RETHINKING INFORMATION PRIVACY IN AN AGE OF ONLINE TRANSPARENCY

*Robert Sprague**

INTRODUCTION

Wikipedia Foundation's Ex-Chief Operating Officer Has a Criminal Record.[1] The type of headline every employer dreads seeing in the newspaper. Carolyn Bothwell Doran had been promoted from a part-time bookkeeper for the Wikimedia Foundation (the foundation that runs and accepts donations for the online encyclopedia, Wikipedia) and spent six months as chief operating officer, responsible for personnel and financial management.[2] But, the Wikimedia Foundation had failed to run a rudimentary background check—if it had, it would have discovered that Doran had spent time in prison for a hit-and-run accident, had multiple drunken-driving convictions, and had run-ins with authorities for theft, writing bad checks, and wounding her boyfriend with a gunshot to the chest.[3] No wonder employers have begun turning to the Internet as a source of job applicant pre-screening.[4]

I. ONLINE TRANSPARENCY

The Internet has changed dramatically since its inception in the 1960s (as an information sharing network used by the military, scientists, and academics), and since it was opened to the public in the mid-1990s.[5] The Internet, and more specifically, the World Wide Web,

* J.D., M.B.A., Assistant Professor, University of Wyoming College of Business, Department of Management and Marketing.

1. *See* Brian Bergstein, *Wiki Officer's Sketchy History*, MERCURY NEWS, Dec. 22, 2007, http://www.mercurynews.com/business/ci_7786536.

2. *Id.*

3. *Id.*

4. *See, e.g.*, Ellen Nakashima, *Harsh Words Die Hard on the Web*, WASH. POST, Mar. 7, 2007, at A1.

5. *See* Barry M. Leiner et al., *A Brief History of the Internet*, Dec. 10, 2003,

is where more and more people first turn for news,[6] entertainment,[7] and commerce.[8] Particularly, the information sharing nature of the Internet has thrived in the first decade of the Twenty-first century. There are over seventy million online Web logs (known as "blogs")[9] chronicling every conceivable topic, many with the capability for readers to post comments to entries. Together, the two most popular social networking sites, MySpace and Facebook, which allow users to create online profiles and share information, photos, and videos with other users, boast nearly 100 million users.[10]

Between blogs and social networking sites, a staggering amount of personal information is being published online.[11] For a new generation, both authenticity and reputation come from online exposure.[12] "People are not just findable, they are knowable."[13] And even those who do not wish to actively participate online still leave "digital footprints."[14] The digitization of public records, combined with the increasing accuracy of search engines, has made it easier for the general population—including prospective employers—to join creditors, law enforcement, and professional investigators to discover individuals' personal data.[15]

A generation is emerging whose members post their opinions and

---

http://www.isoc.org/internet/history/brief.shtml.

6. *See, e.g.*, JOHN B. HORRIGAN, PEW INTERNET & AM. LIFE PROJECT, ONLINE NEWS: FOR MANY HOME BROADBAND USERS, THE INTERNET IS A PRIMARY NEWS SOURCE (2006), *available at* http://www.pewinternet.org/pdfs/PIP_News.and.Broadband.pdf (noting that, in a typical day by the end of 2005, 50 million Americans got news online).

7. The Writers Guild of America strike that began in late 2007 centered principally on how much writers should be paid when their work is distributed digitally for viewing on computers. *See* Sarah McBride & Rebecca Dana, *Scenes From Next Week…?*, WALL ST. J., Nov. 1, 2007, at B1.

8. "Cyber Monday" has entered the lexicon, describing the Monday after Thanksgiving when employees use their employers' high-speed Internet access to conduct their online holiday shopping. *See* Mylene Mangalindan, *'Cyber Monday' Sets Record For Retail Sales on the Web*, WALL ST. J., Nov. 28, 2007, at B2.

9. Posting of David Sifry to Sifry's Alerts: The State of the Live Web, http://www.sifry.com/alerts/archives/000493.html (Apr. 5, 2007) (recording over 70 million blogs as of April 2007, with some 120,000 new blogs created every day).

10. *See* Brad Stone, *Facebook Goes Off the Campus*, N.Y. TIMES, May 25, 2007, at C2.

11. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 29 (2007).

12. *See* Clive Thompson, *The See-Through CEO*, WIRED, Apr. 2007, at 136-38; *See generally* SOLOVE, *supra* note 11.

13. MARRY MADDEN ET AL., DIGITAL FOOTPRINTS: ONLINE IDENTITY MANAGEMENT AND SEARCH IN THE AGE OF TRANSPARENCY, PEW INTERNET & AMERICAN LIFE PROJECT 4 (Dec. 16, 2007), *available at* http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf.

14. *Id.*

15. *Id.* at 3.

live their daily lives online.[16] Virtual environments originated within subsets of society, with their own ethos developed by largely anonymous, tech-savvy insiders.[17] Online social networking has now gone mainstream. While many foundations of the virtual world still exist—unbridled conversations, baring souls online, presumed anonymity—the virtual world is also now more scrutinized by third parties who do not necessarily share "the Net culture's free-wheeling values."[18] Additionally, what may be merely posturing in front of online friends, can be viewed and taken seriously by an "outsider," such as a prospective employer.[19] "Poorly chosen words," or a photograph published online, could have career-altering consequences.[20]

II. EMPLOYMENT PRE-SCREENING

Employers are not just worried about embarrassing publicity when an employee's, checkered past becomes a news item.[21] Surveys have

16. *See* David Rosenblum, *What Anyone Can Know: The Privacy Risks of Social Networking Sites*, 5 IEEE SECURITY & PRIVACY 40, 40 (May/June 2007), *available at* http://csdl.computer.org/dl/mags/sp/2007/03/j3040.pdf.

17. *Id.* at 40-41.

18. *Id*. at 41. *See also* Nancy Hass, *In Your Facebook.com*, N.Y. TIMES, Jan. 8, 2006, § 4A (discussing a "Facebook war" between college students and campus police, in which students "caught" campus police monitoring student Facebook pages when students posted notices of a fake party that police responded to); Jared Miller, *UW Lifts Student Suspensions*, CASPER STAR-TRIBUNE, Dec. 11, 2007, http://www.trib.com/articles/2007/12/11/news/wyoming/ab805643dafc47b2872573ae00063d63.txt (discussing the suspension of four University of Wyoming students in response to pictures from a fraternity party posted on one of the student's Facebook page); Libby Sander, *New Software to Monitor Athletes' Web Sites Troubles Legal Experts*, CHRON. HIGHER EDUC., Jan. 14, 2008, http://chronicle.com/daily/2008/01/1210n.htm (analyzing YouDiligence, a "social-network monitoring service" being marketed to college athletics departments which promises to search Facebook and MySpace for up to 500 objectionable words and phrases ranging from profanity to slang used to describe drug use).

19. *See, e.g.*, Alan Finder, *When a Risqué Online Persona Undermines a Chance for a Job*, N.Y. TIMES, June 11, 2006, at 1 (discussing the ramifications of a job applicant's Facebook page describing his interests as "smokin' blunts," shooting people, and obsessive sex). Online postings can also be taken out of context, resulting in serious consequences. *See, e.g.*, Andy Guess, *Inside Higher Ed, Maybe He Shouldn't Have Spoken His Mind* (Jan. 11, 2008), http://www.insidehighered.com/news/2008/01/11. The blog discusses a Valdosta State University sophomore who was administratively withdrawn because he presented a "clear and present danger to [the] campus" based on a posting on his Facebook page entitled, "Shoot it. Upload it. Get Famous. Project Spotlight is searching for the next big thing. Are you it?" However, the university administration failed to read the words in their proper context. "Shoot it" merely referred to an online digital video contest. *Id.*

20. *See, e.g.*, Randall Stross, *How to Lose Your Job on Your Own Time*, N.Y. TIMES, Dec. 30, 2007, § 3, at 3.

21. *See supra* text accompanying notes 1-3. *See also* Peter Elkind, *Can This Man Save*

indicated that nearly half of job applicants lie about their work history and education.[22] Employers also seek to find individuals who will work and perform well within the organization.[23] The Internet provides a potential, and tempting, treasure trove of information about prospective employees.

