Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media

by SARA E. STRATTON*

Liberty finds no refuge in a jurisprudence of doubt.[1]

Introduction

Imagine interviewing for your dream job. You do so well during the interview that you are immediately offered the position. However, there is one stipulation attached to your offer: You must divulge your social media usernames and passwords so the employer can conduct a search of your personal social media accounts. While this hypothetical situation may seem surprising, there have been several recent reports of employers and universities requesting applicants' social media information.[2] Although the pervasiveness of this practice is not widely known,[3] the response from some state and federal legislators indicates resistance to this type of conduct.

---

* J.D. Candidate 2014, University of California, Hastings College of the Law; B.A. 2010, San Diego State University, Political Science. I would like to thank Professor Lois Schwartz for her guidance throughout the writing process. In addition, I would like to thank the editors of the *Hastings Constitutional Law Quarterly* for refining and fine-tuning this Note. Finally, I would like to thank my family for their continued love, support, and inspiration.

1. Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 844 (1992).

2. *See infra* pp. 2–3.

3. Press Release, Senator Charles E. Schumer, United States Senator for New York, 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 (Mar. 26, 2012), *available at* http://www.schumer.senate.gov/Newsroom/record.cfm?id=336396. United States Senators Charles Schumer and Richard Blumenthal "called on the U.S. Equal Employment Opportunity Commission ("EEOC") and the U.S. Department of Justice ("DOJ") to launch a federal investigation into a new disturbing trend of employers demanding job applicants turn over their user names and passwords for social networking and email websites to gain access to personal information like

Attention surrounding social media privacy and the workplace began when the American Civil Liberties Union ("ACLU") protested a practice by Maryland Department of Public Safety and Correctional Services ("DOC") in 2010.[4] Robert Collins, a Corrections Supply Officer with the DOC, approached the ACLU asserting that he was bothered by a DOC[5] practice requiring him to provide his Facebook[6] login information and password during a recertification interview.[7] Collins was hired to work at the DOC in 2007 and took a personal leave of absence in April of 2010.[8] Upon returning to work in July 2010, Collins discovered that his position had been reassigned.[9] Before he could be placed in another position, DOC policy required Collins to go through a recertification process.[10] The process included fingerprinting, another background check, and interview.[11] During Collins' interview on December 1, 2010, the interviewer asked if he used social media websites; Collins replied that he used Facebook.[12] The interviewer then directed Collins to divulge his username and password to permit the "government to review wall postings, email communications, photographs, and friend lists, in order to ensure that those employed as corrections officers are not engaged in illegal activity or affiliated with any gangs."[13] Collins then asked the Officer how long the DOC would need the information.[14] The interviewer responded that background checks could take up to one or two months, and that the DOC would likely use the information again during that time period.[15]

---

private photos, email messages, and biographical data that is otherwise deemed private." *Id.*

4. Melissa C. Goemann, *Maryland Passes Nation's First Social Media Privacy Protection Bill*, ACLU BLOG OF RIGHTS (May 4, 2012, 4:30 PM), http://www.aclu.org/blog/technology-and-liberty/maryland-passes-nations-first-social-media-privacy-protection-bill.

5. *Id.*

6. *See infra* pp. 5–7.

7. Meredith Curtis, *Want A Job? Password, Please!*, ACLU BLOG OF RIGHTS (Feb. 18, 2011, 2:04 p.m.), http://www.aclu.org/blog/technology-and-liberty/want-job-password-please.

8. Letter from Deborah A. Jeon, Legal Dir., Am. Civil Liberties Union of Md., to Gary D. Maynard, Sec'y, Md. Dept. of Pub. Safety and Correctional Servs. (Jan. 25, 2011), *available at* http://www.aclu-md.org/uploaded_files/0000/0041/letter-_collins_final.pdf.

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

In addition to the story of Officer Collins, there have been several reports of this practice across the United States. For instance, Justin Bassett, a statistician from New York City, had finished an interview and was asked to "hand over his Facebook login information after the interviewer couldn't locate his profile on the site."[16] In addition, the City of Bozeman, Montana, required its job applicants to disclose a variety of personal information, including social media passwords to websites like Facebook.[17] The specific language on the application states: "Please, list any and all, current personal or business websites, web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc."[18] As such, the application has designations for "Username/ Member Log-In" and "Password."[19]

This Note contends that the practice of the Maryland DOC, in addition to any similar practices conducted by public employers requiring applicant social media login information, violates the constitutional right to informational privacy. With increasing access to the Internet and the popularity of social media, personal information on the Internet is becoming more accessible than ever before. Although the advent of the Internet may have been a cause for privacy concerns,[20] the pervasive use of social media and the extensive amount of information many individuals disclose about their personal lives only exacerbates the problem.[21]

This Note argues that the Supreme Court should recognize a constitutional right to informational privacy under the Fourteenth Amendment to the United States Constitution. The scope of this Note is relatively narrow, as it specifically addresses the issues surrounding employer access to social media policies in order to

16. Joanna Stern, *Demanding Facebook Passwords May Break Law, Say Senators*, ABC NEWS (Mar. 26, 2012), http://abcnews.go.com/Technology/facebook-passwords-employers-schools-demand-access-facebook-senators/story?id=16005565.

17. Kelly Phillips, *Are Social Media Passwords Fair Game for Potential Employers?*, ERBLAWG (June 24, 2009), http://www.erblawg.com/are-social-media-passwords-fair-game-for-potential-employers/.

18. CITY OF BOZEMAN, MONTANA, CONSENT AND RELEASE TO CONDUCT CRIMINAL BACKGROUND AND REFERENCE CHECK, *available at* http://privacy.org/Background_Check_Form_Interview_MASTER.pdf (last visited Mar. 2, 2014).

19. *Id.*

20. *See generally* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085 (2002).

21. *See infra* p. 8.

highlight the debate around constitutional informational privacy rights.[22] Further, this Note is limited to protection of public employee information against governmental action.[23] Finally, this Note asserts the need for the Supreme Court to recognize the right to informational privacy from a substantive due process perspective under the Fourteenth Amendment and does not focus on privacy under the Fourth Amendment[24] or First Amendment.[25]

Part I provides background information on social media websites. Specifically, it examines the Facebook social networking website and the privacy interests that could be implicated if forced disclosure is required by government employers.

Part II discusses proposed state, federal, and constitutional solutions to the problem of employers requesting applicant social media usernames and passwords. First, this section addresses the inadequacy of a state response to this problem. Second, it discusses the deficiency of a federal legislative solution by examining the federal government's proposed bill, the Social Networking Online Protection Act ("SNOPA"), and other federal laws. Finally, this section addresses the constitutional background of the right to privacy and explores the right's ambiguous nature. This section will explain the Supreme Court's limited development of the information privacy doctrine, and will highlight the circuit court split in the area of informational privacy.

---

22. Current laws are combating forced disclosures for employment applicants and prospective university students. This Note, however, primarily focuses on employment applicants.

23. The Supreme Court's recognition of the right to privacy only protects public employees against government action. Private actors are not included. *See* Kevin C. McAdam & John R. Webb, *Privacy: A Common Law and Constitutional Crossroads*, 40 COLO. LAW. 55 (2011). Only in limited circumstances have private sector employees been afforded constitutional protections. For instance, when a private employer acts as an agent of the government. *See* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 614 (1989) (holding that private sector employees were entitled to First Amendment protections when the employer was heavily intertwined with the government).

24. Although not discussed in this Note, the Supreme Court has recognized that public employees are entitled to Fourth Amendment privacy protections. The Court applies a two-prong test, which first assesses whether the employee had a reasonable expectation of privacy. O'Connor v. Ortega, 480 U.S. 709, 716–18 (1987), *aff'd,* City of Ontario v. Quon, 130 S. Ct. 2619, 2622–23 (2010). If the expectation of privacy was reasonable, the Court then assesses whether the search was reasonable under the circumstances. *O'Connor*, 480 U.S. at 719; *Quon*, 130 S. Ct. at 2628.

25. The Supreme Court has also noted that the First Amendment protects publishing the name of a rape victim obtained from a public police report. The Fla. Star v. B.J.F., 491 U.S. 524, 526 (1989).

