.

New litigation setting strategies could be explored in clinical settings through a series of questions about information privacy that were recently proposed in the state of Florida concerning meeting with clients about a matter likely to result in litigation and the need to provide advice and counsel clients about privacy settings and removal of information from social media in the pre-litigation setting[206]

The Florida Bar Professional Ethics Committee also recently provided an advisory opinion[207] which proposes that attorneys explore a series of information privacy questions with their clients. The following questions, based on that opinion could then be explored in class:

(1) Pre-litigation, may a lawyer advise a client to remove posts, photos, videos, and information from social media pages/accounts that are related directly to the incident for which the lawyer is retained?

(2) Pre-litigation, may a lawyer advise a client to remove posts, photos, videos, and information from social media pages/accounts that are not related directly to the incident for which the lawyer is retained?

(3) Pre-litigation, may a lawyer advise a client to change social media pages/accounts privacy settings to remove the pages/accounts from public view?

(4) Pre-litigation, must a lawyer advise a client not to remove posts, photos, videos, and information whether or not directly related to the litigation if the lawyer has advised the client to set privacy settings to not allow public access?[208]

(5) Can members of the Bar be considered competent absent a working knowledge of the benefits and risks associated with social media?[209]

---

206. Professional Ethics of the Florida Bar, *Proposed Advisory Opinion 14-1*, FLA. BAR ASSOC. (Jan. 23, 2015), http://www.floridabar.org/DIVEXE/RRTFBResources.nsf/Attachments/8E73C71636D8C23785257DD9006E5816/$FILE/14-01%20PAO.pdf?OpenElement.

207. *Id.*

208. Cheri Budzynski, *Legal Ethics and Social Media: What Pre-Litigation Advice May an Attorney Provide to His or Her Client?*, ABOVE THE LAW (Feb. 23, 2015, 4:07 PM), http://abovethelaw.com/2015/02/legal-ethics-and-social-media-what-pre-litigation-advice-may-an-attorney-provide-to-his-or-her-client/.

209. Recent ethics opinions issued by the New York State Bar Association reveal that a lack of knowledge about the risks and benefits of social media use may violate the Bar's Guidelines on the use of social media. Joel Stashenko, *State Bar Updates Guidelines on Use of Social Media*,

Additionally, the Rules of Professional Responsibility can be probed using questions about "privileged" information on social media sites and e-discovery. These questions could be expanded to include authentication issues surrounding the use of social media evidence.[210] Newer technologies that are being proposed to assist with "freezing" social media evidence could also be discussed.[211]

In the corporate clinical setting, questions about marketing strategies and using online endorsements and testimonials could be explored through questions such as:

(1) Are Facebook, YouTube, or Twitter endorsements subject to FTC sanctions or other actions?[212]

(2) Must a corporation refrain from modifying a blogger review of a product?[213]

(3) What is a "Disclosure and Relationships Statement" and how might it relate to Tweets made about a product or service?[214]

(4) What qualifies as "user generated content" in the corporate setting and what are some of the risks associated with such content?[215]

(5) What risks are inherent in the use of social media sites for the inadvertent release of corporate proprietary information by employees?[216]

(6) What lessons learned in a variety of business settings and potential litigation scenarios should be incorporated into a company's social media policy?[217]

Other discussions about the duty of competence and attorney's' need to understand how big data and predictive analytics affect privacy interests of clients could be tested by asking questions such as:

(1) Is a data brokers' sale of "people search" products containing personal information to whomever wishes to purchase them ethical to use in a business setting?[218]

N.Y.L.J. (June 19, 2015), http://www.newyorklawjournal.com/id=1202729712423/State-Bar-Updates-Guidelines-on-Use-of-Social-Media?slreturn=20150830203521.

210. NAVIGATING SOCIAL MEDIA LEGAL RISKS, *supra* note 189, at 91.

211. *See, e.g.*, Ed Silverstein, *WebPreserver Allows for Collection of Legally Admissible Content from Social Media*, LEGALTECH NEWS (Apr. 14, 2015), http://m.legaltechnews.com /module/alm/app/ltn.do#!/article/1740907186.

212. NAVIGATING SOCIAL MEDIA LEGAL RISKS, *supra* note 189, at 39.

213. *Id.* at 40.

214. *Id.* at 47.

215. *Id.* at 103–21.

216. *Id.* at 210–14.

217. NAVIGATING SOCIAL MEDIA LEGAL RISKS, *supra* note 189, at 222–24.

218. Peter Segrist, *How The Rise Of Big Data And Predictive Analytics Are Changing The Attorney's Duty Of Competence*, 16 N.C. J. L. & Tech. 527, 599 (2015).

