1-1-2014

Legislating Our Reasonable Expectations: Making the Case for a Statutory Framework to Protect Workplace Privacy in the Age of Social Media

David Miller

LEGISLATING OUR REASONABLE EXPECTATIONS: MAKING THE CASE FOR A STATUTORY FRAMEWORK TO PROTECT WORKPLACE PRIVACY IN THE AGE OF SOCIAL MEDIA

DAVID MILLER

INTRODUCTION: THE MILLENNIAL GENERATION HAS A PROBLEM

"We lived on farms, then we lived in cities, and now we're gonna live on the internet!"[1]

Perhaps no other area of the law has struggled to adapt to the internet's exponentially increasing ubiquity and permeation into citizens' everyday lives than fundamental privacy protection. It is not news that the internet has become the definitive first stop in the quest to read the latest news, check the most recent sports scores, and research any topic. Critically, however, with the exponential rise of online social networks (OSNs), the internet is also where people share the most personal, intimate details of their lives. Extremely popular services such as Facebook[2] provide forums to post pictures, message friends, and engage in social commentary in ways that are as novel as they are easy to use. Never before have the vast majority of citizens possessed such a public mouthpiece to broadcast such seemingly private details, and never before has such a mode of personal expression become a social necessity for so many so quickly.

However, accompanying this dramatic increase in the dissemination of personal information are profound difficulties in applying current workplace privacy protections to OSN use. In fact, the Supreme Court recently opined that these "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior" and thereby make it so "the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize them as reasonable."[3] Noting these tough questions, the Court did what has all-too-often been the norm for privacy cases and held "[t]hough the case touches issues of farreaching significance . . . it can be resolved by settled

---

1 The Social Network (Columbia Pictures 2010)(quoting Sean Parker as played by Justin Timberlake).

2 *See* Geoffrey A. Fowler, *Facebook: One Billion and Counting*, WALL STREET JOURNAL, Oct. 5, 2012, at B1. (Reporting that Facebook officially surpassed one billion monthly active members on September 14, 2012).

3 City of Ontario v. Quon, 130 S.Ct. 2619, 2629-30 (2010).

principles."[4] These "settled principles," of course, remain amorphous—predicated on malleable, abstract conceptions that are fundamentally unsettled in their application to the millennial generation and OSNs.

The unfortunate reality is that OSN use is setting social norms, including those regarding workplace privacy expectations, at far too fast a pace for the existing legal protections.[5] In the private employer context, devoid of the baseline protection of the Fourth Amendment (and to a lesser degree certain First Amendment protections), the legal enforcement of privacy protections regarding OSNs takes on even further complexity. Court precedent and current statutory protections are altogether outdated, inadequate, and unprepared to recognize the seismic societal shifts consequence to OSNs.

Concurrent with this murky protection, private employer use of OSN information in the hiring process, monitoring current employees, and making disciplinary decisions are all on the rise.[6] These trends are mirrored in education, especially at the high school and college levels.[7] Indeed, survey data from the Society for Human Resource Management reported that in 2011 56% of employers reported use of social media in the hiring process, an increase from 34% in 2008.[8] Employers undoubtedly have legitimate interests in learning about prospective candidates they wish to hire and shielding themselves from liability against negligent hiring down the line amongst other concerns. Furthermore, employers also possess a tremendous need to ensure their current employees do not damage the reputation of the company, gain access to or publicize critical financial information or trade secrets, use employer provided resources for personal purposes, and ensure workplace morale by preventing overt criticism of the business. The legal question concerns the point at which the methods of OSN information acquisition and surveillance employers engage to effectuate these goals intrude upon the privacy rights of employees and applicants. There is an inevitable tension, and thus far the scales tip grossly towards the employers.

---

4 *Id.* at 2624.

5 *See generally* Patricia Sanchez Abril, Avner Levin, & Alyssa Del Riego, *Blurred Boundaries: Social Media and the Twenty-First Century Employee*, 49 AM. BUS. L.J. 63 (2012) [hereinafter *Blurred Boundaries*].

6 Ian Byrnside, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 457 (2008) ("It is clear that employers are increasingly checking the social networking profiles of their applicants and that those applicants may suffer as a result of the information they have posted on the Internet.").

7 *Id.*

8 Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, 60 THE ADVOC. (TEXAS) 8, 9 (2012).

Due to their unique nature, OSNs represent more than merely the next technological difficulty in the long chain of difficult privacy law adaptations[9]. Rather, because of the interplay between customizable privacy settings on OSNs themselves, the distribution of content to many people as opposed to direct one-on-one discussion, and the sheer number of people in the network itself many of the traditional privacy analysis factors do not apply[10]. OSNs remove physical space and blur the line between public statements and personal items of self-identification intended to remain outside the bounds of inquiry[11].

Recently, academic research has elucidated the notions of privacy expectations of OSN users[12]. The apparent discord between the unwavering desire to post private information on OSNs and the adamant intrusiveness felt when that information falls into particular hands or is used for particular purposes is resolved by the theory of network privacy.[13] Network privacy posits "information is considered by online socializers to be private as long as it is not disclosed outside of the network to which they initially disclosed it, if it originates with them, or as long as it does not affect their established online personae, if it originates with others."[14]

Put another way, the OSN user notion of privacy is grounded in *access*: it is invasive of protected privacy interests when particular information reaches unintended audiences without permission based on the contextual appropriateness of that access. OSN users simply desire what was at the heart of privacy advocacy in Brandeis and Warren's seminal article originally arguing for its legal basis here in the United States[15] - the ability to maintain separate spheres in ones life between what is public and what is private. This notion of autonomy over the audience

---

9 *See* Patricia Sanchez Abril, *Private Ordering: A Contractual Approach to Online Personal Privacy*, 45 WAKE FOREST L. REV, 689, 701 (2010) ("To date, however, the law has suffered from dubious applicability in the online social world.") [hereinafter *Private Ordering*].

10 *See* Patricial Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 5 (2007) ("New technologies have enabled novel social situations that generate privacy harms and concerns that were unforeseeable. . .") [hereinafter *Privacy Torts*].

11 *Id.* at 3.

12 *See* Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001 (2009). [hereinafter *Two Notions*]. The findings and discussions in this article are foundational to the arguments made in this piece and form the basis for the theoretical underpinnings of why OSN user privacy expectations are indeed reasonable. This work has been cited thoroughly in the academic literature on OSN privacy and its valuable contribution to the discourse on this topic cannot be overstated.

13 *Id.* at 1002.

14 *Id.*

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

for which certain expressions are intended was central to their influential writing: "In every such case the individual is entitled to decide whether that which is his shall be given to the public."[16] Thus, while OSNs have made certain information easier to gather on an applicant or employee, this should not be taken as an excuse to legitimize the departure from long established principles of privacy law and policy. Thus, the key to protecting privacy interests surrounding OSNs in the workplace moving forward is having a law grounded in clear distinctions regarding employer and employee access to the wealth of contextual information shared on OSNs.

Critically, to effectively protect the privacy interests of employees and the legitimate business interests of employers the enactment of legislation is required. In the wake of a failed federal effort[17], a recent trend of states, beginning with Maryland[18], passing laws that for the first time explicitly draw lines for what private employers can and cannot do in the realm of OSNs in the workplace is underway. This is the greatest evidence so far of the access theory in action-and the results have been positive. While this trend is certainly encouraging, much more needs to be done.

This note will make the case that it is only through explicit federal legislation, and not reliance on the courts, private employers, the states, or OSN company policies to strike the proper balance between individual privacy and employer interests. Part I discusses the network privacy theory, analyzing it as the extension of traditional notions of reasonable privacy expectations and their Constitutional underpinnings to digital age OSN use. Next, Part II outlines in detail the current state laws that have been passed, comparing differences in methodology and the resulting consequences. These laws reflect for the first time a proactive approach predicated on the access theory of privacy and the direction the law must continue on. Part III provides a discussion of the tangential privacy protections currently in place for private employee OSN use to illustrate their woeful inadequacy when translated to OSNs while noting there are encouraging trends in the law. Finally, Part IV concludes that the time is ripe for Congress to pass uniform, comprehensive legislation in this field

---

16 *Id.* at 199.

17 Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012) [hereinafter "SNOPA"]. The bill failed to pass along party lines due to Republican opposition and never made it out of committee, but has since been reintroduced in the 113th Congress. Eliot Engel, Jan Schakowsky, & Michael Grimm, *SNOPA addresses online privacy concerns*, THE HILL'S CONGRESS BLOG: WHERE LAWMAKERS COME TO BLOG (May 15, 2012, 1:46 PM), http://thehill.com/blogs/congress-blog/technology/227509-snopa-addresses-online-privacy-concerns.