Part III concludes that the best solution to address social media privacy concerns for employment applicants—at least in terms of state action—is for the Supreme Court to recognize a constitutional right to *informational privacy* through substantive due process under the Fourteenth Amendment. In doing so, this Note argues that the Court should employ the "reasonable expectation of privacy approach" to determine whether a right to privacy should apply and then utilize the balancing test developed by the Third Circuit in *United States v. Westinghouse Electric Corp.*[26] to determine whether the right to privacy is outweighed by the government's interest in disclosure.[27]

I. The Social Media Problem

Social media refers to user-driven, interactive Internet applications that allow for the creation and exchange of user-generated content.[28] There is a wide range of social media applications, including collaborative projects,[29] blogs,[30] content communities,[31] social networks,[32] and virtual worlds.[33] Because of the

26. United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980).

27. *Id.* at 578.

28. Andreas M. Kaplan & Michael Haenlein, *Users of the world, unite! The challenges and opportunities of Social Media*, 53 BUS. HORIZONS 59, 59–62 (2010), *available at* http://michaelhaenlein.com/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf.

29. "Collaborative projects enable the joint and simultaneous creation of content by many end-users and are, in this sense, probably the most democratic manifestation of [user-generated content]." *Id.* at 62. Wikipedia is an example of a collaborative project. *Id.*

30. Blogs "are the Social Media equivalent of personal web pages and can come in a multitude of different variations . . . . Blogs are usually managed by one person only, but provide the possibility of interaction with others through the addition of comments." *Id.* at 63.

31. The purpose of content communities is to share media between users. *Id.* Flickr (a photo-sharing website) and YouTube (a video-sharing website) are examples of content communities. *Id.*

32. "Social networking sites are applications that enable users to connect by creating personal information profiles, inviting friends and colleagues to have access to those profiles, and sending e-mails and instant messages between each other." *Id.* Facebook and MySpace are examples of social networks. *Id.* at 63–64.

33. "Virtual worlds are platforms that replicate a three-dimensional environment in which users can appear in the form of personalized avatars and interact with each other as they would in real life." *Id.* at 64. There are two types of virtual worlds: virtual game worlds and virtual social worlds. *Id.* Virtual game worlds "require their users to behave according to strict rules in the context of a massively multiplayer online role-playing game." *Id.* World of Warcraft is an example of a virtual game world. *Id.* Conversely, virtual social worlds "allows inhabitants to choose their behavior more freely and

added sharing component of online interaction, social media differs from other methods of online communication, such as emailing or instant messaging.[34] Individuals typically use social media for storage[35] and connecting with others.[36] As of December 2013, the most notable social media networks are Facebook, Twitter, LinkedIn, Pinterest, and Instagram.[37]

Although all forms of social media contain user-specific information that might implicate privacy concerns, this Note focuses specifically on the Facebook social networking website in order to narrow the scope of the discussion. Facebook is the largest and most widely accessed social networking site in the world.[38] Sixty-seven percent of American adults use Facebook.[39] As of December 2012, Facebook had over one billion users internationally, 618 million daily active users, and 680 million monthly active users accessing Facebook mobile products.[40]

In addition to being the most widely accessed social networking site, Facebook allows users to post a vast amount of information on their Facebook profiles.[41] The following information is available on a fully disclosed Facebook profile: work and education, schooling, address, relationship status, family members, email address, telephone numbers, street address, screen name, political views,

essentially live a virtual life similar to their real life . . . . [T]here are no rules restricting the range of possible interactions except for basic physical laws such as gravity." *Id.*

34. *See* Alexander Naito, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 860 (2012).

35. *See* Peter Vajgel, *Needle in a haystack: efficient storage of billions of photos*, FACEBOOK (Apr. 30, 2009, 2:27 PM), https://www.facebook.com/note.php?note_id=76191543919.

36. *See generally People You May Know*, FACEBOOK, https://www.facebook.com/help/501283333222485/ (last visited Mar. 2, 2014).

37. *See* Maeve Duggan & Aaron Smith, *Social Media Update 2013,* PEW INTERNET (Dec. 30, 2013), http://www.pewinternet.org/2013/12/30/social-media-update-2013/.

38. *Social Media Report 2012: Social Media Comes of Age*, NIELSON (Dec. 3, 2012), http://www.nielsen.com/us/en/newswire/2012/social-media-report-2012-social-media-comes-of-age.html.

39. Maeve Duggan & Joanna Brenner, *The State of Social Media Users*, PEW INTERNET (Feb. 14, 2013), http://www.pewinternet.org/Reports/2013/Social-media-users/The-State-of-Social-Media-Users.aspx.

40. *Key Facts*, FACEBOOK, http://newsroom.fb.com/Key-Facts (last visited Mar. 2, 2014).

41. *See Facebook & your privacy*, CONSUMER REPORTS (June 2012), http://www.consumerreports.org/cro/magazine/2012/06/facebook-your privacy/index.htm.

religious views, and language spoken.[42] In addition to basic personal information, Facebook allows users to upload pictures, videos, post comments on other profiles, send email-like messages, and instant message. Users can also make status updates[43] and "check-in" to locations in order to share information about where they are going or what they are doing.[44] The "check-in" option enables other users to view one's location.[45] Facebook users even have the option of disclosing their organ donor status.[46]

Facebook has various privacy options available for its users.[47] In order to use Facebook, a user must sign up, disclose his or her "name, birthday, gender and email address," and provide a password.[48] To log in to the Facebook account thereafter, users must enter the username and password they used to originally sign up.[49] Once logged into the account, users can set their profiles to either "public," where any individual on the Internet can access their account, or "private," where only "friends"[50] can view the user's information. There are also customized options available where users can restrict access of pictures, messages, and postings to specific individuals.[51] Users can vary their access between completely private, semi-private, and public.[52]

---

42. *Update Your Basic Info*, FACEBOOK, http://www.facebook.com/help/334656726616576/ (last visited Mar. 2, 2014).

43. *Sharing*, FACEBOOK, http://www.facebook.com/help/418076994900119/ (last visited Mar. 2, 2014).

44. *Find Places Nearby and Check In*, FACEBOOK, https://www.facebook.com/help/461075590584469 (last visited Mar. 2, 2014).

45. *Id.*

46. *Share Your Organ Donor Status*, FACEBOOK, http://www.facebook.com/help/416967021677693/ (last visited Mar. 2, 2014).

47. Privacy concerns on Facebook are often a topic of discussion in the news media. *See* Rosa Golijan, *Consumer Reports: Facebook privacy problems are on the rise*, NBC NEWS (May 3, 2012), http://www.nbcnews.com/technology/technolog/consumer-reports-facebook-privacy-problems-are-rise-749990.

48. *Create an Account*, FACEBOOK, http://www.facebook.com/help/345121355559712/ (last visited Mar. 2, 2014).

49. *Login Basics*, FACEBOOK, http://www.facebook.com/help/418876994823287/ (last visited Mar. 2, 2014).

50. A friend is another Facebook user who the primary user authorizes to access their personal profile. *See generally Adding Friends & Friend Requests*, FACEBOOK, http://www.facebook.com/help/360212094049906/ (last visited Mar. 2, 2014).

51. *See generally Choose Who You Share With*, FACEBOOK, http://www.facebook.com/help/459934584025324/ (last visited Mar. 2, 2014).

52. *See* Naito, *supra* note 34, at 859–60.

Facebook has also provided avenues for third-party access to personal profile information through "games" and "applications."[53] Whenever a user authorizes a game or an application, the application can often access information such as a user's name, picture, gender and list of friends.[54] In some instances, applications can see even more data if a user grants that application permission.[55] Furthermore, some third-party applications provide options for users to purchase items from the provider.[56] Facebook enables users to store credit and debit card information on their accounts.[57]

The vast amount of easily accessible personal information is a problem with social media. There has been a transformation from strictly static, independent websites to a platform of interconnected social media websites—popularly referred to as Web 2.0.[58] Web 2.0 has caused a proliferation of personal disclosures that individuals might not otherwise feel comfortable disclosing through other methods of communication.[59] In a study conducted by Carnegie Mellon University, researchers hypothesized that Facebook users have increased the amount of personal disclosures on their profiles

53. *See All Games,* FACEBOOK, https://www.facebook.com/appcenter/category/games/ (last visited Mar. 16, 2014); *Apps,* FACEBOOK, https://www.facebook.com/appcenter/category/apps/?platform=web (last visited Mar. 16, 2014); *see also King Games—Terms and Conditions*, KING, http://about.king.com/consumer-terms/terms/en (last visited Mar. 25, 2014) (explaining that they "will only *collect, process, use and share your personal information* in accordance with our Privacy Policy and as set out in these terms.") (emphasis added).