Indeed, an employer may even argue that it is legally obligated to Google its job applicants.[24] The doctrine of negligent hiring has evolved to impose liability on employers in certain situations where third parties are harmed as the result of conduct by an employee, even where the employee was acting outside the scope of employment.[25] The modern application of the negligent hiring theory imposes liability on an employer when it "places an unfit person in an employment situation that entails an unreasonable risk of harm to others."[26] "[A]n employer owes a duty of reasonable care to third persons in the hiring and retention of employees whose aggressive or reckless characteristics or lack of competence in the performance of their employment duties may endanger such third persons."[27] This duty requires that employers investigate employment candidates.[28] "Negligent hiring occurs when, prior to the time the employee is actually hired, the employer knew or should have known of the employee's unfitness, and the issue of liability primarily focuses upon the adequacy of the employer's pre-employment investigation into the employee's background."[29]

A negligent hiring claim will arise where there is actual injury to a

RadioShack?, FORTUNE, Mar. 13, 2007, http://money.cnn.com/magazines/fortune/fortune_archive/2007/03/19/8402335/index.htm (recounting that RadioShack's former CEO, David Edmondson, resigned following a local newspaper report that he had been arrested for drunk driving and had fabricated his bachelor's degree).

22. *See* Inst. of Mgmt. & Admin., *How to Ferret Out Instances of Résumé Padding and Fraud*, COMPENSATION & BENEFITS FOR L. OFFICES, 3, 5 (June 2006).

23. *See* Chris Piotrowski & Terry Armstrong, *Current Recruitment and Selection Practices: A National Survey of Fortune 1000 Firms*, 8 N. AM. J. PSYCHOL. 489, 489 (2006).

24. "Googling" is derived from the Internet search site, http://www.google.com, operated by Google, Inc. "To google," has entered the English lexicon as a verb describing the act of searching the Internet for a person, place, event, story, or document. Thus, Googling someone refers to searching the Internet for information about that person.

25. Rodolfo A. Camacho, *How to Avoid Negligent Hiring Litigation*, 14 WHITTIER L. REV. 787, 790 (1993).

26. Rosanne Lienhard, *Negligent Retention of Employees: An Expanding Doctrine*, 63 DEF. COUNS. J. 389, 389 (1996).

27. Di Cosala v. Kay, 450 A.2d 508, 510 (N.J. 1982).

28. Garcia v. Duffy, 492 So. 2d 435, 438 (Fla. Dist. Ct. App. 1986).

29. *Id.* (citing Williams v. Feathersound, Inc., 386 So. 2d 1238 (Fla. Dist. Ct. App. 1980), *petition for review denied*, 392 So. 2d 1374 (Fla. 1981).

third party which could have been prevented had the employer not put the employee in a position to cause that harm.[30] For example, the owner of an apartment complex should not give a master key to an employee when a background check would have revealed that the employee had a criminal record.[31]

While employers use pre-screening techniques (such as personality tests and background checks)[32] to weed out undesirable candidates, they also use them to help identify candidates who possess desirable traits.[33] In this regard, because employers are most likely not going to receive any substantive information about an applicant from his references, they may be compelled to search the Internet to gather information about the applicant's character traits.[34] Employers perform background checks and review employment histories of applicants based on the notion that "past performance is the best predictor of future behavior."[35] However, former employers fear defamation suits from past employees arising from references,[36] despite a legal environment described by Finkin as "hospitable to the free exchange of information about prospective employees . . . ."[37] Googling job applicants offers a compelling substitute for references, as a search is more likely to reveal (snippets of) the character of the applicant.

Traditional, pre-screening techniques are also severely restricted by various laws. For example, an employer may not ask questions which would allow the employer to screen applicants based on a protected class (race, color, national origin, religion, or gender) under Title VII of the Civil Rights Act of 1964.[38] Employers also face legal restrictions in the

30. *See* Ponticas v. K.M.S. Invs., 331 N.W.2d 907, 910 (Minn. 1983).

31. *See, e.g.*, *id.* at 909. The employer, an owner of an apartment building, was held liable for the rape of a tenant by the manager on the theory of negligent hiring. The employer hired the manager, and therefore, had the duty to exercise reasonable care when hiring individuals who possess job duties that may impose a threat of injury to members of public. *Id.*

32. *See* Piotrowski & Armstrong, *supra* note 23, at 492.