18 MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

to provide a mandatory minimum for workplace OSN privacy. This approach helps maintain employee privacy while employers shield themselves from potential discrimination suits under Title VII of the Civil Rights Act[19] and claims under the National Labor Relations Act (NLRA)[20]. Ultimately, this note will offer reasonable uniform legislative minimum standards to provide the best outcome for all parties involved so that lines may continue to be drawn and protection of privacy expectations may flourish in the age of social media.

PART I: NETWORK PRIVACY AND THE ACCESS THEORY OF REASONABLE EXPECTATIONS

The fact that privacy law in the United States is struggling to adapt to critical technological changes in society is neither new nor surprising.[21] Since the constitutional recognition of privacy as a fundamental right[22] its doctrinal development often raises more questions than it answers. The twin pillars of the generally reactionary nature of United States common law and having grounded privacy protections in societal and individual "reasonable expectations" created a system wherein the law must consistently adapt to social norms that technological innovation has already exerted its considerable influence upon. However, contrary to what certain academics and industry leaders have posited,[23] the purported disconnect between OSN users expectations of privacy online and the core principles of American privacy law ideals are not so fundamental.

---

19 42 U.S.C. § 2000-e-2 (2012).

20 National Labor Relations Act, 29 U.S.C. §§ 151-169 (2012).

21 Blurred Boundaries, *supra* note 5, at 698 ("If we cannot always agree on what is properly private subject matter in the physical world, consensus online is surely impossible in a universe devoid of physical boundaries, traditional culture, and shared understandings among its participants.").

22 ". . . specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy." Griswold v. Connecticut, 381 U.S. 479, 484 (1965). The "penumbra" here, the right to marital privacy, was "formed by emanations" from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. Justice Douglas's majority decision garnered seven votes, but the penumbra rationale merely five as Justices White and Harlan wrote concurrences grounded in the due process clause, the latter of which would form the doctrinal basis for recognition of further unenumerated privacy rights. Justice Goldberg wrote a concurrence joined by Justices Brennan and Chief Justice Warren relying on the Ninth Amendment as an alternative source of the fundamental privacy right. Justices Black and Stewart each dissented. Needless to say, the Court did not mark a clear path upon which constitutional privacy jurisprudence was to develop.

23 Facebook founder, Chairman and CEO Mark Zuckerberg himself has asserted internet privacy is no longer a social norm. Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN (JAN. 10, 2010), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

Academics and legal scholars have long debated the definition of privacy, and as a result the rationales for protection of the right.[24] Despite the lack of a unanimous definition, colloquially or legally, as to precisely what privacy *is*, the law remains a function of citizen expectations of *it* and whether society objectively finds *those expectations* reasonable.

Without an explicit textual basis in the Constitution the wide breadth of "reasonable" expands further into private sector norms without the cognizable limits imposed by other constitutional provisions[25]. Because all of these protections depend in part on an actual expectation of privacy "that society is prepared to recognized as reasonable," private employers retain the right to determine what *in fact* the reasonable expectations of privacy its employees retain through the issuance of company policies and rules[26]. From its inception, United States constitutional privacy protection created specific "zones of privacy" stemming from the "penumbras" of other rights, and "emanations of guarantees" made textually explicit[27]. Therefore, because privacy is defined solely in terms of individuals right to privacy *in a certain capacity*[28] all ensuing legislation protects privacy in narrow circumstances against particularized, and mainly governmental intrusions. This dichotomy presents the permanent difficulty of privacy law in common law tort jurisprudence, legislative proposals and enactments, and constitutional interpretation: what is the foundational premise behind what "reasonable expectations of privacy" the government, the Constitution, and courts aim to protect? In other words, what is the underlying link between these "zones" of privacy and how do citizens, society, and the courts inform their "reasonable expectations" before they gain legal recognition?

Legal analysis summarizes the approaches taken by modern, Western, democratic states by generally placing them in two broad categories:

---

24 *See generally* Two Notions, *supra* note 12 at 1006-1017.

25 "Private sector employees do not enjoy any Fourth Amendment rights vis-à-vis searches or surveillance by their employers under the U.S. Constitution. Any work-related privacy rights that private employees may have are derived from a common law right to privacy developed among the states during the twentieth century." Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, Berkeley Tech. L.J. 979, 990 (2011).

26 "Employers can destroy actual expectations through the use of notices and consent forms." *Id.* at 991.

27 *Griswold*, 381 U.S. at 484-85.

28 "The United States has taken a sectoral approach to privacy, enacting laws that apply to specific industries and practices. . .This patchwork approach is in contrast to the European nations, Canada, Australia, New Zealand, and Hong Kong." Beth Givens, Open Presentation at Santa Clara University Symposium on Internet Privacy (Feb. 11-12, 2000)(transcript available at https://www.privacyrights.org/ar/expect.htm). Both the "penumbras" and due process rationales of *Griswold* adhere to this sectoral approach.

privacy as a protection of control and privacy as a protection of dignity.[29] The control, or autonomy approach, theorizes that "When individuals are allowed to act with autonomy and are treated as ends in and of themselves, their human rights, dignity, and liberty are assured."[30] The autonomy theory revolves around the value people place on the protected *choice* for people to "barter away their privacy" in specific circumstances.[31] In a similar, but functionally distinguishable manner, the privacy as a protection of individual dignity approach emphasizes the personal development of the inner self and personality.[32] Thus, an individual maintains several "public personas": each are accessible only by specific constituencies in specific contexts and it is the protection of the individual's inability to freely manage disclosure of these "personas" that forms the impetus for privacy protection.[33]

United States privacy law is often said to fit within the autonomy theory. The emphasis placed on the protection of free speech and the difficulty in judicially assessing the merits of someone claiming to have been "shamed" or "disrespected" by a privacy violation arguably make control-based protections of privacy more practical[34]. For example, in tort law to win a claim of public disclosure of private facts the plaintiff generally must show the defendant publicized a private fact that was not of legitimate public concern, where such disclosure was highly offensive to a reasonable person.[35] Thus, the inquiry turns on the "reasonable expectations" of the victims in guarding that particular private fact (provided it is not of legitimate public concern), inherently giving much weight to whether or not the plaintiff relinquished control to therefore impact how reasonable the expectation of it remaining private remained over that fact[36].

On the other hand, the European Union (EU) provides an excellent illustration of the privacy as dignity theory promoting particular policy[37]. Under Article 8 of the European Union Convention on Human Rights citizens are protected from state interference with "his private life and

---

29 Two Notions, *supra* note 12 at 1008.

30 *Id.*

31 *Id.*

32 *Id.* at 1013.

33 *Id.*

34 Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 231 (2012) [hereinafter Henderson].

35 Restatement (Second) of Torts § 652D (1977).

36 *See* Two Notions, *supra*, note 12 at 1010-1011.

37 *Id.* at 1014.

family life, his home and his correspondence."[38] Moreover, "There shall be no interference by a public authority with the exercise of his right [to private life] except such as is in accordance with the law."[39] Thus, the law takes a hardline approach to individual dignity interests as opposed to the choice of disclosure, setting up privacy protection as the default rule. It is the concern with casting the private lives of citizens as "off limits" from government scrutiny that is reflected by the privacy legislation. This disconnect between the approaches can be seen in Europe's reluctance to provide lessened privacy protection for celebrities and public figures, while the US makes this an explicit part of its libel and slander laws[40]: what expectations are "reasonable" are again a product of the disclosure choice and public figures in a sense have forfeited a great deal of this choice[41].

However, it is disingenuous to pigeonhole the US patchwork approach to privacy protection as neatly fitting in the autonomy sphere entirely at the expense of the dignity sphere. Not only are the concepts so intertwined to make this distinction often superfluous in practice, but US privacy law also has roots in aspects of the dignity theory. Warren and Brandeis' aforementioned landmark article famously discussed privacy as simply "the right to be let alone."[42] The authors noted that "solitude and privacy have become more essential to the individual" and therefore the law must protect the privacy interests of individuals' "inviolate personality" in a clear formulation of what is now referred to as the dignity approach.[43] But the initial proponents of privacy protection went on to assert that the law "secures to each individual the *right of determining*, ordinarily, to what *extent* his thoughts, sentiments, and emotions shall be communicated to others."[44] This right to determine the "extent" of communication adheres precisely to network privacy and the particular difficulties of OSNs, notably the practical inapplicability of the wholly binary distinction between "private" and "public" to determine reasonable expectations of privacy.

Federal law has generally addressed privacy concerns only tangentially

---

38 European Convention on Human Rights. art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

39 *Id.*

40 New York Times Co. v. Sullivan, 376 U.S. 254, 280 (Establishing "actual malice" standard for public officials to recover in libel actions without contravening First Amendment protections).

41 Two Notions, *supra,* note 12 at 1015-16.

42 Warren and Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193, 193 (1890).

43 *Id.* at 201.