54. Whenever a user connects to an application, game or website using their Facebook account, Facebook will provide the application information from the user's "public profile" and friend list. *See Data Use Policy: Other Websites and Applications,* FACEBOOK, https://www.facebook.com/about/privacy/your-info-on-other#applications (last visited Mar. 16, 2014). Under the definition of "public profile," Facebook treats a user's "name, profile pictures, cover photos, gender, networks, username and User ID" as if they were public information. *Data Use Policy: Information We Receive and How It Is Used,* FACEBOOK, https://www.facebook.com/about/privacy/your-info#public-info (last visited Mar. 16, 2014).

55. *See Data Use Policy: Other Websites and Applications, supra* note 54 (explaining how users can grant applications more permission to view information, such as stories, photos, or likes).

56. *See Facebook Payments*, FACEBOOK, http://developers.facebook.com/docs/payments/ (last visited Mar. 2, 2014).

57. *Credit/Debit Cards*, FACEBOOK, http://www.facebook.com/help/359291094142663 (last visited Mar. 2, 2014).

58. Rory Bahadur, *Electronic Discovery, Informational Privacy, Facebook and Utopian Civil Justice*, 79 MISS. L.J. 317, 347 (2009).

59. *Id.* (highlighting a situation where bloggers often use their online blogs to "come out" of the closet).

for at least four reasons.[60] First, Facebook increased the number of fields in which users can enter personal disclosures.[61] Second, Facebook enabled sharing options allowing users to regularly share changing information as opposed to simply displaying static information.[62] For instance, users are now able to share information through chatting and messaging with their friends (the "share option") rather than simply being restricted to displaying static information like names, email addresses, and birthdates. Facebook profiles have shifted from showing static information to hosting "'habitats' through which new information is frequently created . . . by virtue of interacting with others (users, companies, sites) through the network."[63] Third, the data generated by new third-party applications can be posted to Facebook users' profiles.[64] Finally, "friends" of the Facebook user are now allowed to add more information about the user on the user's profile, such as photographs depicting the user.[65]

The expansive amount of information available about users on social media websites is further complicated in the context of employment. While social media websites, such as Facebook, are valuable tools for users to keep in touch with friends and family members,[66] they are also advantageous for employers and universities who utilize such websites as part of the applicant prescreening process.[67] Many employers and universities run criminal background checks on prospective employees and students, and general Google[68]

60. Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. OF PRIVACY & CONFIDENTIALITY 7, 26–27 (2012), *available at* http://repository.cmu.edu/jpc/vol4/iss2/2/ (select "Download").

61. *Id*. at 26.

62. *Id.*

63. *Id.*

64. *Id.* at 27.

65. *Id.* at 28.

66. A study conducted by Pew Internet found that Internet users' primary purpose for using social networking websites includes connecting with friends and family. Other reasons were sharing hobbies or interests, making new friends, reading comments by public figures, and finding potential love interests. Aaron Smith, *Why Americans use social media*, PEW INTERNET (Nov. 15, 2011), http://www.pewinternet.org/Reports/2011/Why-Americans-Use-Social-Media.aspx.

67. *See generally* 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, 448–60 (2008).

68. *See* Allan Hoffman, *Job Applicant, Beware: You're Being Googled*, MONSTER, http://career-advice.monster.com/job-search/getting-started/hr-googling-job-applicants/article.aspx (last visited Mar. 2, 2014). *See also* Byrnside, *supra* note 67, at 458.

and social media searches[69] are commonly utilized. Many employers search the *public* profiles of individuals on Facebook, MySpace, or LinkedIn to acquire additional information about their applicants. Employers even hire outside companies to perform social media background checks.[70]

An example of a social media application that could implicate privacy concerns if accessed by an employer is the "Down" application on Facebook. According to the application's website, its purpose is to enable users to anonymously "find friends who are down for the night"[71]—in other words, to locate Facebook "friends" who mutually want to have sexual relations with each other. Pursuant to the website, three steps are required to use the application: (1) the user signs into Facebook in order to see other Facebook friends who have also downloaded the application; (2) the user then selects any "sexy" Facebook friends who the user would like to have sex with or date; and then, (3) the application sends a notification to the user and "friend" if they mutually decide they want to have sexual relations with each other or go out on a date.[72] Users who access the application manage it directly from their Facebook pages. The "Bang with Friends" application was reported in January 2013 to have had roughly 30,000 users since it launched earlier that month.[73] Although it was initially provided only for heterosexuals, the application's creators planned a "same-sex" option for its users.[74] As discussed *infra*, constitutional issues may arise when government employers become privy to employees' sexual preferences.[75]

69. *See* Jocelyn Richard, *37 Percent Of Employers Use Facebook To Pre-Screen Applicants, New Study Says*, HUFFINGTON POST, (Apr. 20, 2012, 3:13 P.M.), http://www.huffingtonpost.com/2012/04/20/employers-use-facebook-to-pre-screen-applicants_n_1441289.html.

70. *See, e.g.*, SOCIAL INTELLIGENCE, http://www.socialintel.com/ (last visited Mar. 2, 2014).

71. DOWN, http://www.downapp.com/ (last visited Mar. 18, 2014).

72. *Id.*

73. Anita Li, *Bang With Friends Sex App Registers 5 Users Per Minute*, MASHABLE (Jan. 29, 2013), http://mashable.com/2013/01/29/bang-with-friends/.

74. *Id.*

75. Some circuit courts have found that intrusions into areas that implicate "fundamental rights" under Supreme Court jurisprudence should receive constitutional informational privacy protection. *See infra* pp. 674–75.

II. Finding a Solution to the Social Media Problem

The practice of employers requesting applicants' social media information raises significant privacy concerns. In response to this practice, several states have passed social media protection laws prohibiting this type of employer conduct. The federal government is considering a proposed bill—SNOPA—to rectify this problem. However, as the following discussion will illuminate, state and federal responses are insufficient to protect individual privacy rights. Thus, in order to provide more complete protection for public employee information, a constitutional solution is necessary: The U.S. Supreme Court should recognize a constitutional right to informational privacy.

a. State Efforts are Incomplete Solutions to Resolving Constitutional Privacy Rights

The rise in reports of employers requesting applicant social media usernames and passwords has compelled several state legislatures to enact social media protection laws. As of March 2014, only fourteen states—Arkansas, California, Colorado, Delaware, Illinois, Maryland, Michigan, Nevada, New Mexico, New Jersey, Oregon, Utah, Vermont, and Washington—have enacted legislation protecting employee or student applicants from being compelled to disclose social media usernames and passwords.[76] This section will distinguish the Maryland, Illinois, and California laws to highlight the various approaches states are taking to address this contentious practice.

Maryland was the first state to enact a law protecting employees from disclosing social media login information.[77] The Maryland law, codified at section 3-712 of the Labor and Employment Code, was prompted after Officer Collins' allegations about the DOC's policy requesting his Facebook username and password.[78] The law covers private businesses and state and local governments.[79] The law prohibits employers from "request[ing] or requir[ing] that an

76. *See Employer Access to Social Media Usernames and Passwords*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last visited Mar. 19, 2014) (click on "2013 Legislation" to access a summary of legislation passed in 2013; and click on "2012 Legislation" to access a summary of legislation passed in 2012).

77. *See* Goemann, *supra* note 4; *see also* MD. CODE ANN., LAB. & EMPL. § 3-712 (2012).

78. *See* Curtis, *supra* note 7.

79. MD. CODE ANN., LAB. & EMPL. § 3-712(a)(4)(i)(1)–(2).

employee or applicant disclose *any* user name, password, or other means for accessing a *personal account or service* through an electronic communications device."[80] However, there is an exception that permits the employer to require the employee to disclose the username and password to access nonpersonal information in the work computer.[81] Further, employers are permitted to investigate employees to ensure compliance with financial laws and regulatory requirements.[82] The language of section 3-712 is fairly expansive, as it prohibits requiring *any* disclosure of *any* personal account. Thus, the law broadly prohibits employer access to personal information relating not only to Facebook or other social networking sites, but also to electronic communication accounts and services, which can presumably include email. This makes the law inclusive and protective of employee and applicant privacy.