(2) Is it ethical for attorneys to employ data brokers to assist in gaining information about an adversary for use in settlement negotiations, investigatory tactics, or trial strategy?[219]

Externship Training

Using blogs to record student activity in an externship setting has become more and more typical. However, students should be cautioned to refrain from postings that are unethical, illegal, or that might harm their school's reputation. A variety of the techniques and questions used in clinical training sessions set out below could be applied to externship training discussions as well.

4. Best Practices in Law Schools – Career Services Office (CSO) Counseling in Law School

When law students are ready to enter the job market is a prime time to educate them about some of the issues they may face in a business setting. Educate users about social media as well as business etiquette using a scenario such as the one that follows:[220]

> Three law school externs regularly posts content about other firm employees using the Facebook timeline feature.[221] Most of their posts are about their boss Bill, whom they believe will soon be terminated, and a recently retired co-worker, Judy, a partner's executive assistant. Some of these Facebook posts could be construed as hostile towards the law firm, and in one instance, one of the externs bragged about destroying company property.
>
> One of the externs hoping to be hired recently found out that she would not be. She regularly sends passive-aggressive tweets at work and at home from her company smartphone via Twitter. Although the vast majority of her nearly 3,000 tweets are nonthreatening and do not name the firm or its employees, some could be construed as veiled threats towards the company.
>
> All three externs use their personal Facebook and Twitter profiles at work on company-provided laptops and smartphones, and at home on

219. *Id*. at 535.

220. *See* a similar scenario on which this is based in Will N. Widman, Note, *Does My Employer "Control" My Facebook Account?: Emerging Social Media Privacy Concerns In The Workplace*, 32 TEMP. J. SCI. TECH. SCIENCE, TECHNOLOGY & ENVTL. LAW 211 (2013).

221. The "Timeline" feature recently replaced the "Wall" feature on Facebook. *See* Zoe Fox, *Ready or Not, You're Getting Facebook Timeline*, MASHABLE (Jan. 24, 2012), http://mashable.com/2012/01/24/facebook-timeline-everyone-2/. This feature is a much expanded version of the previous "Wall" concept, where users can "share" content in the form of written "status updates," uploaded pictures, video, audio, or attached hyperlinks; "tag" "friends" in their posts; "check-in" at certain locations; self-identify "likes"; and establish relationships with other users. *But see*, Dan Schawbel, *Is It a Bad Idea to Friend Co-workers on Facebook? How About Your Boss?* TIME (Jan. 17, 2012), http://business.time.com/2012/01/17/is-it-a-bad-idea-to-friend-co-workers-on-facebook-how-about-your-boss/.

> their personal computers. One has linked his company-provided email address to his Twitter account, but he has protected his tweets so that only his followers can see what he writes. All three have linked their personal email addresses to their Facebook profiles. All of them have the highest level of privacy protection on their Facebook accounts. Moreover, they can choose among their friends who can and cannot see certain Timeline content.
>
> The firm does not explicitly prevent employees from using their company-provided laptops or smartphones for social networking purposes at work or home. Every firm employment contract, however, contains a boilerplate clause stating, "All content created, stored or exchanged on hardware and software provided to the employee by Law Firm is the property of Law Firm."
>
> When Law Firm burns to the ground, the partners suspect a disgruntled employee is responsible. Prosecutors are now seeking access to all related content, messages, and chats contained on the three externs Facebook accounts.

The scenario allows Career Service Office employees to explore issues such as (1) the terms of an employment contract, (2) company policies, especially those concerning granting access to personal social media content, and (3) ethical behavior in a workplace setting, at a minimum.

Other training and counseling sessions can include information about how traditional background checks that are performed on potential employees may now include Facebook pages.[222] CSO personnel may suggest having students perform a search of their name on multiple sites to unearth the personally identifiable information a potential employer might locate.[223] In counseling students about what they should post, and what they should (and can) delete from an online profile, one useful exercise could be to have the students prepare a checklist based on their initial findings about themselves located by searching multiple Internet sites.[224]

a. Problematic Content - Generally

Students can be advised about how to best clean up their online presence. They might be advised to check for variations with a middle name and initials to ensure that they have located all personal information and could be advised to remove images as well as friend postings naming them. Additionally, CSO

222. Bridget Miller Friday, *Using Facebook for Background Checks*, HR DAILY ADVISOR (June 20, 2014), http://hrdailyadvisor.blr.com/2014/06/20/using-facebook-for-background-checks.