44 *Id.* at 198 (emphasis added).

as they relate to other harms[45], and the inevitable inconsistencies render it impossible for one theory to dominate the other. Inevitably, the protection of individual autonomy of what information is disclosed remains a function of dignity for if the exposure of that information did not negatively affect the individual than no protection would be sought. In the tort of private disclosure example, *supra*, the determination of reasonability in the privacy expectation is "highly dependent on the nature of the space or information invaded, the circumstances surrounding the breach, and the prevailing social norms."[46] Thus, while surely not an all-encompassing *right to dignity* as enacted in the EU, the privacy infringement is predicated on *both* protecting autonomy of choice in disclosure *and* on that choice itself as the ultimate protection for dignity based on prevailing social norms and individual circumstances. In other words, when the choice has been breached by an unwanted disclosure, the privacy violation results in dignitary harm to the individual by stripping them of this choice.

Therefore, in essence, US privacy regulation is grounded in concepts of both autonomy and dignity. The "right to privacy" that Warren and Brandeis sought in 1890 has never materialized in the form of an explicit, all-encompassing piece of legislation or even a determination that it is constitutionally provided in the form they sought[47]. Rather, the subsequent "zones of privacy" show the accurate paradigm through which to view the foundation of privacy expectations in the US is that of access. The protection of individual privacy is a function of protecting dignity through the maintenance of autonomy: in other words, privacy protection aims to prevent access to certain items by certain people in certain contexts by placing the onus on the individual to reasonably control the perceived potential dignitary harms based on reasonable expectations of

---

45 Federal statutory examples include the Fair Credit Reporting Act of 1970 (regulating consumer financial information), the Privacy Act of 1974 (regulating use of personal identifying information in federal records), the Cable Communications Policy Act of 1984 (prohibiting cable television providers from disclosing personally identifiable information and allowing customers to view and verify this information), the Electronic Communications Privacy Act of 1986 (extending government wiretap restrictions to electronic computer transmissions), the Video Privacy Protection Act of 1988 (preventing wrongful disclosure of video tape rental and sale records), the Telephone Consumer Protection Act of 1991 (restricting telephone solicitation and the use of automatic dialing systems), the Drivers Privacy Protection Act of 1994 (governing privacy and disclosure of personal information possessed by state motor vehicle administrations), and the Children's Online Privacy Protection Act of 1998 (setting privacy guidelines for personal information collection concerning children).

46 Two Notions, *supra*, note 12 at 1010-11.

47 "We must therefore conclude that the rights, so protected, whatever their exact nature are not rights arising from contract or from special trust, but are rights as against the world." Warren & Brandeis, *The Right to Privacy*, at 213.

privacy. In other words, network privacy. Once one accepts that access, autonomy, and dignity are inevitably intertwined in the reasonable expectation of privacy analysis under the US system, the theory of network privacy becomes the logical extension of this notion to the most difficult technological challenge to individual privacy yet–the internet and OSNs.

OSN user behavior and research affirm access as the foundation for reasonable expectations of privacy[48]. Studies indicate that overwhelming majorities of OSN users are well aware of the ease in which unintended audiences may see posted content,[49] consistently use privacy settings available[50], and yet will not consider eliminating OSN use for the sake of increased privacy[51]. In fact, a majority of OSN users in a recent survey agreed with the statement, "It is not right when people can have access to information not intended for them."[52] The problem lies in the inherent legal assumption that voluntary disclosure extinguishes reasonable expectations to the world–an assumption entirely foreign to millennial OSN users. Likewise, these notions are not contradictory, but rather reflect first and foremost the social necessity that OSNs have attained in that their continued use is functionally equivalent to attaining employment. Furthermore, user behavior illustrates that although users acknowledge breaches of their privacy they do not find them acceptable. Seventy-five percent of survey respondents indicated that "employer monitoring or accessing of employees' OSN profiles" is inappropriate while a similar majority said they would be "willing to *share certain* private information *openly* with employers."[53]

The distillation of OSN user behavior and academic survey data shows a desire, and arguably a perceived necessity to enjoy the social utility of OSNs with clearly defined boundaries as to *who* may view *particular* content. In essence, just as ones in-person identity means something different to one network as it does to another, individuals view their OSN personae with the same ability to segregate for various audiences-even when those groups are large in number.[54] However, users are not willing

---

48 *See generally*, Two Notions, *supra* note 12. *See also* Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12 (2011) [hereinafter Newell].

49 Two Notions, *supra*, note 12 at 1036.

50 72% of users surveyed restricted their privacy settings and 54% blocked specific people from accessing their profile. *Id.* at 1033.

51 *Id.* at 1045.

52 Blurred Boundaries, *supra*, note 5 at 100.

53 *Id.* (emphasis added).

54 Newell, *supra*, note 48 at 18.

to sacrifice OSN participation to achieve this because they generally do indeed *expect* the information posted on OSNs to remain private from unauthorized parties[55]. It is this expectation, that certain content is "off limits" from employers and prospective employers because of the decision made by the user that the law must recognize as reasonable. It is time for this "zone of privacy" to gain legal recognition as something society is willing to accept as reasonable.

PART II: LEGISLATIVE RECOGNITION, ACCESS, AND MOVING IN THE RIGHT DIRECTION

"[I]nternet users have a reasonable expectation of privacy in their social networking site communications and affairs."[56] No longer merely the battle cry of internet privacy proponents or advocacy groups, the Delaware General Assembly recognized explicitly, along with five other states, that OSN privacy expectations are reasonable, subject to harmful violation, and are in need of legislative protection. As of March 2013 Maryland[57], California[58], Illinois[59], New Jersey[60], Delaware[61], and Michigan[62] have each passed legislation that for the first time specifically targets OSN privacy and places legal restrictions on *private* institutions as to what they can and cannot do regarding prospective and current members OSN information. Maryland began the charge, and along with Illinois its law regulates private employer conduct. New Jersey and Delaware passed laws concerning higher education institutions, while California and Michigan[63] took the most comprehensive approach to regulate both employers and educational institutions. In addition, legislation to similar effect has been introduced and is pending at some

---

55 Blurred Boundaries, *supra,* note 5 at 109.

56 H.R. 309, 146th Gen. Assemb., Reg. Sess. (De. 2012).

57 MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

58 CAL. LAB. CODE § 980 (West 2013); CAL. EDUC. CODE § 99120-99122 (West 2013).

59 820 ILL. COMP. STAT. 55 / 10 (2013).

60 N.J. STAT. ANN. § 3-29 to 3-32 (West 2013).

61 DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013).

62 MICH. COMP. LAWS § 37.271 to § 37.278 (2012).

63 Michigan's legislation is arguably the most comprehensive in terms of its coverage breadth of applicable entities. It reaches all employers, public and private, as well as *any* "educational institution." The law states, "Educational institution . . . includes an academy; elementary or secondary school; extension course; kindergarten; nursery school; school system; school district; intermediate school district; business, nursing, professional, secretarial, technical, or vocational school; public or private educational testing service or administrator; and an agent of an educational institution." *Id.*

phase of the law-making process in a total of 31 states[64].

While the laws possess significant variability in many important aspects, their common thread is to effectuate the setting of reasonable privacy expectations and norms in the OSN context. Critically, the laws adhere to the access theory of network privacy in their intent and functionality through formal definitions and the creation of specific zones of privacy. The laws remove the onus from the courts to determine reasonability of certain specific behaviors in the OSN arena, and this approach represents evidence of the access theory in action. The speed and proliferation of these laws provides optimism, and is not only a massive first step towards OSN privacy protection in the workplace, but also a signal that the proper legislative course has been chartered.

A. State Legislation Predicated on Access to Protect Reasonable Expectations of Network Privacy

"Members of the workforce should not be punished for information their employers don't legally have the right to have. . .As use of social media continues to expand, this new law will protect workers and their right to personal privacy."[65] Echoing the sentiment of the Delaware General Assembly, *supra*, Illinois Governor Pat Quinn spoke those words upon signing the Right to Privacy in the Workplace Act. However, the potential legal significance of the particular legislative method of attack goes far beyond pleasant-sounding political rhetoric.

First, the proposed and enacted laws at the state level are *unanimously* aimed at precluding employer (or educational institution) access to

---

[64] As of March 2013 these states are: Maryland, Illinois, Delaware, California, New Jersey, Michigan, Arizona, Colorado, Connecticut, Georgia, Hawaii, Iowa, Kansas, Maine, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Vermont, and Washington. *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, EMPLOYER ACCESS TO SOCIAL MEDIA USERNAMES AND PASSWORDS 2013 (MAR. 6, 2013), *available at* http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx *and* NATIONAL CONFERENCE OF STATE LEGISLATURES, EMPLOYER ACCESS TO SOCIAL MEDIA USERNAMES AND PASSWORDS 2012 (JAN. 17, 2013), *available at* http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx [together hereinafter NCSL OSN Summary]. While there are significant aspects of the proposed laws yet to be enacted, the focus here is on the six states whose legislation has become law not only because it is merely speculative to analyze the proposed legislation before it is amended, let alone passed, but also because the six states form a representative sample for all of the proposals.