Illinois has enacted a social media law that is both narrower and broader than the Maryland law.[83] The Illinois law prohibits employers from "request[ing] or requir[ing] any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's . . . account or profile on a social networking website or to demand access in any manner . . . ."[84] The law also allows employers to create policies regarding Internet use, monitor workplace electronic equipment, and obtain information available in the public domain.[85] Unlike the Maryland law, the Illinois law is broader because it is only restricted to "social networking" websites.[86] Such social networking websites are defined, under this law, as services that allow users to "connect" with others and do not include electronic mail.[87] The "connection" requirement may, therefore, preclude application to other social media, such as blogs. Presumably, since the law prohibits "gain[ing] access" to accounts, the law would cover "over-the-shoulder" surfing of social-networking accounts (i.e., asking an

80. *Id.* at § 3-712(b)(1) (emphasis added).

81. *Id.* at § 3-712(b)(2).

82. *Id.* at § 3-712(e)(1).

83. *Compare* MD. CODE ANN., LAB. & EMPL. § 3-712, *with* 820 ILL. COMP. STAT. § 55/10 (2013).

84. 820 ILL. COMP. STAT. § 55/10(b)(1) (2013).

85. *Id.* at § 55/10(b)(2)(A)–(B) & (b)(3).

86. *Compare* MD. CODE ANN., LAB. & EMPL. § 3-712, *with* 820 ILL. COMP. STAT. § 55/10. It does not appear that it would apply to email or blogs, as these are not considered "social networking" websites.

87. 820 ILL. COMP. STAT. § 55/10(b)(4) (2013).

employee or applicant to log into his social media account to allow the employer to view his social media profile "over his shoulder"), and asking others with access to the account to login so that the employer can conduct a search. Furthermore, the law is narrower because it does not provide any exceptions for workplace investigations nor does the law apply to electronic mail.[88]

California has also enacted two social media laws targeting public and private universities, as well as private employers.[89] The California legislature is currently considering amending the law to include public employers.[90] Codified at section 980 of the California Labor Code, the law prevents employers from "requir[ing] or request[ing] an employee or applicant [to] . . . disclose a username or password for the purpose of accessing personal social media," "[a]ccess[ing] personal social media in the presence of the employer," or "[divulging] any personal social media."[91] However, the law also takes employer's interests into account by permitting disclosure if the employer "reasonably believe[s] [it is] . . . relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations" so long as the social media is only used in relation to the investigation.[92] The law further permits disclosure of "a username, password, or other method for the purpose of accessing an employer-issued electronic device."[93] California's law differs from Maryland and Illinois in that it takes a more balanced approach to address employer interests. It protects employers by applying a reasonable belief standard for employer conduct, allowing for instances in which password disclosure is permitted.[94] Thus, this law appears to give employers more discretion in accessing employee personal login information and, as a result, provides less security for employees and applicants.

Based on these state laws protecting applicants from divulging social media usernames and passwords to potential employers, it would seem that state legislation would be sufficient to regulate this

88. *See id*.

89. CAL. LAB. CODE § 980 (2013); CAL. EDUC. CODE § 99120 (2013).

90. *See* A.B. 25, at 1 (Cal. 2014), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB25#.

91. CAL. LAB. CODE § 980(b) (2013).

92. *Id.* at § 980(c).

93. *Id.* at § 980(d).

94. *See* CAL. LAB. CODE § 980(c) (2013) (explaining that employers can request social media passwords if it is related "to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations.").

conduct and protect constitutional privacy interests. The current protection, however, is insufficient. First, not all states have laws prohibiting this practice, though many states have responded quickly to address this issue.[95] Second, Delaware's law only protects applicants applying for admission into a university, not applicants applying for employment.[96] Third, California's law only protects applicants to private employment, not applicants to public employment. Finally, the provided level of protection may not necessarily be adequate. Illinois, for instance, only protects applicants from being forced to disclose social networking passwords, leaving open the possibility of employers being permitted to request usernames and passwords to other social media websites, such as blogs.[97]

b. The Uncertain Future and Application of Federal Legislation Is Also an Inadequate Solution to Protect Constitutional Privacy Interests

In addition to the states' response to this practice, SNOPA was introduced in Congress on April 27, 2012.[98] Although the bill died when Congress adjourned in 2012, it has been reintroduced for the 2013 term.[99] The 2013 bill covers any employer, whether private or public, and it covers university admissions.[100] It prohibits any employer from "requir[ing] or request[ing] that an employee or applicant for employment provide the employer with a user name, password, or any other means for accessing a private email account of the employee or applicant or the personal account of the employee or

95. Maryland was the first state to enact a password protection law on May 2, 2012. *See* Goemann, *supra* note 4. As of February 21, 2014, at least 39 states have enacted or are considering enacting social media protection laws. NAT'L CONFERENCE OF STATE LEGISLATURES, *supra* note 76 (listing the states considering legislation in 2014, and the states that already passed legislation in 2013 and 2012).

96. *See* DEL. CODE ANN. tit. 14, § 8103 (2013).

97. *See supra* Part I (explaining social media is a broad, user-driven, interactive platform which allows users to create and exchange information, whereas social networking is a subset of social media which allows for the creation and exchange of user-generated conduct through personal profiles).

98. Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2nd Sess. 2012). *See also* Joanna Stern, *Legislation Would Make it Illegal for Employers to Ask for Passwords*, ABC NEWS (Feb. 6, 2013), http://abcnews.go.com/Technology/snopa-law-make-illegal-employers-passwords-reintroduced-congress/story?id=18422329#.UVUeVc0Tkuc.

99. Social Networking Online Protection Act, H.R. 537, 113th Cong. (1st Sess. 2013).

100. *Id.* at §§ 3, 5(1).

applicant on any social networking website."[101] It also imposes penalties on employers who "discharge, discipline, discriminate . . . or deny employment or promotion . . . or threaten to take any such action against" the employee if the employee "refuses or declines" to provide the information, makes a complaint, institutes a proceeding, or testifies.[102]

While SNOPA may be adequate to protect the privacy of social media information, this congressional response still poses problems. First, it is unclear whether Congress will in fact pass the bill. If Congress fails to pass SNOPA, applicants would be required to rely on the incomplete patchwork of state laws or rely on federal laws. It is unclear, though, that any existent federal law provides sufficient protection because none are specifically targeted at employers in the context of social media. For instance, the most relevant federal statute protecting electronic disclosures is the Stored Communications Act ("SCA").[103] The SCA, however, is outdated and has not responded to the expansion of modern electronic communications, such as social media.[104] One of the principal condemnations of the SCA is that it has "fail[ed] to provide a clear framework for understanding whether a user has a reasonable expectation of privacy in his communications stored in the cloud."[105] Moreover, lower courts are confused about its applicability to social media.[106] Another federal statute, the Fair Credit Reporting Act ("FCRA"), also provides tangential protection to applicants by providing notice and consent requirements for background checks, but it only applies to third-party screening companies.[107] Thus, it is

101. *Id.* at § 2(a)(1).

102. *Id.* at § 2(a)(b).

103. To be fair, there are varied legislative protective measures that have been granted. For instance, in regulating government record keeping, Congress has passed The Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988. In addition, Congress has enacted The Fair Credit Reporting Act, which protects information obtained by the credit reporting industry. *See* Susan E. Gindin, *Lost & Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1119–1210 (1997).

104. *See* Lindsay S. Feuer, *Who is Poking Around Your Facebook Profile?: The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites*, 40 HOFSTRA L. REV. 473, 511 (2011).

105. *Id.* at 496 (internal citation and quotations omitted).

106. *See generally id.* at 499–502.

107. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2014). *See also* Nathan J. Ebnet, Note, *It Can Do More than Protect Your Credit Score: Regulating Social Media Pre-*

unclear whether these statutes could adequately protect constitutional privacy interests implicated by public employer social media searches.