223. Susan Adams, *6 Steps To Managing Your Online Reputation*, FORBES (March 14, 2013 6:17PM), http://www.forbes.com/sites/susanadams/2013/03/14/6-steps-to-managing-your-online-reputation/.

224. David D. Perlmutter, *Your Unofficial Job-Application Checklist*, CHRON. HIGHER ED. (Nov. 19, 2012), http://chronicle.com/article/Your-Unofficial/135798/.

personnel might suggest that students check for tweets or blog posts conveying negative comments about an authority figure, over-the-top political comments, sloppy or rambling content, or a disjointed discussion blog post, friend swipes[225] that appear to be compromising, or comments from third-parties about poor job performance.[226]

Mindsets are changing, and the Career Services Office will know what is and is not important to keep or remove. Students should have that discussion with those professionals. Improving a student's professional image is vital.

In order to remove damaging content, students might be counseled to begin by contacting the few friends who have posted information that is deemed inappropriate and request that it be removed. Other requests to remove damaging content posted by people not known personally could be made by a simple request – followed by a demand letter threatening defamation or another legal action.[227] And, after cleaning up a variety of social media sites, a student might consider creating a Google alert for her name and common variations so that anything that appears at any time can be taken down, cleared up, or contextualized."[228]

Building a positive profile is the next part of the process that most CSO personnel will recommend. This should include crowding out the harms to a person's reputation. Students should start by coordinating positive images on all social media sites after removing the negative information. A Google score will rise and will edge out the bad reputational items. Students should then proofread anything added or edited to ensure that that professional image remains pristine.[229]

5. Best Practices in Law Schools – Libraries

Libraries play a central role in working with students in the area of privacy protection and create privacy codes and policies for students, employees, and others using library resources. Since libraries sign contracts that are not always favorable to library patrons, they are well versed in protecting patron privacy.[230] Librarians can offer a variety of information to their institution about privacy principles which must be followed as well as ensure that the contracts the school

225. Friend swipes are social discovery application tool that facilitates communication and potential dating opportunities as a person swipes through a virtual stack of photos or communications looking for new friends.

226. *Supra note 224.*

227. *Id.*

228. *Id.*

229. *Id.*

230. April Glaser and Alison Macrina, *Librarians Are Dedicated to User Privacy. The Tech They Have to Use Is Not*, SLATE MAG. (Oct. 20 2014 12:33 PM), http://www.slate.com/blogs/future_tense/2014/10/20/adobe_s_digital_editions_e_book_software_and_library_patron_privacy.html.

signs prohibit vendors from collecting any personal information unless a student or user authorizes it.[231]

If students are interested in helping to draft a school-wide privacy policy or create a set of best practices, librarians can provide information about key areas of data intrusion, privacy intrusions, information accuracy issues, property rights to information, and information accessibility issues.[232] Although the lists that follow are not extensive, they outline privacy topics that could easily be discussed in a series of short sessions during brown bag presentations or table talks during a law school lunch hour.

A training program could include:

(1) a policy discussion about privacy risks and risk management,

(2) library privacy practices, from circulation to managing DMCA rights,

(3) how to review a terms of services agreement with a vendor and make appropriate edits and other changes,

(4) property rights in library materials and in user generated content, and

(5) accuracy, authenticity, and accessibility of information.

Many librarians are also trained in improving processes and in analyzing issues surrounding information privacy risks. A second set of training sessions could include:

(1) discussions about common (and sometime uncommon) information risks such as identity theft, online and physical stalking, embarrassing posts, price discrimination and blackmailing[233] and

(2) librarians can also illustrate how to create tables or grids to analyze risk and mitigate it.

Librarians can also offer training sessions about potential harm to attorney and client confidentiality from commercial tracking of online research.[234] The training session can include developing the following ideas with the audience:

---

231. *Id.*

232. Privacy Issues involve collecting, storing and disseminating information about individuals. Accuracy Issues involve the authenticity, fidelity and accuracy of information that is collected and processed. Property Issues involve the ownership and value of information. Accessibility Issues revolve around who should have access to information and whether they should have to pay for this access. *See* R. KELLY RAINER AND EFRAIM TURBAN**,** INTRODUCTION TO INFORMATION SYSTEMS: SUPPORTING AND TRANSFORMING BUSINESS 63 (2009).

233. Risk mitigation occurs when an organization takes concrete actions against risk and develops controls to prevent identified threats from occurring, and a means of recovery should the threat become a reality. Discussions could include asking questions about when risk acceptance is tolerable, and when the organization should accept a potential risk and absorb any damages that occur by possibly limiting it or transferring it via an insurance mechanism.