[65] Press Release, Illinois Government News Network, Governor Quinn Signs Legislation to Protect Workers' Right to Privacy (Aug. 1, 2012), *available at* http://www3.illinois.gov/PressReleases/ShowPressRelease.cfm?SubjectID=2&RecNum=10442 [hereinafter IL Press Release]

particular OSN information on employees and applicants[66]. After a series of news reports spearheaded by an Associated Press story[67] stirred tremendous controversy over employers asking for Facebook passwords as a precondition to employment in the hiring process, states responded swiftly with legislation. Thus, the press has characterized these laws as "password protection" or "Facebook password" bills[68], but this oversimplification clouds the fundamental impact this particular legal approach and the interests sought to protect carries with it.

States did not choose merely to prohibit employers from using OSN information for specific purposes or preclude what they find through snooping, coercion, or company policies concerning OSNs from affecting hiring or promotion decisions. The laws also do not simply say that employees reserve the right not to provide their password information if they so chose. Rather, the laws literally place certain employer access out of bounds in a legal sense. Thus, the laws provide a direct impediment on private employer conduct in an area where legitimate reasons for the conduct is at least arguable[69]. This alone is a monumental step forward to protect individual OSN privacy rights.

For example, the Maryland law provides, "An employer may not request or require that an employee or applicant disclose any user name, password, or *other means for accessing* a personal account or service through an electronic communications device."[70] In Illinois employers may not "*demand access in any manner* to an employee's or prospective employee's account or profile on a social networking website."[71] Michigan employers cannot "Request an employee or an applicant for employment to *grant access to*, allow observation of, or disclose information that *allows access to* or observation of the employee's or applicant's personal internet account."[72]

---

66 NCSL OSN Summary, *supra*, note 64.

67 Manuel Valdes, *Job Seekers getting asked for Facebook passwords*, YAHOO! FINANCE (Mar. 20, 2012, 7:55 AM), http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-080920368.html

68 *See* David Kravets, *6 States Bar Employers From Demanding Facebook Passwords*, WIRED (Jan. 2, 2013, 2:24 PM), http://www.wired.com/threatlevel/2013/01/password-protected-states/; *see also Maryland Becomes First State to OK Facebook Password Protection Bill*, HUFFINGTON POST (Apr. 22, 2012, 12:06 PM), http://www.huffingtonpost.com/2012/04/20/maryland-becomes-first-st_n_1439866.html

69 "While an appplicant's interest in keeping an OSN profile private is understandable, employers also have compelling and legitimate business interests in obtaining as much information about job applicants as possible." Alissa Del Riego, Patricia Sanchez Abril, Avner Levin, *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, 16 NO. 3 J. INTERNET L. 1, 18 (2012) [hereinafter *Password or Paycheck*].

70 MD. CODE ANN., Labor and Employment § 3-712 (West 2013) (emphasis added).

71 820 ILL. COMP. STAT. 55 / 10 (2013) (emphasis added).

72 MICH. COMP. LAWS § 37.271 to § 37.278. (2012) (emphasis added).

Of the enacted legislation, California pushes the farthest, prohibiting employers and schools from "requiring or requesting. . .to disclose a username or password *for the purpose of accessing personal social media, to access personal social media* in the presence of the employer, or to divulge any personal social media."[73] The enacted and proposed legislation uniformly contain the word "access" and use employer access as the starting point for protection[74].

This approach has major consequences. First, it makes explicit that the OSN content, and not solely the password or user information, is itself protected. It successfully shifts control to the individual OSN user, by requiring the need for a password or other means, as to what employers can and cannot see regarding their personal OSN content. Thus, through legal requirement users have a reasonable expectation of privacy in their personal OSN use that, at a minimum, requires user-created access controls to view. This differs extraordinarily from legal restrictions on what employers may *do* with specific OSN-related information after acquisition. That would not codify any newfound privacy expectations or truly disrupt workplace norms and would provide employers considerable leeway in creating ad hoc justifications for decisions influenced by OSN content.

Moreover, "the current trend for young Americans toward using social networks as a primary vehicle for effecting positive social and political change establishes social networks as the new digital age 'public square' for important discourse."[75] By conforming the laws to the network privacy theory of access-based expectations of privacy, these OSN laws acknowledge and effectively promote the benefits of OSN use in society. Research indicates that OSN users are "willing to take on acknowledged privacy risks" despite being "highly cognizant that they are relinquishing control over their information and its destination."[76] This truth, combined with the overwhelming popularity of OSNs[77] means that this is not a short-term phenomenon, but rather, the future course of critical societal discourse. The role that OSNs play in society is no longer in dispute, and by centering legislation on employer access this effectuates

---

73 CAL. LAB. CODE § 980 (West 2013) (emphasis added).

74 NCSL OSN Summary, *supra*, note 64.

75 H.R. 309, 146th Gen. Assemb., Reg. Sess. (De. 2012).

76 Two Notions, *supra*, note 12 at 1045.

77 The Delaware General Assembly estimated in May 2012 that "75% of American online adults ages 18 to 24 and 56% of American online adults ages 25 to 34 have a profile on a social network site." H.R. 309, 146th Gen. Assemb., Reg. Sess. (De. 2012).

a formal recognition of activity states wish to promote[78].

The protection of OSNs from this perspective can only be achieved with the network privacy approach. Only if the valuable uses are promoted while the potential harms, including workplace and educational privacy, are simultaneously defended may OSNs prosper at the level they need to. California emphasized this in Section 1 of its social media legislation: "The legislature finds and declares that quickly evolving technologies and social media services and Internet Web sites create new challenges when seeking to protect. . .privacy rights. . .It is the intent of the legislature to protect those rights."[79] States have adroitly refused to cabin their legislation purely to password protection, and have instead taken a firm, network-privacy based view wherein seeking access to specific user-protected content is flat-out off limits from private employers or institutions of higher learning. With this foundation, the legislation protects privacy interests and allows OSNs to proliferate in their critical role to facilitate discourse.

B. The Use of Formal Definitions

The first step any access-based approach to privacy regulation must take is to formally define specific terms and elements. This task is as essential as it is difficult. In the six states with OSN laws on the books there is substantial variance in terminology, and consequently in the implementation of the scheme of regulation.[80] Furthermore, the states take different paths to reconcile the inherent difficulty in placing legal parameters around colloquial and technological terms that are subject to change at a rapid pace. The precise definitions of terminology are significant also because it is the primary vehicle through which the scope of protection and rights are defined. A state cannot purport to regulate OSN use without first defining what OSNs are in the context of social media and the technological landscape. Again, the use of formal definitions helps inform individuals as to what privacy expectations are reasonable in the OSN context by placing boundaries around particular networks.

Maryland was the first state to pass OSN-related legislation, and

---

78 "Permitting public and nonpublic institutions of higher learning to demand that students and applicants provide access to their social networking site profiles and accounts could substantially chill the important discourse occurring on social networking sites" *Id.*

79 CAL. EDUC. CODE § 99120-99122 (West 2013).

80 NCSL OSN Summary, *supra*, note 64.

interestingly the only state not to attempt to define in any way the types of OSNs, services, or technology that falls under its purview.[81] In this sense, Maryland came closest to truly passing a "password protection" bill: "an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."[82] The terms "personal account" or "service" are not defined. Thus, Maryland potentially provides broad protection through its "other means for accessing" language, but OSN privacy protection may likewise be hindered by failing to place qualifying parameters around "personal" and "nonpersonal" accounts in an age where work life and personal life often blend together. For example, Maryland courts may eventually wrestle with the difficult question of whether business accounts unrelated to the employer's business seeking to access OSN content is truly "nonpersonal".[83]

However, Maryland did define "electronic communications device" as "any device that uses electronic signals to create, transmit, and receive information. . .includes computers, telephones, personal digital assistants, and other similar devices."[84] Delaware and New Jersey also define the term similarly[85]. All three appear attempts at providing a "catch all" for any device that may be used to gain access to a personal OSN account, but New Jersey uses the most inclusive language.[86]

Unlike Maryland, the balance of the laws do make one attempt or another to define the types of accounts, services, or sources employers or educational institutions are precluded from coercing or requesting access into. Illinois, Delaware, and New Jersey each provide strikingly similar definitions of "social networking" websites or sites. Illinois defines a

---

81 MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

82 *Id.*

83 William Carleton, *Grading the social media savvy of six state legislatures*, COUNSELOR @ LAW BLOG (Jan. 13, 2013), http://www.wac6.com/wac6/2013/01/grading-the-social-media-savvy-of-six-state-legislatures.html [hereinafter Social Media Grades] (Compiling opinions and quotations from five attorneys with internet-law based practices in assessing the six state OSN legislative efforts).

84 MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

85 "Electronic communication device means a cell phone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device, 2-way messaging device, electronic game, or portable computing device" DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013) (internal quotation marks omitted); "Electronic communications device means any device that uses electronic signals to create, transmit, and receive information, including a computer, telephone, personal digital assistant, or other similar device" N.J. STAT. ANN. § 3-29 to 3-32 (West 2013) (internal quotation marks omitted).