33. *See* Ann Marie Ryan & Marja Lasek, *Negligent Hiring and Defamation: Areas of Liability Related to Pre-Employment Inquiries*, 44 PERSONNEL PSYCHOL. 293, 304 (1991).

34. *See id.*

35. *Id.* at 293 (citation omitted).

36. Matthew W. Finkin, *From Anonymity to Transparence: Screening the Workforce in the Information Age*, 2000 COLUM. BUS. L. REV. 403, 422 (2000).

37. *Id. See generally* Ramona L. Paetzold & Steven L. Willborn, *Employer (Ir) Rationality and the Demise of Employment References*, 30 AM. BUS. L.J. 123, 136-37 (1992) (analyzing survey results indicating the relative frequency of reference-based defamation litigation probably has not increased, that defamation law still privileges employers so that (former) employees seldom win any award, and that the size of awards has declined over time).

38. 42 U.S.C. § 2000e-2(a) (2007). *See also* 29 C.F.R. § 1605.3 (2007) (regulating selection practices that discriminate on the basis of religion); 29 C.F.R. § 1606.6 (2007) (regulating selection

use of ability, integrity, and personality tests.[39] The use of any selection procedure, which has an adverse impact on the hiring, promotion, or other employment opportunities of members of any race, sex, or ethnic group, will be considered to be discriminatory unless the procedure has been validated in accordance with EEOC guidelines.[40]

If employers wish to check the credit history of an applicant, the Fair Credit Reporting Act (FCRA) requires the employer to notify the applicant in writing if a report is to be obtained,[41] and employers must notify an applicant if a credit report is used in making an adverse decision (such as deciding not to hire the applicant).[42] An employer cannot use worker compensation claims information before an offer of employment is made because the Americans with Disabilities Act prohibits employers from inquiring whether an applicant has a disability.[43] In addition, the Bankruptcy Act prohibits employers from discriminating "with respect to employment" against an individual who is seeking or has sought bankruptcy protection under the Bankruptcy Act.[44]

III. PRIVACY IN THE UNITED STATES

For the most part, restrictions on applicant pre-screening have more to do with preventing discrimination than protecting the privacy of

practices that discriminate on the basis of national origin); 29 C.F.R. § 1604.7 (2007) (regulating pre-employment inquiries as to sex); State *ex rel.* McClure v. Sports & Health Club, Inc., 370 N.W.2d 844, 849-50 (Minn. 1985) (discussing discrimination based on "religious beliefs, or lack thereof"). The Equal Employment Opportunity Commission ("EEOC") has issued guidelines for employers with suggestions as to what are permissible and impermissible employment application and interview questions under Title VII. *EEOC Guide to Pre-Employment Inquiries*, 8A [Fair Employment Practices Manual] LABOR REL. REP. (BNA) No. 695, at 443:65-66 (2002). Similarly, the EEOC has issued guidelines for employers with suggestions as to what are permissible and impermissible employment application and interview questions under the Americans with Disabilities Act (ADA). 42 U.S.C. §§ 12101-117) (2003); *EEOC: Enforcement Guidance on Pre-Employment Inquiries Under the Americans With Disabilities Act*, 8 [Fair Employment Practices Manual] LABOR REL. REP. (BNA) No. 783, at 405:7191-202 (1995).

39. 29 C.F.R. § 1607 (2007). The EEOC has issued guidelines in the use of pre-employment tests as a selection procedure. *Id.*

40. 29 C.F.R. § 1607.3(A). The guidelines essentially require that the selection procedure be linked to attributes of successful job performance. *Id.* § 1607.5(B).

41. 15 U.S.C. § 1681d(a) (2000).

42. *Id.* § 1681m(a).

43. Benjamin Belcher et al., *The Regulation of Employee Information in the United States*, 21 COMP. LAB. L. & POL'Y J. 787, 802-03 (2000).

44. 11 U.S.C. § 525(b) (2000). *See also* Belcher et al., *supra* note 43, at 804 (discussing restrictions on prospective employers' use of wage garnishment records).

applicants. As a general matter, courts will respect the privacy of job applicants in situations in which the prospective employer pries too deeply—beyond any legitimate business purpose—into applicants' personal lives.[45] The manner in which the right to privacy in the United States has developed, however, affords essentially no protection for applicants when prospective employers turn to the Internet to investigate their thoughts, musings, recreations, or even what others may have said about them online.