234. Anne Klinefelter, *When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking,* 16 VA. J.L. & TECH. 1 (2011).

(1) Best practices for students and attorneys in protecting commercial tracking of their online research.

(2) A discussion about ways to encourage online industry support for confidentiality.

(3) How to seek stronger legal protections for online confidentiality if industry encouragement fails.[235]

(4) Ways to locate and analyze vendor policies online.[236]

(5) Ways to solicit personalized recommendations about books that a student or other library user places online at a vendor site without breaching confidentiality of personal information.[237]

(6) Discussion about the definitions of the terms "appropriation," "modification," and "re-appropriation" as they apply to privacy and personal information.

(7) Explanations and group discussions about "the Internet of Things (IoT)"[238] its impact on corporate liability, risk management, and the impact of the IoT on privacy.

(8) Discussions about how librarians protect the privacy of checkout records.[239]

(9) Protecting privacy in RSS feeds.

Finally, librarians are generally experts in tagging records, indexing, and adding metadata to information resources. As such, they are also very adept at explaining many issues such as the archiving, sharing, and valuation of personal information that occur when companies use data mining techniques to analyze a user's information requests. The training sessions they could offer about indexing systems and data mining can include:

(1) Defining and identifying data mining and behavioral marketing techniques used by data mining companies.[240]

---

235. *Id.*

236. *See, e.g.*, Trina J. Magi, *A Content Analysis of Library Vendor Privacy Policies: DO They Meet Our Standards?*, 71 COLL. & RES. LIBR. 254 (2010) (reviewing several standards for reader or researcher privacy including library organization standards, testing online research systems' promises for compliance, and reporting aggregate statistics); *see* The American Library Association ("ALA") Office of Intellectual Freedom's "Campaign for Reader Privacy" pursuing conformity to the ALA ethical commitment to confidentiality of library use. *Office for Intellectual Freedom*, AM. LIBR. ASS'N, http://www.ala.org/offices/oif(last visited Sep. 5, 2010).

237. *See* Marc Parry, *As Libraries Go Digital, Sharing of Data Is At Odds With Tradition of Privacy*, CHRON. OF HIGHER ED. (Nov. 5, 2012), http://chronicle.com/article/As-Libraries-Go-Digital/135514/.

238. *Supra* note 88.

239. Meredith G. Farkas, *Social Software in Libraries: Building Collaboration, Communication, and Community Online*, 12 INFO. TODAY 4, 140 (2007).

240. Scott, *supra* note 14; Martha C. White, *Big Data Knows What You're Doing Right Now*, TIME (July 31, 2012), http://business.time.com/2012/07/31/big-data-knows-what-youre-doing-

(2) Discussions of some of the current privacy legislative protections available to students and businesses.

(3) Discussion of the FTC's Fair Information Practices principles and their application to many settings.

(4) Identifying trust-based Internet providers.[241]

6. Best Practices in Law Schools – Technology Services Training Ideas

Technology training sessions about privacy issues and ways of avoiding them are critical to the success of law students who will transition in to the work force in a few short years. Good habits and information about how to clean up or at least tidy up files and information that can be access and could lead to reputational injuries are necessary. New paradigms, security controls, and other updated information about preventing privacy breaches should be presented, and topical areas and presentations may need to be updated every semester since privacy is a fast moving target. Training sessions for students can include a variety of information and exploration of ideas. Although this list is not extensive it presents privacy and other related topics that could easily be presented in a series of short sessions over a two semester time frame.

Some training sessions could include:

(1) A demonstration on how to scrub a student's digital footprint.[242]

(2) Building a reputation building website of your own outside of Facebook.[243]

(3) How to perform a privacy audit of your online reputation.[244]

(4) Protecting privacy on mobile devices.[245]

(5) How to conduct an information audit to discover information systems that expose personal information through any website system's inputs, outputs and processing features.

---

right-now/.

241. Sudhir Aggarwal et al., *Trust-Based Internet Accountability: Requirements and Legal Ramifications*, 13 J. INTERNET L. 3, 6–7 (2010).

242. Carolyn Thompson, *Google Yourself: Colleges Help Students Scrub Online Footprints*, HUFFINGTON POST/TECH (May 21, 2015), http://www.huffingtonpost.com/2012/12/26/google-yourself_n_2366413.html.

243. Sara Grossman, *Web-Hosting Project Hopes to Help Students Reclaim Digital Destinies*, CHRON. OF HIGHER ED. (July 25, 2013), http://chronicle.com/blogs/wiredcampus/web-hosting-project-hopes-to-help-students-reclaim-their-digital-destinies/45035.