86 *Id.*

"social networking website" as "an Internet-based service that allows individuals to: (A.) construct a public or semi-public profile within a bounded system, created by the service; (B) create a list of other users with whom they share a connection within the system; and (C) view and navigate their list of connections and those made by others within the system."[87] Delaware's definition differs slightly, but contains largely the same elements: "an internet-based, personalized, privacy-protected website or application whether free or commercial that allows users to construct a private or semi-private profile site within a bounded system, create a list of other system users who are granted reciprocal access to the individual's profile site, send and receive email, and share personal content, communications, and contacts."[88]

This granular approach with specific criteria appears directly targeted at Facebook and services currently in existence that follow a similar model.[89] In stark contrast, California and Michigan attempted to employ a broader formulation to capture existing services as well as future ones.[90] California defines "social media" as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations" in each of its OSN-related laws, covering employers and higher education institutions.[91] The practical result is that any user-generated content a candidate or current employee/student posted to the internet that requires some level of username knowledge is protected.

This demarcation is significant, and the immensely popular Twitter service[92] provides an instructive example. Not all OSNs concern systems wherein a list of users are granted reciprocal access to ones profile. Twitter

---

87 820 ILL. COMP. STAT. 55 / 10 (2013). The New Jersey law has an identical definition. N.J. STAT. ANN. § 3-29 to 3-32 (West 2013).

88 DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013).

89 "The definition may or may not capture the essence of the next generation of social media services, but it gets granular enough so as to make meaningful distinctions. It describes (and thus captures) the way Facebook, Twitter, and Google+ work today, but the definition is narrow enough that it probably doesn't snare too many other kinds of web services." William Carleton, *Quite Possibly the World's First Statutory Definition of "Social Networking Website"*, COUNSELOR @ LAW BLOG (Jun. 21, 2012), http://www.wac6.com/wac6/2012/05/quite-possibly-the-worlds-first-statutory-definition-of-a-social-network.html

90 Jesse Koehler, *California Privacy Legislation: Wins and Losses*, BERKELEY TECH. L.J. BOLT (October 17, 2012), http://btlj.org/?p=1904 ("[T]his broad definition the legislature attempted to reach all existing and future social media services") [hereinafter Koehler].

91 CAL. LAB. CODE § 980 (West 2013); CAL. EDUC. CODE § 99120-99122 (West 2013).

92 Twitter is the fastest growing "social platform" in the world. Studies estimate the service has approximately 288 million active monthly users accounting for 21% of the global internet population. *See* TJ

involves sending out micro-blog entries with text or images in the form of "tweets" and does not readily conform to the structured peer-to-peer networking definitions offered by New Jersey, Delaware, and Illinois[93]. California eschews the specific criteria for a sweeping formulation in the hopes of capturing any and all OSN services at the expense of potentially ensnaring unintended entities as a consequence.[94]

Michigan takes this approach further and avoids defining OSNs by their "social" nature at all.[95] Instead, Michigan restricts employer and educational institution access to any "Personal Internet Account."[96] Michigan defines "personal internet account" as "an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account info, profile, display, communications, or stored data."[97] Thus, there is nothing inherently "social" about the OSN protection. Rather, anytime a user must "input or store access information" the account gains privacy protection under the law.

Significantly, Michigan alone defines "access information" in its statute: "user name, password, login information, or other security information that protects access to a personal internet account."[98] This emphasis on user control falls directly in line with network privacy and an access-based approach. As long as the user has employed any measure, likely to be some variant of login credentials, to prevent unwanted third party access the OSN content is legally protected. Therefore, the Michigan law "also includes bank websites, online ticketing sites, message boards, Dropbox, and virtually every other site somebody could theoretically log into and store private information."[99] Consequently, the user exclusively determines the legal enforceability of privacy protection for OSN content in Michigan, so long as the particular service in question has access-control features.

McCue, *Twitter Ranked Fastest Growing Social Platform In The World*, FORBES (Jan. 29, 2013, 4:01 AM), http://www.forbes.com/sites/tjmccue/2013/01/29/twitter-ranked-fastest-growing-social-platform-in-the-world/.

93 TWITTER ABOUT, https://twitter.com/about (last visited Mar. 8, 2013).

94 *See generally* Koehler, *supra*, note 90.

95 MICH. COMP. LAWS § 37.271 to § 37.278 (2012).

96 *Id.*

97 *Id.*

98 *Id.*

99 Social Media Grades, *supra*, note 83.

C. Establishing "Zones of Privacy"

Formal definitions provide the baseline of protection, but state legislatures also must grapple with the vexing question of *how* and *when* to protect privacy interests of OSN users. They must, in effect, cabin off certain "zones" of privacy by taking what they have defined and applying restrictions on employer and educational institution behavior in relation to them. As noted in Part II-A, *supra*, the states have unanimously used access to certain content as the threshold rationale, but what particular "zones" of privacy the legislation creates varies considerably.

Each law prohibits some variation on employers and educational institutions ability to "request or require" any "user name, password, or other means for accessing" current and prospective employee or student OSN content.[100] This is where the unanimity ends. Maryland and New Jersey each place the qualifier ". . .through an electronic communications device" as blanket requirement for any attempted access to fall within the prohibition.[101] Delaware also includes this provision in its "prohibited acts" section,[102] but it applies solely to particular prohibitions and not the entire legislative scheme. The limitation imposed is significant because it forces the courts to interpret "through" in any context beyond directly requesting password and user name information. Thus, the question of whether employers in Maryland and educational institutions in New Jersey may peer over the shoulder of employees or applicants while using OSNs remains open. Furthermore, because the access must be acquired via an electronic device, as defined in the statute, this may hamper the applicability as technological advances undoubtedly continue into the future.

Acknowledging these risks, states included further prohibitions on conduct. One common theme concerns accessing private individual OSN content through means of observation. Michigan makes it illegal for employers to "Request an employee or an applicant for employment to grant access to, *allow observation of*, or disclose information that allows access to *or observation of* the employee's or applicant's personal internet

---

100 This language comes directly from Maryland's law, but all five others possess functionally identical wording. MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

101 Id.; N.J. STAT. ANN. § 3-29 to 3-32 (West 2013).

102 "(a) A public or nonpublic academic institution shall not request or require that a student or applicant disclose any password or related account information in order to gain access to the student's or applicant's social media networking site profile or account by way of an electronic communication device." DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013).

account."[103] California echoes this approach, specifically disallowing employers and schools from requesting to "Access personal social media in the presence of the employer" or to "Divulge any personal social media."[104] In Delaware academic institutions "shall not require or request that a student or applicant log onto a social networking site, email account, or any other internet site or application by way of an electronic communication device *in the presence of an agent of the institution so as to provide the institution access.*"[105] These explicit provisions can arguably be found in the more general phrasing in the aforementioned Maryland and New Jersey formulations, but their explicit nature is more in line with network privacy. They reiterate that it is the private OSN content that the law seeks to protect, and not the property interest of the password or user name information itself.

Delaware protects this rationale further than any other state. Its legislation goes on to prohibit educational institutions from monitoring student devices including through use of "intercept technology".[106] More significantly though are a pair of provisions that specifically address the problem of access acquisition through use of the OSN itself. First, "No public or nonpublic academic institution shall request or require a student or applicant to add the employer or its representative to their personal social networking site profile or account."[107] Basically, in Facebook parlance this equates to a prohibition on requesting or requiring the student or applicant to "friend" the institution at any level. Research proves this a major concern amongst young applicants[108] and Delaware reinforces this protection with the next provision: "A public or nonpublic institution is prohibited from accessing a student's or applicant's social networking site profile or account indirectly through any other person who is a social networking contact of the student or applicant."[109]

Taken together, these edicts place a firm barrier between the institution and the OSN profile. In the school setting, as well as the workplace, the existence of social relationships between classmates and co-

---

103 MICH. COMP. LAWS § 37.271 to § 37.278 (2012) (emphasis added).

104 CAL. LAB. CODE § 980 (West 2013).

105 DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013) (emphasis added).

106 "(c) No public or nonpublic academic institution shall monitor or track a student's or applicant's personal electronic communication device by installation of software upon the device, or by remotely tracking the device by using intercept technology." *Id.*

107 *Id.*

108 "Eighty-one percent of respondents considered it inappropriate for employers to be required to invite their supervisor to their OSN profile." Blurred Boundaries, *supra* note 5 at 107.

109 DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013).

workers is inevitable and should be encouraged. Thus, the likelihood that these cohorts would also be "social media contacts" is extremely high and the social and professional pressures of accepting a "friend" request from ones boss or superior at school are self-evident. Delaware effectively removes an easy, and already used method for employers and schools to circumvent password and other more basic OSN privacy protections.