Second, though the focus of this Note is limited to informational privacy in the context of public employers requiring disclosure of social media usernames and passwords, it must be remembered that this is only a small facet of the informational privacy debate.[108] Potential threats to informational privacy have been identified in numerous areas such as medical records,[109] financial information,[110] electronic filing,[111] and the Internet in general.[112] Privacy protection targeted at specific threats does not do away with the greater, overarching informational privacy dilemma.

Notably, commentators have argued that legislative solutions are an insufficient means of protecting privacy rights.[113] The ambit of legislation is often very narrow and targeted. As indicated above, a patchwork of legislation addresses some aspects of informational privacy, but the protections are by no means sufficiently

Employment Screening With the Fair Credit Reporting Act, 97 MINN. L. REV. 306, 308 (2012).

108. Although concerns surrounding the right to informational privacy are much broader than simply protecting social media username and password privacy, this Note is limited to discussion of social media privacy.

109. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) (explaining that "[t]here can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection").

110. Plante v. Gonzalez, 575 F.2d 1119, 1135 (5th Cir. 1978) (finding that a privacy interest in financial information is significant but also noting that the fact that the plaintiffs are state senators matter in this determination).

111. *See generally* Kyla Kitajima, *Electronic Filing and Informational Privacy*, 27 HASTINGS CONST. L.Q. 563 (2000) (discussing the informational privacy problems in electronic filing).

112. *See* Lin, *supra* note 20, at 1090 (arguing that "a constitutional right to informational privacy is necessary and appropriate for protecting privacy on the Internet").

113. Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 134 (1991) (noting that "[t]he inherent conflict between the government as 'collector' and the government as 'protector' casts doubt on the efficacy of relying on state and federal legislatures to protect individuals' interest in informational privacy"). *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1538 (2000) ("It is already far too late to prevent the invasion of cameras and databases. . . . No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay.") (internal citations and quotations omitted).

comprehensive.[114] One of the major issues in protecting privacy in a technological age is the rapid pace at which technology develops. It is difficult for legislatures to quickly respond to the threats posed by emerging technology.[115] Although the federal and state governments are responding to the problem of employers requesting social media usernames and passwords, it is possible that these bills may be rendered obsolete when new forms of technology are created.[116]

c. Recognizing a Broader Constitutional Protection is the Best Way to Safeguard Informational Privacy Rights in Social Media and Online Information

The better solution to protect social media privacy rights is recognizing informational privacy as a constitutional right under the Fourteenth Amendment. This would allow public employees to challenge government practices when state and/or federal protections are inadequate.

1. Origins of the Right to Privacy

Samuel Warren and Justice Louis Brandeis, the "fathers of privacy law,"[117] famously noted that the right to privacy is "the right to be let alone."[118] The right to privacy provides "rights as against the world"[119] and is separated into two areas: common law tort privacy and constitutional privacy.[120] Under the common law, there are four torts that violate an individual's privacy rights: "(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) Public disclosure of embarrassing private facts about the plaintiff; (3) Publicity which places the plaintiff in a false light in the public eye; (4) Appropriation, for the defendant's advantage, of the plaintiff's name

114. *See* Gindin, *supra* note 103, at 1196 (noting that Congress has enacted statutes "in a piecemeal fashion to address specific privacy needs").

115. *See* William Jeremy Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1197 (2010) (explaining that it is difficult for legislatures to "keep up with the pace of change in computer networking. . . . [because] [b]y the time legislatures or courts figure out how to deal with a new product of service, the technology has already progressed").

116. The SCA exemplifies the failings of Congress to respond to technology changes because it was developed around technology in 1986. *Id.*

117. Lin, *supra* note 20, at 1094.

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

119. *Id.* at 213.

120. McAdam, *supra* note 23, at 55.

or likeness."[121] In contrast, under constitutional privacy, protections are afforded to "personal information, individual autonomy, and searches and seizures."[122] Although there is no explicit mention of the right to privacy in the Constitution,[123] the Supreme Court has recognized the right to privacy through several interpretations of the Bill of Rights. The Court's initial recognition of the right to privacy centered around property rights.[124] Initially, the Court found a right to privacy only under the Fourth and Fifth Amendments,[125] and then under the First Amendment.[126] The most contentious area of privacy rights under the Constitution, however, has been under the Substantive Due Process Clause of the Fourteenth Amendment—the focus of this Note.

2. The Supreme Court Has Neglected Defining the Scope and Application of Informational Privacy

Two rights are at play under the constitutional right to privacy: decisional privacy and informational privacy.[127] Decisional privacy ensures personal autonomy in making personal decisions, while informational privacy relates to ensuring confidentiality in information.[128] While the Supreme Court recognizes and protects decisional privacy under the Fourteenth Amendment, the Court has not protected informational privacy.

At the inception of the right to privacy, the Supreme Court focused on decisional privacy. In the landmark decision *Griswold v. Connecticut*, the Supreme Court recognized a generalized

121. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

122. *Id. See, e.g.*, Whalen v. Roe, 429 U.S. 589, 599 (1977) (noting a right to privacy of information which includes an "individual interest in avoiding disclosure or personal matters"); Paul v. Davis, 424 U.S. 693, 713 (1976) (noting the right to privacy protects "matters relating to marriage, procreation, contraception, family relationships, and child rearing, and education"); Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (noting the beginnings of the Fourth Amendment recognition of a "reasonable expectation of privacy").

123. *Paul*, 424 U.S. at 712.

124. Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 765 (2004).

125. *Id.*

126. *See* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1374–91 (1992).

127. Some have argued that the courts should be focusing on autonomy rights rather than focusing on a distinction between informational and decisional privacy. *See* Suter, *supra* note 124, at 1096.

128. *Whalen*, 429 U.S. at 598–600.

constitutional right to privacy.[129] In *Griswold*, the Court held that a statute criminalizing the sale of contraceptives to married couples was unconstitutional.[130] The Court rooted its decision on the notion that the "Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."[131] The effect of recognizing this privacy right was to credit the understanding that personal liberties were fundamentally important under the Constitution.[132]

The Supreme Court expanded its right to privacy doctrine in another landmark case, *Roe v. Wade*.[133] In *Roe*, the Court acknowledged that the right to privacy is founded in the Fourteenth Amendment's concept of personal liberty.[134] The Court invoked the substantive due process theory in its decision,[135] which is analyzed under the Due Process Clause of the Fourteenth Amendment.[136] *Roe* specifically recognized the right to have an abortion as a fundamental right entitled to constitutional privacy protections.[137] However, the Court also noted that the right to privacy was not absolute.[138] Rather, "where certain fundamental rights are involved, the Court has held that regulation limiting these rights may be justified by a compelling state interest, and that legislative enactments must be narrowly drawn to express only the legitimate state interests at stake."[139] Since *Roe*, the Court has identified the following as fundamental rights under decisional privacy: "marriage, procreation, contraception, family relationships, child rearing, education" and "certain intimate conduct."[140] These decisions indicated a shift in the Court towards

129. Griswold v. Connecticut, 381 U.S. 479 (1965).

130. *Id.* at 485–86.

131. *Id.* at 484 (noting that the First, Third, Fourth, Fifth, and Ninth Amendments contain privacy implications which formed the basis for a general constitutional right to privacy).

132. *Id.* at 494 (Goldberg, J., concurring) ("[T]he right of privacy is a fundamental personal right, emanating 'from the totality of the constitutional scheme under which we live.'") (citing Poe v. Ullman, 367 U.S. 497, 521 (1961)).

133. Roe v. Wade, 410 U.S. 113 (1973).

134. *Id.* at 153.

135. *See* Jed S. Crumbo, *Constitutional Law—Right to Privacy—Government Contract Employees' Right to Informational Privacy*, 79 TENN. L. REV. 417, 422 (2012).

136. *Id.*

137. *Roe*, 410 U.S. at 153.

138. *Id.* at 155.

139. *Id.* at 155–56 (internal citations omitted).

140. Lawrence v. Texas, 539 U.S. 558, 573–74 (2003).

recognizing a broader scope of personal information under the substantive due process clause of the Fourteenth Amendment.