244. Jennifer Howard, *Worried about Message, Colleges Scrutinize Social Media*, CHRON. HIGHER ED. / TECHNOLOGY (Sep. 23, 2013), http://chronicle.com/article/Worried-About-Message/141773/.

245. *See* articles to hand out in training sessions, such as: Kimberly Palmer, *10 Ways to Keep Your Phone Safe*, US NEWS – MONEY (Jan. 13, 2015), http://money.usnews.com/money/personal-finance/articles/2015/01/13/10-ways-to-keep-your-phone-safe.

(6) Regular training sessions on how to access and change privacy settings on a variety of social media sites.

(7) Demonstrations of Snapchat [or any newer technology that is on the bleeding edge] followed by a discussion of the privacy breaches it can bring about because it has not yet been well tested.

Faculty training about privacy offers a different set of challenges. While some faculty at any institution may be on the cutting edge of technology and privacy issues, others may lag far behind. Different types of privacy information should be considered based on questions faculty are asking the IT staff and presentations should be tailored accordingly. Sessions could include the following topics:

(1) A discussion about the benefits and detriments of maintaining a digital online presence.[246]

(2) A presentation on how to make online social networks work for different faculty at different stages in the promotion and tenure process and how privacy could be affected in terms of using blogs or Facebook pages to promote scholarship. A discussion might take place afterwards about the advantages and privacy disadvantages of using sites like YouTube to augment teaching with blog-enabled interactive assignments.[247]

(3) A demonstration by IT staff along with a knowledgeable faculty member about how to control your own digital content through blogs, Facebook, Twitter, etc. as self- publishing tools.

(4) Information audit training which can guide faculty to regularly implement best practices in searching for their digital persona and how to limit or erase that persona.

(5) Regular training sessions on how to access and change privacy settings on a variety of social media sites.

(6) Regular trainings about how to track new "big data" and data mining threats to privacy and avoid them.[248]

(7) Protecting privacy on mobile devices.[249]

(8) How to prevent unwanted intrusions into locational settings information.

---

246. Kelli Marshall, *How to Maintain Your Digital Identity As An Academic*, CHRON. HIGHER ED. VITAE (Jan. 9, 2015), https://chroniclevitae.com/news/854-how-to-maintain-your-digital-identity-as-an-academic.

247. David D. Perlmutter, *Facebooking for the Tenure Track*, CHRON. HIGHER ED. (Sep. 4, 2009), http://chronicle.com/article/Facebooking-for-the-Tenure/48218/.

248. Universities are now tracking and data mining student activity – with student permission. *See, e.g.*, Goldie Blumenstyk, *Blowing Off Class? We Know*, NY TIMES OPINION PAGES (Dec. 2, 2104), http:nyti.ms/12pxZb6.

249. Palmer, *supra* note 245.

VI. CONCLUSION

Every person has an online identity and leaves a digital footprint with every digital/virtual action he or she takes; intentionally or not. Social media users appear to desire more control over privacy in their own personal information, posts, and in their locational settings. The sheer number of news, blog, and media posts about online privacy reveal a revitalized interest in at least some type of privacy protection for information posted on social media sites. A Consumer Bill of Privacy Rights has been proposed by President Obama, but is unlikely to be formally passed into a legislative scheme in the near future due to business concerns over the cost of implementation and struggles over which executive body should enforce it.[250] Other cutting-edge proposals remain untested in the courts.

When the lack of control over personally identifiable information affects society and individual's digital reputations, consumers are bound to demand change. However, proposals aimed at protecting personally identifiable information that is aggregated by commercial entities may take years to catch up to the current state of technology. In large part, "privacy law has become the law of broken promises and the law of inadequately disclosed information practices."[251]

If a critical goal for most consumers who have posted information for over twenty years without realizing the consequences is to take away their regrets over ill-advised posts or pictures, or if it is to moderate the amount and types of personal information they place in social media settings,[252] then this author's proposal may be the only way to accomplish such a goal in a systematic and measured fashion. An educational curriculum and training techniques should be instituted quickly and systematically, and can be designed to cover the entire kindergarten through post-graduate spectrum.

250. *See* Astringer, *supra* note 39.

251. CHRISTOPHER WOLF, A *Practicing Privacy Lawyer's Perspective on Use Analysis as a Way to Measure and Mitigate Harm*, 12 COLO. TECH. L.J. 353, 354(2014).

252. *Id.* at 355.