A. The Civil Right to Privacy

The origins of privacy protection in the United States date back to 1890, when Samuel Warren and Louis Brandeis published their seminal work, *The Right to Privacy*, recognizing a "right to be let alone[,]"[46] enforceable through legal protection from "injurious disclosures as to private matters."[47] Legend has it that the impetus for *The Right to Privacy* was Warren's dismay after reading about his own daughter's wedding being reported in the newspaper.[48] In particular, Warren and Brandeis expressed concern not only over the aggressive activities of the press, but their accompanying technology as well.[49] They argued for "a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing

45. *See, e.g.*, Johnson v. K Mart Corp., 723 N.E.2d 1192, 1196-97 (Ill. App. Ct. 2000) (denying employer's motion for summary judgment for invasion of privacy claim by employees who were subjects of reports by undercover investigators which contained personal information unrelated to workplace); Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 86 (Cal. Ct. App. 1991) (holding that questions regarding applicants' religious beliefs and sexual orientation in a 704-question psychological test were not job-related and therefore invaded applicants' privacy).

46. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). *See also* James H. Barron, *Warren and Brandeis,* The Right to Privacy, *4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875, 877 (1979) (noting courts and commentators have deemed *The Right to Privacy* to be the underpinning of the foundation for tortious claims of invasion of privacy).

47. Warren & Brandeis, *supra* note 46, at 204-05.

48. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960) (reporting that in a city and an era "in which a lady and a gentleman kept their names and their personal affairs out of the papers[,]" Warren became annoyed "when the newspapers had a field day on the occasion of the wedding of a daughter . . . ."). *But see* Barron, *supra* note 46, at 893 (noting that Warren's first daughter was only six years old in 1890, and speculating the newspaper story in question may have covered the wedding of one of Mrs. Warren's cousins). *See generally* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 128 (2007) (discussing that there were "social privacy" invasions into the lives of families similar to Warren's).

49. Warren & Brandeis, *supra* note 46, at 206.

scenes or sounds."[50] "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[51]

But to create a legal protection from public invasions of privacy, Warren and Brandeis shifted the privacy argument in the United States from an already established body of law that protected privacy as confidentiality.[52] A confidential relationship requires just that—a relationship (either through contract, trust, or both).[53] Warren and Brandeis noted, for example, that the photographic arts once required the subject to "sit" for a portrait; therefore, the law of contract or trust would protect against improper circulation of the portrait.[54] But by the late 1800's, instantaneous photography allowed for surreptitious photographs, eliminating any sort of relationship between the photographer and the subject.[55] Coupled with an expanding press, Warren and Brandeis were most concerned with a law that would prevent "injurious disclosures as to private matters" in circumstances where there was no relationship between the parties.[56] For Warren and Brandeis, this type of privacy did not arise "from contract or from special trust, but are rights as against the world."[57]

By the mid-Twentieth century, based in large part on Warren and Brandeis's *The Right to Privacy*, the majority of states recognized a civil right to privacy.[58] In 1960, Prosser identified four distinct types of invasion of privacy recognized by the courts: (1) intrusion upon seclusion, (2) public disclosure of embarrassing private facts, (3) publicity which places a person in a false light in the public eye, and (4) commercial appropriation of a person's name or likeness.[59] But an additional requirement had become ingrained in the first three types of invasion of privacy: highly offensive conduct.

Perhaps the tone was originally set in what is generally considered the first reported case recognizing a right to privacy. In *De May v.*

50. *Id.*
51. *Id*. at 195.
52. *See* Richards & Solove, *supra* note 48, at 127.
53. *See id*. at 132.
54. *See* Warren & Brandeis, *supra* note 46, at 211.
55. *See id*.
56. *Id*. at 204.
57. *Id*. at 213.
58. *See* Prosser, *supra* note 48, at 386.
59. *Id.* at 389.