Although the Supreme Court has recognized decisional privacy interests, the Court's stance in the realm of informational privacy is less clear. In 1977, for the first time, the Court tangentially addressed the right to informational privacy in two cases: *Whalen v. Roe* and *Nixon v. Administrator of General Services*.[141] While the Court in both cases identified the existence of a right to informational privacy, the Court did not define the scope of the right.[142]

In *Whalen*, the issue before the Court was whether New York violated privacy interests by maintaining a centralized computer database that contained the names and addresses of individuals who obtained certain prescription drugs.[143] The Court recognized that there are two types of privacy interests: (1) "the individual interest in avoiding disclosure of personal matters;"[144] and (2) "the interest in independence in making certain kinds of important decisions."[145] Lower courts have acknowledged the first privacy interest—avoiding disclosure of personal matters—as the Supreme Court's recognition of the right to informational privacy.[146] In relation to the informational privacy claim, the plaintiffs argued that the availability of the information created concern that the information would become publically known and negatively impact their reputations.[147] Ultimately, the *Whalen* Court did not find that New York's database collection program violated the Constitution because the security provisions were adequate to protect against unwarranted disclosures, and certain disclosures were already required under other law.[148]

The Court acknowledged in *Whalen* that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive

141. Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 455 (1977); Whalen v. Roe, 429 U.S. 589, 600 (1977).

142. *See* Crumbo, *supra* note 135, at 420 n.24 (noting that "the courts of appeals have been unable to develop uniform jurisprudence across the circuits and have adopted substantially different approaches to analyzing and deciding informational privacy cases").

143. *Whalen*, 429 U.S. at 591.

144. *Id.* at 599 (footnote omitted).

145. *Id.* at 599–600 (footnote omitted).

146. Lin, *supra* note 20, at 1094.

147. *Whalen*, 429 U.S. at 600.

148. *Id.* at 600–02; *see, e.g., id.* at 602 n.29 (explaining that there are existing "statutory reporting requirements relating to venereal disease, child abuse, injuries caused by deadly weapons, and certifications of fetal death").

government files."[149] However, the Court noted that it did not need to decide "any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions."[150] Thus, the Court explicitly chose not to address the issue of whether similar statutes would violate a constitutional right to informational privacy.

Four months after the *Whalen* decision, the Supreme Court decided another informational privacy case, *Nixon v. Administrator of General Services*. The *Nixon* case involved a lawsuit by President Richard Nixon challenging the Presidential Recordings and Materials Preservation Act, which would have required President Nixon to turn over his tape recordings and presidential papers for review.[151] The Court found that Nixon's interest in retaining his tape recordings was weaker than the claim in *Whalen*.[152] The Court found that President Nixon had a legitimate expectation of privacy in his "private communications."[153] However, after weighing President Nixon's privacy interest against the public interest in subjecting administrative materials to archival screening, the Court found the public interest to be paramount.[154] Ultimately, the Supreme Court did not find a violation of President Nixon's informational privacy rights.

Nixon and *Whalen* made significant pronouncements in the area of informational privacy. First, the Supreme Court noted that there are two situations when informational privacy is applicable—government collection of information and dissemination of information.[155] Second, the Court noted that although an expectation of privacy exists for private information,[156] the expectation is diminished when the information is regularly disclosed to third parties.[157] Third, the Court identified an interest-balancing approach when evaluating informational privacy claims, where the interest of

149. *Id.* at 605.

150. *Id.* at 605–06.

151. Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 429–33 (1977).

152. *Id.* at 459.

153. *Id.* at 458–59.

154. *Id.*

155. *Id.* at 599 n.24 (noting that the right to informational privacy "applies both when an individual chooses not to disclose highly sensitive information to the government and when an individual seeks assurance that such information will not be made public").

156. *Id.* at 455–58.

157. Whalen v. Roe, 429 U.S. 589, 602 (1977).

the state is weighed against the interest against disclosure.[158] The Court's opinions in *Whalen* and *Nixon* seemed to indicate a departure from the traditional right to privacy analysis under the Fourteenth Amendment.[159] The Court had previously suggested in *Paul v. Davis* that zones of privacy analysis might be necessary when assessing a right to privacy claim against the right of the government to require disclosure.[160]

After *Nixon* and *Whalen*, the Supreme Court did not address informational privacy rights for thirty years. In 2010, the Court decided *National Aeronautics & Space Administration v. Nelson*, which brought the issue back.[161] This case involved the California Jet Propulsion Laboratory ("JPL"), a National Aeronautics and Space Administration ("NASA") facility.[162] NASA is an independent federal agency that oversees the federal government's "space activities."[163] JPL is operated by the California Institute of Technology under a government contract, but is staffed only by contract employees.[164] Prior to 2007, JPL employees were not required to undergo background checks for employment.[165] The issue in this case arose from a recommendation made by the 9/11 Commission requiring a uniform identification standard, which would require all employees with long-term access to federal facilities to

158. *Nixon*, 433 U.S. at 458; *Whalen*, 429 U.S. at 602. *See* Colin M. O'Brien, *Homeland Security Presidential Directive-12, Background Investigation, and Informational Privacy Rights*, 80 MISS. L.J. 299, 325–26 (2010) (Noting that *Nixon* and *Whalen* identified the following interests: (1) the nature of the information collected or disseminated—the more commonly this information is disclosed by the individual, the weaker the individual's interest in protecting his or her privacy; (2) the scope of the information collected in comparison to the scope of information in which the individual has a privacy interest; (3) the existence of safeguards to protect against the unauthorized dissemination of the collected information will weigh in favor of the government; and (4) the availability of practical alternative means of achieving the government's purpose in collecting or disseminating the information.) (internal citations omitted).

159. *See* Helen L. Gilbert, *Minor's Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375, 1380 (2007).

160. Paul v. Davis, 424 U.S. 693, 712–13 (1976) (noting that publically posting a photograph of the defendant did not invoke the Fourteenth Amendment because it did not fall within a zone of privacy).

161. Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746 (2011).

162. *Id.* at 751–52.

163. *Id.* at 751.

164. *Id.* at 752.

165. *Id.* (noting that only federal civil servants had been required to undergo background checks, not contract employees).

submit to a background check.[166] Any JPL employee who refused to comply would face termination.[167] The process entailed filling out two documents: (1) SF-85, a questionnaire; and (2) Form 42.[168] SF-85 requested biographical information, information about citizenship, military status, and whether the employee had "'used, possessed, supplied, or manufactured illegal drugs' in the last year."[169] If the employee answered "yes" to the drug-affiliation question, the employee was required to provide information about any treatment or counseling he or she received.[170] Form 42 was a reference sheet, which was meant for the JPL employee's landlords and references.[171] The reference sheet asked questions about the references' knowledge of the employees, such as the employee's drug use, unlawful conduct, financial integrity, mental health, and general conduct.[172]

Before the case went to the Supreme Court, the Ninth Circuit Court of Appeals held that mandatory disclosures of drug use, possession, supply, and manufacture were "necessary to further the compelling interest" in combating illegal drug use.[173] However, it found that the portion of the SF-58 questionnaire requiring disclosure of drug treatment and counseling likely violated the Constitution.[174] The Ninth Circuit noted that the government had not provided any compelling interest for requiring disclosure, especially since treatment and counseling would create a lesser need for disclosure.[175] Further, the Ninth Circuit found Form 42's open-ended questions to be particularly problematic.[176] Not only did the questions implicate the right to privacy, but the disclosure requirements were not narrowly tailored to meet the government's purported interests of ensuring the security of its facilities and verifying the identity of its contractors.[177]

When *Nelson* finally came before the Supreme Court, the Court again refrained from providing further guidance or specific contours

166. *Id.*
167. *Id.*
168. *Id.* at 752–53.
169. *Id.* at 753 (internal citations omitted).
170. *Id.*
171. *Id.*
172. *Id.*
173. Nelson v. Nat'l Aeronautics & Space Admin., 530 F.3d 865, 879 (9th Cir. 2008).
174. *Id.*
175. *Id.*
176. *Id.* at 880.
177. *Id.*

on whether there is a constitutional right to informational privacy.[178] Writing for the Court, Justice Samuel Alito held that, for purposes of SF-85 and Form 42, the Privacy Act's safeguards against public disclosure were sufficient to protect the JPL employees.[179] For purposes of the decision, the Court assumed that the rights at issue "implicate[d] a privacy interest of constitutional significance."[180] However, the Court declined to provide any further guidance or clear answer on the informational privacy claim, simply stating that it "assumed without deciding" whether the right existed.[181] Although the Court's ultimate holding was unanimous, the Court differed in its rationale. Both Justices Antonin Scalia and Clarence Thomas argued that a federal constitutional right to informational privacy does not exist.[182]

Pertinent to this Note, a significant portion of the opinion is the Court's emphasis of the government's decision-making role. The Court noted that the government acting as an employer, rather than a sovereign, had a significant interest in conducting background checks of its employees.[183] The Court grants much higher deference to the government when the government acts as an employer making managerial decisions in running their place of employment, than when the government acts as law enforcement.[184]

3. Without Guidance From the Supreme Court, the Circuit Courts Have Developed an Unclear and Fragmented Patchwork of Informational Privacy Doctrine

With the exception of the D.C. Circuit, all of the circuit courts[185] have recognized a constitutional right to informational privacy.[186] Despite recognizing this right, however, the circuit courts are

178. Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746, 751 (2011) (holding "that the challenged portions of the Government's background check do not violate [the right to informational privacy]" and again "assum[ing], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*").