In a similar vein New Jersey prevents educational institutions to "In any way inquire as to whether a student or applicant has an account or profile on a social networking website."[110] The statute continues by stating, "An agreement to waive any right or protection under this act is against the public policy of this State and is void and unenforceable."[111] This presents a newfound, unique take on OSN access: the *mere fact* that users engage in OSN activity is presumptively out of bounds for educational institutions. New Jersey, unlike the other states, has made explicit that whatever information may potentially be gleaned from an individual's OSN use pales in value when compared with the privacy concerns at stake.

The six laws also make critical categorical distinctions. Maryland and Michigan each distinguish between "personal" and "nonpersonal" accounts. For the former the entire legislative scheme is predicated on this distinction as highlighted above, but without legislative guidance as to the specific characteristics underlying the distinction.[112] Michigan, however, does elucidate this difference somewhat: "This act does *not* prohibit an employer from. . .Requesting or requiring an employee to disclose access information to the employer to gain access to or operate. . .An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purpose."[113] This explanation is absolutely critical for this distinction to have real value without court interpretation, and stays within the network privacy paradigm. It is entirely reasonable for accounts related to the business purpose of the employer to be outside an employee's reasonable expectation of privacy. The difficulty lies in the fact that ones personal and professional (or academic) lives are no longer easy to separate in the binary sense and often OSNs are indeed used for both

---

110 N.J. STAT. ANN. § 3-29 to 3-32 (West 2013).

111 *Id.*

112 *Supra*, Part II-B. However, Maryland does provide that when accounts are used "for business purposes" investigations into certain topics to ensure compliance are permitted. MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

113 MICH. COMP. LAWS § 37.271 to § 37.278 (2012).

purposes.[114] Thus, Michigan attempts to provide some guidelines for employees, employers, and the courts and while it may not be perfect this is absolutely the direction the law must move in.

Along these lines, the majority of statues distinguish between employer and employee devices. Only Delaware and New Jersey fail to make some type of legislative categorization based on the ownership of particular devices.[115] Again, this comports to notions of network privacy and access. Employees should not possess a reasonable expectation of privacy in the property of their employer, and even personal OSN use could reasonably be argued to fall outside of a protected privacy interests because the device was given for work. In many contexts this distinction will alleviate the tension between "personal" and "nonpersonal" accounts because it brings all OSN use within the fold for devices properly belonging to the employer under the respective statutes. This is where workplace policies are critical, and these states have codified the privacy interests at stake. Not all network privacy or access-based decisions necessarily provide increased protection for OSN use and this should not be the goal.

Finally, the vast majority of the laws enact specific, explicit exceptions or carve outs for employer or educational institution behavior that is allowable despite the general statutory provisions.[116] Indeed, Maryland goes as far as to proscribe certain *employee* conduct: "An employee may not download unauthorized employer proprietary information or financial data to an employee's personal web site, an internet web site, a web-based account, or a similar account."[117] While no other states cast formal prohibitions on employee or student conduct per se, they each allow employers or academic institutions to access otherwise protected OSN content to investigate a range of items.

Illinois makes an explicit allowance for "obtaining. . .information that is in the public domain."[118] The term "public domain" is not defined in the statute and thereby presents major problems in application to the digital world. Where and when something is in the "public domain", traditionally a copyright question, is magnified by the fact that OSNs by

---

114 "Nearly one-third (29%) of respondents included their immediate supervisor as an online "friend". . .some welcomed their employer's participation in their social networks; others reported being required to give their employers access to their profiles." Blurred Boundaries, *supra*, note 5 at 102.

115 DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013); N.J. STAT. ANN. § 3-29 to 3-32 (West 2013).

116 Only New Jersey does not contain any such provisions. N.J. STAT. ANN. § 3-29 to 3-32 (West 2013).

117 MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

118 820 ILL. COMP. STAT. 55 / 10 (2013).

their nature allow and prelude access based on a litany of factors. Consequently, what is the result when a third party re-posts applicant information onto an account that an employer can view? Is this "public domain" material? Does the applicant's original post receive copyright protection and thereby preclude applicability of the statutory provision entirely? Does crafty Google searching that produces OSN-related material equate to a user having put this information in the "public domain"? Questions like these are easily avoided[119] and yet left drastically open in the statute and it is one of the worst failings of any of the six passed pieces of legislation.

The other states generally take a different strategy by specifying particular investigatory contexts based on content as opposed to availability that alleviate OSN privacy protections. Maryland and Michigan each allow, provided specific information exists, investigations into sensitive financial, proprietary, and regulatory information and requirements. Maryland's law touches these topics in connection with "the use of a personal web site, Internet Web site, Web-based account, or similar account by an employee for business purposes" and "the unauthorized downloading of an employer's proprietary information or financial data"[120] while Michigan provides nearly identical protections with slightly different language.[121] Neither statute defines the type of "information" required to bring OSN content within what employers may do, and this is an issue employers will face in drafting their workplace policies and procedures.

Michigan[122] and California[123] extend further to include "applicable laws" meaning any investigation into alleged illegal employee conduct permits cooperation into OSN content provided a sufficient level of information has been provided and the OSN content is used reasonably related to the investigatory proceeding. These broader formulations are echoed in accompanying provisions allowing investigations into "misconduct"[124] and Delaware allows "investigations of suspected criminal activity performed by a public or nonpublic institution's public safety department or policy agency" and investigations "pursuant to an academic institution's threat assessment policy or protocol" effectively

---

119 *See infra* Part IV.

120 MD. CODE ANN., Labor and Employment § 3-712 (West 2013).

121 MICH. COMP. LAWS § 37.271 to § 37.278 (2012).

122 *Id.*

123 CAL. LAB. CODE § 980 (West 2013).

124 Id.; MICH. COMP. LAWS § 37.271 to § 37.278 (2012).

providing the same protections provided the criminal conduct investigations are performed by a third party.[125]

This represents perhaps the best evidence of lawmakers taking into account the competing employer and employee interests involved in this sphere of legislation. Employers must be able to protect their property and reasonably enforce legal workplace policy regulations while employees must have their reasonable expectations of privacy respected in the OSN context. The balance of these interests is one area where the courts and administrative agencies must inevitably play a role, and the text of legislation alone simply cannot be determinative of all outcomes where technology will continually evolve along with societal norms.

In sum, these "zones of privacy" epitomize the network privacy rationale. They place certain conduct in certain specified contexts in or out of the purview of employers and educational institutions. More than anything else legislation is necessary for OSNs for this precise reason: illustrating, at least roughly, where lines exist and where clear violations occur. At the margins it is undoubtedly difficult to administer certain aspects of these laws, but there are still courts and reasonable workplace policies to intervene, and it is not the goal of any legislation to immediately take effect and cure all potential ills. The wide degree of variability in defining terms, making distinctions, and creating the "zones" of protected privacy for OSN must be acknowledged and gives pause for reflection at just how difficult this area is to regulate effectively through legislation.

PART III: EXISTING PROTECTIONS INADEQUATE DESPITE ENCOURAGING DEVELOPMENTS

A. The Law Fails to Protect OSN Privacy in Private Employment Context

The current patchwork of Constitutional rights, torts, and statutes governing privacy in the United States is woefully inadequate to address the concerns OSN use in the workplace necessitates.[126] The slow pace and general difficulty tort law has adapting to changing technology[127] and the unpredictability involved when courts inquire as to the "reasonability"

---

125 DEL. CODE. ANN. tit. 14, § 8101-8105 (West 2013).

126 *See generally* Password or Paycheck, *supra*, note 69.

127 "New technologies have enabled novel social situations that generate privacy harms and concerns that were unforeseeable by the Restatement's authors." Privacy Torts, *supra*, note 10 at 5.

of privacy expectations in the OSN context[128] each contributed to privacy law's failure to maintain the pace of technological innovation. The latter is often characterized to reflect a generational divide between the millennial generation and the older individuals that tend to comprise the judiciary.[129] Outdated, tangential legislation likewise has not translated well to OSNs.[130]

When Congress introduced the Social Networking Online Protection Act (SNOPA)[131], two US Senators explicitly requested the Department of Justice and the Equal Employment Opportunity Commission to investigate existing protections for OSN privacy.[132] This uncertainly alone reflects the difficulty in applying statutes written before the dissemination of the internet and email into ordinary, essential aspects of everyday life–let alone OSN use.

More significant than mere uncertainty, however, is the fact that the relevant legislation as interpreted does not reach the private employer conduct at issue here. The Stored Communications Act (SCA),[133] enacted

---

128 *See* Maremont v. Susan Fredman Design Group, Ltd., No. 10-C-7811, 2011 WL 6101949 (N.D. Ill. 2011) (holding "matters discussed in Maremont's Facebook and Twitter posts were not private and that Maremont did not try to keep any such facts private" because of the size of social networks despite using privacy protections available); *but see* Ehling v. Monmouth-Ocean Hosp. Service Corp., 872 F.Supp.2d 369, 374 (2012) (holding despite there being "no indication of how many people could permissibly view" a Facebook post, the plaintiff stated a plausible claim for "a reasonable expectation of privacy in her Facebook posting because her comment was disclosed to a limited number of people who she had individually invited to view a restricted access webpage."). This note left it up to previous works to fully explain the inconsistencies and fundamental misunderstanding of how OSNs operate the courts have shown, but suffice to say the current state of the law is at best murky and at worst preclusive of privacy on OSNs.