179. *Id*. at 757.

180. *Id.* at 756.

181. *Id.* at 751.

182. *Id.* at 764 (Scalia, J., concurring).

183. *Id.* at 758.

184. *Id.* at 757–58.

185. Am. Fed'n of Gov't Emps. v. Dept. of Hous. & Urban Servs., 118 F.3d 786, 788 (D.C. Cir. 1997) (noting that there are "grave doubts" about whether a constitutional right to informational privacy exists).

186. *See* Gilbert, *supra* note 159, at 1381 n.44.

fragmented on their approach in addressing the issue. As in *Whalen* and *Nixon*, there are two steps in the analytic framework of the circuit courts.[187] First, the courts determine whether a privacy right exists in either the collection or dissemination of information.[188] Second, if a privacy interest is implicated, the circuit courts then weigh the privacy interest against disclosure in light of the government collecting or distributing the information.[189] In addressing each step, the circuit courts have adopted a variety of approaches for each step.

A circuit court will first ask whether an individual's privacy right is implicated. The majority of circuit courts have broadly interpreted the right of informational privacy.[190] These courts ask whether an individual has a "reasonable" or "legitimate" expectation of privacy, and then assess whether the interest is of a sufficiently personal nature to infringe on their expectation of privacy.[191] Under this approach, the circuit courts have recognized several categories of information that should be entitled to constitutional protection:[192] medical information,[193] financial information,[194] sexual information,[195] and certain personal information, such as social security numbers.[196]

187. *See* O'Brien, *supra* note 158, at 326 (noting that the courts generally "(1) determin[e] if an individual's privacy interest is implicated by the collection or dissemination of information; and (2) if so, weigh[] the governmental interest in collection or dissemination of that information against the individual interests in avoiding disclosure.").

188. *See, e.g.*, Kallstrom v. City of Columbus, 136 F.3d 1055, 1062–64 (first evaluating whether there were privacy interests in the plaintiffs' personal security and bodily integrity).

189. *See e.g., id*. at 1064–65 (evaluating second whether the plaintiff's interest outweighs the government interest); *see also* O'Brien, *supra* note 158, at 326. This approach is akin to the approach adopted in *Nixon* and *Whalen*. *See id.* at 325.

190. *See* Gilbert, *supra* note 159, at 1382 nn.53 – 59 (synthesizing lists of numerous cases where lower courts applied informational privacy rights to a wide spectrum of information).

191. Gilbert, *supra* note 159, at 1832. *See* Jeffery S. Grand, *The Blooding of America: Privacy & the DNA Dragnet*, 23 CARDOZO L. REV. 2277, 2313–14 (2002). *See also Fraternal Order of Police v. City of Philadelphia,* 812 F.2d 105, 112–13 (3d Cir. 1987) ("In determining whether information is entitled to privacy protection, we have looked at whether it is within an individual's reasonable expectations of confidentiality.").

192. O'Brien, *supra* note 158, at 333–35.

193. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.").

194. Plante v. Gonzales, 575 F.2d 1119, 1135 (5th Cir. 1978).

However, the Sixth Circuit's approach is more limited.[197] In fact, the Sixth Circuit appears to grant the least amount of protection to informational privacy rights[198] by recognizing the right to privacy only in cases that implicate fundamental rights or other constitutional provisions.[199] For instance, the Sixth Circuit recognized an informational privacy violation in *Kallstrom v. City of Columbus* where a group of police officers involved in a high-profile gang prosecution sued the City of Columbus.[200] The officers claimed the City of Columbus violated their right to privacy by distributing sensitive personal information (including phone numbers, driver's licenses, and family members' names, addresses, and phone numbers) to a defense attorney, who then disseminated the information to several gang members.[201] The Sixth Circuit held that the dissemination of the officers' information implicated their privacy interests because such dissemination endangered the officers' and their families' lives, thus violating fundamental liberty interests in personal security and bodily integrity that is recognized by the Supreme Court.[202] Other fundamental rights recognized by the Supreme Court[203] include: child rearing,[204] family relationships,[205]

195. Bloch v. Ribar, 156 F.3d 673, 685 (6th Cir. 1998). *See* Walls v. City of Petersburg, 895 F.2d 188, 193 (4th Cir. 1990).

196. In re Crawford, 194 F.3d 954, 958 (9th Cir. 1999) (recognizing that "the indiscriminate public disclosure" of Social Security numbers could implicate a constitutional informational privacy right, but ultimately concluding that the government's interest in making bankruptcy documents available to the public outweighed nondisclosure). *See also Kallstrom*, 136 F.3d at 1062–63 (noting that there is an interest in protecting personal security and bodily integrity).

197. O'Brien, *supra* note 158, at 328.

198. *See* Lee v. City of Columbus, 636 F.3d 245, 260 (6th Cir. 2011) (noting that the Sixth Circuit has only recognized an informational privacy interest in two situations: "(1) where the release of personal information could lead to bodily harm . . . and (2) where the information released was of a sexual, personal, and humiliating nature") (internal citations omitted).

199. Gilbert, *supra* note 159, at 1382–83. *See* Overstreet v. Lexington-Fayette Urban Cnty. Gov't, 305 F.3d 566, 574 (6th Cir. 2002) (noting that "this Court has not strayed from its holding, and continues to evaluate privacy claims based on whether the interest sought to be protected is a fundamental interest or an interest implicit in the concept of ordered liberty"). This approach has been interpreted from the Supreme Court's opinion in *Paul v. Davis*. *See* Paul v. Davis, 424 U.S. 693, 713 (1976) (noting that marriage, procreation, contraception, family relationships, child rearing, and education are fundamental rights).

200. *Kallstrom*, 136 F.3d at 1059.

201. *Id.*

202. *Id.* at 1062.

203. *See Paul*, 424 U.S. at 713.

204. Pierce v. Soc'y of Sisters, 268 U.S. 510, 534 (1925).

contraception,[206] procreation,[207] and marriage.[208] In the context of informational privacy on social media, the restrictive nature of the fundamental rights approach is likely too limited. It fails to account for a host of information that the Supreme Court has not yet considered "fundamental" but, nonetheless, implicates significant privacy concerns, such as an individual's HIV status or other medical information, which might be accessible on social media.[209]

The Eighth Circuit's approach somewhat mirrors the restrictive view of the Sixth Circuit, but is slightly more inclusive and contains language that follows the majority of the circuits.[210] Like the Sixth Circuit, the Eighth Circuit applies the informational privacy right to fundamental rights, but also applies the right to matters involving "highly personal medical or financial information."[211] However, the Eight Circuit restricts right to privacy claims to violations that are of "shocking degradation or . . . egregious humiliation."[212] Similar to the limited reach of the "fundamental rights" approach of the Sixth Circuit, the Eighth Circuit's approach is also restrictive and might not reach information that other circuit courts protect, such as medical health records.[213]

After the courts recognize a right to informational privacy, the second step in the inquiry is to assess the level of scrutiny attached to government intervention in that area. A majority of circuit courts utilize a balancing test[214] to determine if the societal interest in

205. Prince v. Massachusettes, 321 U.S. 158, 167 (1944).

206. Eisenstadt v. Baird, 405 U.S. 438, 454–55 (1972).

207. Skinner v. Okla. *ex rel.* Williamson, 316 U.S. 535, 541 (1942).

208. Loving v. Virginia, 388 U.S. 1, 12 (1967).

209. *See* Gilbert, *supra* note 159, at 1382–83 (noting the broader coverage of the "legitimate expectation of privacy" approach).