129 "Those who have grown up with the Internet, particularly the recent interactive rise of web 2.0, view online privacy in a very different way than those of previous generations who have—or have not—immigrated to it. Younger "natives" *expect* technological barriers—whether real or merely imagined—to protect their information from unintended audiences, while others view their actions as reckless and foolish." Newell, *supra,* note 48 at 19.

130 Henderson, *supra,* note 34 at 244 ("The technologies and norms of social media have evolved rapidly, whereas the statutory structure—and much of the particular language—has remained constant.).

131 SNOPA, *supra* note 17.

132 Press Release, Senator Richard Blumenthal, Blumenthal, Schumer: Employer Demands for Facebook and Email Passwords As Precondition For Job Interviews May Be A Violation Of Federal law; Senators Ask Feds to Investigate (March 25, 2012) ("I am alarmed and outraged by rapidly and widely spreading employer practices seeking access to Facebook passwords or confidential information on other social networks. . .A ban on these practices is necessary to stop unreasonable and unacceptable invasions of privacy. An investigation by the Department of Justice and Equal Employment Opportunity Commission will help remedy ongoing intrusions and coercive practices, while we draft new statutory protections to clarify and strengthen the law.").

133 Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-2712 (2012).

in 1986, has yet to have its basic structure amended[134]. The SCA forbids the intentional and *unauthorized access* of stored communications.[135] However, if a job applicant or employee grants the employer access to their account this forfeits claims under the SCA.[136] Thus, the onus to prove coercion remains and when an employer merely *requests* this information without explicitly stating that non-compliance will result in punishment the inherent implication that the job may become unavailable or retribution may occur does not necessarily go away, and therefore this pressure incentivizes disclosure.

Similar problems of proving the access to be "unauthorized" exist under the Computer Fraud and Abuse Act (CFAA) and are made even more daunting by the requirement that plaintiffs prove a damage or loss of more than $5,000 over a one-year period.[137] As employment decisions are, or at bottom can be argued, made upon a holistic evaluation of the applicant it will undoubtedly be difficult to show that the OSN access directly led to this type of harm. Furthermore, as the majority of employees in the United States are "at will" the damages resulting for current employees poses an equally difficult burden of proof to recover under CFAA. Where this type of access is not explicitly unauthorized by statute it becomes commonplace, and once commonplace societal norms indicate that considering these requests "unauthorized" will be difficult to prove and therefore inadequate to protect OSN privacy interests.

B. Despite Overall Inadequacy Recent Developments Are Encouraging

Recent decisions by the National Labor Relations Board (NLRB) enforcing rights under the NLRA[138] illustrate the legitimization of OSN use by users on their personal accounts and the law adhering to modern notions of network privacy online.[139] The board backed workers to hold their Facebook posts were the type of "concerted and protected" activity for "mutual aid" covered by the NLRA after an employee posted a Facebook message complaining about work conditions, four coworkers

---

134 Henderson, *supra* note 34, at 244.

135 Password or Paycheck, *supra* note 69, at 19 (emphasis added).

136 *Id.*

137 18 U.S.C. §§ 1030(g), 1030(c)(4)(A)(i)(I) (2012).

138 *See* National Labor Relations Act, 29 U.S.C. §§ 151-169 (2012).

139 *See* Steven Greenhouse, *Even if It Enrages Your Boss, Social Net Speech Is Protected*, N.Y. TIMES, Jan. 22, 2013, at A1 ("The National Labor Relations Board says workers have a right to discuss work conditions freely and without fear of retribution, whether the discussion takes place at the office or on Facebook").

responded to it, and all five were fired.[140] This is a positive, and significant development because it legitimizes Facebook (and therefore OSNs) as an integral, protected means for employees to communicate and acknowledges the OSN potential as the new "water cooler" at the office.

However, protecting "concerted activity"-which is when two or more employees take action for their mutual aid or protection regarding terms and conditions of employment for "mutual benefit" in the labor relations context[141] is not the same as protecting individual privacy. Other NLRB cases have had less sympathy for OSN use, and where singular employees voice displeasure on OSNs this information is entitled to less privacy protection and may be used in termination decisions.[142] This illustrates the critical difference between employers inability to *retaliate* as opposed to the right to *access* particular information initially. This distinction is especially relevant for applicants as the only "retaliation" for employer OSN access from their perspective is a failure to be hired at all. Indeed, the NLRB explicitly covers and affords *employees* certain rights, and while they have done a commendable job updating provisions from a 1935 law enacted to protect the bargaining power of labor unions to the 21st-century OSN context, these tangential protections to individual privacy are simply insufficient to protect all the potential harms this activity poses.

Finally, the Supreme Court recently has shown encouraging signs that its hardline stance against reevaluating privacy jurisprudence may be thawing.[143] In a strongly worded concurrence, Justice Sotomayor posited, "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[144] Sotomayor, more than any Justice before, gives credence to the fact that sweeping, rapid technological change warrants consideration of past doctrine in a new light. Also significant, she asserts a view fully in line with network privacy: "I would not assume that all information

---

140 United Hispanics of Buffalo, Inc. and Carlos Ortiz, 359 N.L.R.B. 37 (2012).

141 NLRA, *supra,* note 20.

142 *See* Greenhouse, *supra* note 139.

143 *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). While admittedly the Fourth Amendment does not protect citizens against private actors, the views of the Supreme Court surely help to inform the expectations society is prepared to recognize as reasonable.

144 *Id.*

voluntarily disclosed to some member of the public for a limited purpose, is for that reason alone" necessarily devoid of a reasonable expectation of privacy.[145]

PART IV: THE NEED FOR UNIFORM, COMPREHENSIVE, CONGRESSIONAL LEGISLATION TO PROTECT PRIVACY INTERESTS OF OSN USERS IN THE PRIVATE WORKPLACE

A. Congressional Legislation Protects Employer Interests

Thus far the focus has been on employee, applicant, and student privacy interests over their OSN use. However, comprehensive legislation in this area is also the best way to protect *employee* interests, notably those related to discrimination.[146] Title VII of the Civil Rights Act ("CRA") of 1964[147] bars employers with fifteen or more employees from making employment decisions based on "race, color, religion, sex, or national origin."[148] Many states have gone further to protect against discrimination based on age, marital status, sexual orientation, disability, political orientation, union membership, and consumption of legal products.[149] Seeking access to OSN content, even without the intent of discovering this applicant information inevitably will produce this result, and therefore open the employer up to discrimination liability. The sponsor of the Illinois legislation, State Representative La Shawn Ford, echoed this rationale: "Social networking accounts are places where we document the personal and private aspects of our lives, and employers have realized they can get answers to questions they are already prohibited from asking by gaining unfettered access to our accounts. . .This legislation may protect employers from future lawsuits as much as it protects employees and jobseekers."[150]

With the millennial generation possessing such a demonstrated commitment to its OSN privacy expectations[151] this avenue of litigation, if privacy rights remain unenforced, is arguably inevitable and certainly conceivable. And while redress in the CRA is a positive thing, it is in no one's best interest for these discrimination suits to persist, especially since decisions may or may not in actuality be tied to discrimination. There is

---

145 *See id.*

146 Password or Paycheck, *supra*, note 69, at 21.

147 42 U.S.C. §§ 2000e-2000e-17 (2012).

148 42 U.S.C. §§ 2000e(b), 2000e-2(a) (2012).

149 Password or Paycheck, *supra*, note 69, at 21.

150 IL Press Release, *supra*, note 65.

151 *See supra* Part I.

no doubt that there is potentially valuable information in an applicant's OSN profile,[152] but the benefits are outweighed substantially by the pitfalls. Using OSNs as a means around existing regulation is disingenuous and illegal, so to protect to employers from themselves legislation safeguards their interests. Again, the aforementioned "tangential" privacy backdrop of United States law becomes readily apparent, and one can surely make the argument that, with Title VII in mind, individuals possess a right to *privacy* in this information (at least for the non-self evident criteria of religion and national origin) during the application process. However, until legal prohibitions specifically tied to OSN information access are enacted employers will continue to operate under the assumption that their conduct is entirely legal, or at worst "murky", and the onus remains on applicants and employees to show discrimination where often the litigation is not worth the reward.