210. There have been instances where the Eighth Circuit has used the legitimate expectation language utilized by a majority of the Circuit Courts. *See, e.g.*, Eagle v. Morgan, 88 F.3d 620, 625 (1996) (noting that determining privacy violations requires "examin[ing] the nature of the material opened to public view to assess whether the person had a legitimate expectation that the information would remain confidential while in the state's possession."). However, the Eighth Circuit's language is limited by the requirement that the disclosure amounts to a "shocking degradation." O'Brien, *supra* note 158, at 330 n.150.

211. Alexander v. Peffer, 993 F.2d 1348, 1350–51 (8th Cir. 1993).

212. *Eagle*, 88 F.3d at 625 (quoting *Alexander*, 993 F.2d at 1350).

213. Gilbert, *supra* note 159, at 1383.

214. *See* Fadjo v. Coon, 633 F.2d 1172, 1176 (5th Cir. 1981) ("[W]here the privacy right is invoked to protect confidentiality, a balancing standard is appropriate as opposed to the compelling state interest analysis involved when autonomy of decisionmaking is at issue."); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980)

disclosure outweighs the privacy interest.[215] Courts have derived the balancing approach from the Supreme Court's decisions in *Whalen* and *Nixon*.[216] In balancing these interests, many of the courts apply some or all of the factors highlighted by the Third Circuit in *United States v. Westinghouse Electric Corp*.[217] At issue before the Third Circuit in *Westinghouse* was whether an employer was required to comply with a government subpoena that requested medical records of its employees during an investigation, and charged the employer with maintaining hazardous materials.[218] The Third Circuit held that the public interest in the government's investigation was sufficient to require disclosure; however, the government was required to notify the employees whose records were sought for examination and those employees were allowed to raise privacy claims.[219] Commentators have viewed this balancing approach as a type of intermediate scrutiny.[220] The *Westinghouse* factors include:

> (1) [T]he type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (6) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[221]

("[W]e must engage in the delicate task of weighing competing interests."); Plante v. Gonzalez, 575 F.2d 1119, 1134 (5th Cir. 1978) ("[W]e believe that the balancing test, more common to due process claims, is appropriate here.").

215. *See, e.g.*, *Westinghouse*, 638 F.2d at 578 (noting that "[i]n the cases in which a court has allowed some intrusion into the zone of privacy surrounding medical records, it has usually done so only after finding that the societal interest in disclosure outweighs the privacy interest on the specific facts of the case."). *See also* Grand, *supra* note 191, at 2316 (noting that the circuits employing the balancing approach vary on "whether the government interest must be legitimate, compelling, substantial, or merely described as a general interest").

216. *See Fajdo*, 633 F.2d at 1176.

217. *See Westinghouse*, 638 F.2d 570.

218. *Id.* at 573.

219. *Id.* at 581.

220. O'Brien, *supra* note 158, at 338 (internal citations omitted).

221. *Westinghouse*, 638 F.2d at 579.

In contrast to the balancing approach used by a majority of the circuit courts, the Sixth, Fourth, and Tenth Circuits[222]—as well as those circuit courts that utilize the fundamental rights approach—apply a strict scrutiny analysis to informational privacy rights deemed fundamental.[223] Under a strict scrutiny approach, the government must show a compelling interest and that the law or regulation is narrowly tailored to meet the government's interest.[224]

III. The Supreme Court Must Recognize a Constitutional Right to Informational Privacy

Thus far, this Note has illustrated one significant problem in the realm of informational privacy—potential government access to social media accounts containing sensitive, private information. However this is only one small facet of the informational privacy debate. Our online presence is expansive and will only continue to expand as technology advances. Therefore, this Note argues that the Supreme Court should recognize a constitutional right to informational privacy under the Fourteenth Amendment. Not only would this clarify the scope of this important right among the fragmented circuit courts, but it also would provide for greater information security when access to this information is growing faster than ever before.

This Note proposes that the Supreme Court apply: (1) the "legitimate expectation of privacy" standard to determine if an informational privacy right is implicated; and (2) if an informational privacy right is implicated, that the Court apply the "intermediate scrutiny" balancing test adopted by the Third Circuit in *Westinghouse*.

First, the "legitimate expectation of privacy" standard should be employed because it is more deferential to precedent than the "fundamental rights" approach employed by the Sixth Circuit. The Supreme Court's decisions in *Whalen* and *Nixon* indicate that the privacy interest in confidentiality extends beyond the "fundamental

222. Gilbert, *supra* note 159, at 1386 n.81 (citing Kallstrom v. City of Columbus, 136 F.3d 1055, 1064 (6th Cir. 1998); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) (internal citation omitted).

223. *See, e.g.*, Bloch v. Ribar, 156 F.3d 673, 686 (6th Cir. 1998). *See also* O'Brien, *supra* note 158, at 337.

224. *Bloch*, 156 F.3d at 686. *See Kallstrom*, 136 F.3d at 1065 (reasoning that the government had an interest in public disclosure of agency records but disclosing extensive information, such as family member names, driver's licenses, and phone numbers, to a defense attorney were not narrowly tailored to serve the government's interests). *See also* Gilbert, *supra* note 159, at 1387.

rights" listed in the Court's opinion in *Paul*.[225] Further, as previously discussed, the Sixth and Eighth Circuits' fundamental rights-focused approaches are too limited. Finally, the "legitimate expectation of privacy" approach is a useful standard to determine if a privacy concern is implicated because it is flexible and has room to account for societal changes.[226]

In applying the "legitimate expectation of privacy standard" to the social media context, the Supreme Court should be aware of the public and private profile options on many social media websites, such as Facebook.[227] Public profile searches pose different privacy concerns than private searches precisely because the user has not chosen to limit the information available to the public. Thus, based on the "legitimate expectation of privacy standard" proposed by this Note, this distinction between "private" and "public" profiles matters; private profiles would be protected, but public profiles would not.[228]

Second, the balancing approach adopted in *Westinghouse*,[229] as a form of intermediate scrutiny, is also ideal because it provides sufficient room to address both government and individual interests. This portion of the test will balance the government's interest in acquiring the information against the individual's right to confidentiality in that information. Most significantly, this test is in accordance with the Supreme Court's prior precedents in *Roe* and *Whalen*, in which the Court also engaged in balancing inquiries.[230]

Finally, it does not appear that the Court's decision in *Nelson* would preclude a finding that a right to informational privacy exists. Though the Court chose not to hold that a right to informational privacy existed, the Court did not foreclose a finding of this right in

225. *See* Fadjo v. Coon, 633 F.2d 1172, 1176 (5th Cir. 1981). *See also* Gilbert, *supra* note 159, at 1387.

226. For instance, fifty years ago individuals may not have considered that there should be privacy in cellular phone "text-messaging" communication, because the technology did not exist. However, the legitimate expectation of privacy approach may allow for recognition of "text-messaging" communication now because the technology is widely used.

227. *See supra* Part I.A.

228. Public profiles are considered to be in the public domain. Courts consider this "fair game." Ebnet, *supra* note 107, at 325.

229. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 579 (3d Cir. 1980).

230. *See* Gilbert, *supra* note 159, at 1387 (suggesting that this approach "may best track the Supreme Court's balancing of factors in both *Whalen* and *Nixon*.").

the future. Rather, the Court seemed to punt the issue for another day.[231]

Conclusion

Individuals need safeguards against government interference with personal information. Public employer requests for an applicant's social media information create constitutional privacy concerns. The widespread use of social media and the concentration of information available online have changed privacy norms. The potential for a breach in information security, whether simply from the government possessing the information or accidental government disclosures, highlights the need for heightened protection.[232] Although state and legislative solutions attempt to address the problems posed by employer access to social media information, the protection is still inadequate for the reasons indicated in this Note. Thus, the Supreme Court should recognize a constitutional right to informational privacy under the Fourteenth Amendment to ensure more comprehensive protection of information in our ever-expanding technological age.

231. Nat'l Aeronautics & Space Admin. v. Nelson, 131 S. Ct. 746, 751 (2011) ("We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*.").

232. *See* Chlapowski, *supra* note 113, at 134.

* * *