B. Suggested Criteria for Effective Comprehensive Congressional Legislation

The proliferation and stunning rise in popularity of OSNs to the point where they are fundamental to modern communication presents a historic opportunity to move workplace privacy protection up to where it must be. Congress must capitalize on this wave of popularity and support while remaining cognizant to not unnecessarily cabin its prohibitions on the technology of the day or enact legislation too expansive as to swallow everything potentially posted online. This delicate balance can only be achieved through the network privacy approach predicated on access to particular information by particular constituencies in particular contexts.

Congress recently reintroduced SNOPA[153] and this provides a useful starting point. The proposal stays true to the access theory of reasonable expectations, but it would behoove Congress to take account of the enacted legislation in the six states and fuse together some of their critical contributions.

First, SNOPA provides protection for "private email account" and "the personal account. . .on any social networking website."[154] Explicitly bringing email within the statute avoids confusion and closer adheres to

---

152 *See* Password or Paycheck, *supra* note 69, at 18 ("Recent studies have shown that an individual's OSN profile can provide an accurate window into the individual's personality and character").

153 Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013).

154 *Id.*

network privacy, unlike Illinois who took the opposite approach.[155] Following Michigan and California it takes the comprehensive approach to protect applicants, employees, and current students. The act defines "social networking website" as "any internet service, platform, or website that provides a user with a distinct account – (A) whereby the user can access such account by way of a distinct user name, password, or other means distinct for that user; and (B) that is primarily intended for the user to upload, store, and manage user-generated personal content on the service, platform, or website."[156] This definition is very similar in effect to Michigan's in that it covers more than "social" websites–the coverage is based on user-generated content protected in some fashion. This is the best approach elucidated in any of the laws, but Congress would benefit from specifying that "personal content" includes information *shared with others*. Again, network privacy is premised on the harm defined when information moves across specified constituencies and therefore even when certain items are shared with others they remain access-protected from those outside the intended network. Additionally, this approach is not over-inclusive because whatever information employers are within their rights to possess, such as financial information, may be requested of the applicant, student, or employee to provide without needing to surrender access information. The onus is on the employee or applicant to affirmative place access barriers on their accounts, and once they have the law creates a presumption of privacy protection and this is essential.

While Congress generally took the right tack with its "social networking website" definition it failed to demarcate the line between "personal" and "nonpersonal" and this must be corrected. Modern OSN use has shown us that this line is difficult to find. Often information relevant to the workplace or school becomes intermingled with purely personal content such as image uploads or messages to third parties. However, what is an employer to make of an employee wearing his work uniform while engaging in illicit activity in his Facebook profile picture? Or an employee Tweeting defamatory statements to an audience of thousands? The best, although admittedly not perfect solution to this problem is to provide an explanation that "personal" accounts do not include those "provided by the employer, obtained by virtue of the employee's employment relationship, or used for business purposes"[157], or

---

155 820 ILL. COMP. STAT. 55 / 10 (2013).

156 Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013).

157 *See generally* MICH. COMP. LAWS §§ 37.272(d), 37.273, 37.275(a)(ii) (2012) (utilizing the language in Michigan's statutes to support that such accounts are not personal because employers are not prohibited from

those accounts "whose content may be viewed without the input of user-created access protections." This final caveat is critical to protect employer interests, and is a much better approach than Illinois' "public domain" provision by alleviating vagueness concerns.[158] Although it leaves room for interpretation at the margins it provides guidance as to what is a *reasonable* expectation of privacy in a statement made on an OSN.

Furthermore, SNOPA eliminates employers right to "require or request than at an employee or applicant provide the employer with a user name, password, or any other means for accessing" these personal email and social networking accounts. Thus, the only prohibited access stems from direct requests *made upon the employee or applicant themselves* and this is an unacceptably limiting provision in the legislation. It does not prohibit explicitly any other means of access or define "means for accessing", and although the language "any other means" could potentially gain a broad construction and cover observing the employee at work it is not ideal to leave this decision up to litigation and interpretation. Rather, Congress should borrow the innovations in the Delaware legislation[159] to proscribe specific conduct including third party contacting and in-person observation. Employers should be explicitly barred from requesting or requiring an applicant or employee to take *any* particular action with a personal internet account. This would go a long way towards enforcing against these more "unorthodox" methods of procuring access to OSNs and prevent certain coercive or investigatory work from being farmed out to third parties. Because the main goal of this legislation to set the law in line with prevailing social norms, the explicit explication of "means of access" is essential to fully promote it.

Congress, like Michigan and New Jersey, provides specific penalties and an enforcement scheme in SNOPA. Violating employers may be assessed civil penalties up to $10,000 as determined by taking "into account the previous record. . .and the gravity of the violation."[160] Also, the Secretary of Labor may take injunctive action to ensure compliance and is given the broad power to provide "such legal or equitable relief incident thereto as may be appropriate, including; employment, reinstatement, promotion, and the payment of lost wages and benefits."[161]

---

requesting or requiring access to such accounts even though employers cannot require access to "personal" accounts).

158 *See supra* Part III.

159 *See supra* Part III.

160 Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013).

161 *Id.*

This enforcement scheme goes well beyond Michigan and differs from New Jersey in power and penalty for violations.[162] The ability to provide injunctive relief, the relatively large dollar amount of the maximum penalty, and the increased punishment for repeat offenders are excellent features, and are necessary to enforce privacy rights where often the showing of actual damages will be difficult. Additionally, empowering the Secretary to take injunctive action may place large entities on notice, thereby requiring their privacy policies to meet a federal minimum helping to inform reasonable expectations for all of society.

Finally, Congress does not place exemptions in SNOPA. There are no distinctions for employee versus employer owned devices or an allowance to monitor equipment at the office or the right to conduct investigations upon receipt of specific information. This is a mistake from both a legislative and political maneuvering standpoint. Opposition to the legislation generally stems from its failure to properly protect business interests, and not allowing reasonable measures to be taken upon a valid showing of legitimate need does indeed fail to fully protect business interests. Passwords and user account information should never be on the table in any circumstance and mere "workplace misconduct" should remain insufficient for access into private OSNs for investigation. However, certain statutory provisions that require employees or current students to provide specific OSN *content* in relation to *specific investigations* of a pressing nature–sensitive financial information, securities regulation, regulatory requirements, and violations of positive law–are not only reasonable, but important to legitimize the legislation as truly representing the interests of both private individuals and institutions. Companies cannot remain liable for certain failures to monitor while being simultaneously prevented from doing so. The sensitivity of data and the ability for OSN use to intermingle with company owned devices makes this a common-sense addition to any Congressional legislation.

Overall, SNOPA is a bold step forward and its influence on the successfully enacted state legislation is evident. Congress effectively defined the types of entities it wished to keep private and free from access in its emphasis on user-generated content. Its definition reinforces privacy expectations in OSNs in how they are actually used. That the enforcement scheme also promotes the goals of the legislation, the unique

---

[162] *Compare* MICH. COMP. LAWS §§ 37.271-37.278 (2012) (providing that violating parties are guilty of a misdemeanor and capping monetary sanctions at $1,000 in Michigan), with [insert correct citation of the new jersey statute here] (permitting injunctive relief, undefined compensatory damages, undefined consequential damages, and "any other available remedy" in its enforcement scheme in New Jersey).

federal enforcement capacity, and has comprehensive breadth to cover educational institutions and all employers is admirable. However, the legislation falls short in its prohibition solely of those means of access wherein requests are made directly upon the employee or applicant. This leaves open loopholes with potential to swallow the protection. Additionally, Congress fails to delineate and define what makes accounts "personal" and this ambiguity is not one the courts should have to wrestle without any guidance. Last, Congressional legislation needs to make more allowances for circumstances where some level of OSN information access is warranted. As constituted SNOPA does not allow for reasonable requests for employee content or information even to assure compliance with applicable laws and regulations. These are essential provisions that must be added to fully ensure the rights and obligations of employers and educational institutions are protected.

CONCLUSION

Congress alone possesses the power to enact legislation that creates mandatory legal minimums for all citizens to follow. While the trend of state law proposals and enactments in a majority of states is undoubtedly encouraging, this patchwork approach is an insufficient substitute for a federally enforced baseline of protection as there is no guarantee every state will pass such a law nor is there any guarantee particular states will reach far enough to effectively protect OSN privacy interests. Thus, Congress is uniquely situated to address a problem that other areas of the law have thus far failed to and that affects the lives of every citizen every single day.

If we cannot control access to the content we post on OSNs we face the certain reality of losing the documented social and societal utility these incredible technologies present. We lose freedom of information and we chill valuable protected speech. We lose autonomy and we lose dignity. Without legislation to enforce privacy expectations that are overwhelmingly reasonable in all eyes besides the law the internet ceases to be as powerful of an instrument that we as a society should require it to be. Technological progress has made it easier for private information to fall in the hands of unintended constituencies, but our fundamental right to privacy as citizens should not pay the price for that progress. Incredibly, Congress has the power to alleviate the vast majority of these concerns with a simple piece of legislation. The time is now for us to ensure that Americans online existence comes equipped with the same privacy protections as its offline counterpart.