Roberts,[60] a man had impersonated a doctor in order to be present when a woman gave birth.[61] Given circumstances approximating an intrusion upon seclusion, the *De May* court acknowledged the woman's right to privacy during "a most sacred" occasion, ruling "[i]t would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy."[62] Or perhaps it was set by Warren and Brandeis when they limited protection to "those persons with whose affairs the community has no legitimate concern," to prevent them "from being dragged into an undesirable and undesired publicity. . . ."[63] This tone was also reflected in the later case of *Melvin v. Reid*[64] (involving public disclosure of private facts), in which a former prostitute and murder defendant, who had abandoned her "life of shame," married and led a life in a "respectable society."[65] The community, unaware of her past, was forced to face the publication of these facts.[66] The California Court of Appeal held that the publication "of the unsavory incidents in the past life of [the woman] after she had reformed, coupled with her true name, was not justified by any standard of morals or ethics known to" the court.[67]

The modern application of intrusion upon seclusion occurs when someone "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs . . . , if the intrusion would be highly offensive to a reasonable person."[68] In the employment context, employers have generally been found to invade the privacy of employees only in the most extreme circumstances, such as prying—in detail—about an employee's sex life.[69] In one instance, a court found that an employer may have invaded the privacy of employees regarding non-work related information, based on how the employer collected the

60. 9 N.W. 146 (Mich. 1881).
61. *Id.* at 146.
62. *Id*. at 148-49.
63. Warren & Brandeis, *supra* note 46, at 214.
64. 297 P. 91 (Cal. Dist. Ct. App. 1931).
65. *Id.* at 91.
66. *Id.*
67. *Id*. at 93.
68. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
69. *Compare* Phillips v. Smalley Maint. Servs., 435 So. 2d 705, 711 (Ala. 1983) (finding an intrusion upon employee's private activities based on employer's repeated inquiries into employee's sex life), *with* Morenz v. Progressive Cas. Ins. Co., No. 79979, 2002 WL 1041760, at *2-4 (Ohio Ct. App. May 23, 2002) (finding no intrusion upon employee's private activities where employer asked employee if he was gay because the purpose of the question, asked in private, was merely to ascertain employee's job satisfaction and comfort living in the south).

information.[70] In *Johnson v. K Mart Corp.*,[71] the employer had hired private detectives to investigate employees regarding instances of theft, vandalism, sabotage, and potential drug use.[72] The investigators, posing as employees, submitted reports detailing their conversations with employees, which included information regarding the employees' family problems, health problems, and sex lives.[73] The court denied the employer's motion for summary judgment, holding there was a material issue of fact whether the employer's conduct—allowing the investigators to continue to collect personal information which had no legitimate business purpose—was offensive.[74] Of course, the circumstances would be different if the employer learned the same type of information about an employee based on information the employee published on the Internet.[75]

The publication of private facts is an invasion of privacy "if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[76] This type of invasion recognizes the difference between a "shrinking soul who is abnormally sensitive about . . . publicity" and "details of sexual relations spread before the public gaze," or highly personal portrayals of intimate private conduct.[77] Indeed, Prosser speculates that as this type of invasion has developed, Warren would not have had an actionable claim of invasion of privacy regarding the newspaper accounts which gave rise to his co-authoring *The Right to Privacy*.[78] Finally, false light invasion of privacy is not actionable unless "the false light in which the other was placed would be highly offensive to a reasonable person."[79]

U.S. privacy law is based on a paradigm that understands privacy

70. *See, e.g.*, Johnson v. K Mart Corp., 723 N.E.2d 1192 (Ill. App. Ct. 2000).

71. *Id.*

72. *See id.* at 1194.

73. *See id.* at 1196.

74. *See id.* at 1197.

75. *See, e.g.*, Robyn v. Phillips Petroleum Co., 774 F. Supp. 587, 592-93 (D. Colo. 1991) (holding that employee did not have a cause of action for an invasion of privacy, based on the presence in her personnel file of her bank statement and certain diary entries communicated to her psychiatrist, because there was no evidence employer had improperly obtained the information).

76. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

77. Prosser, *supra* note 48, at 397.

78. *See id.*

79. RESTATEMENT (SECOND) OF TORTS § 652E (1977). The fourth type of invasion, the commercial appropriation of a person's name or likeness, applies when "appropriates to his own use or benefit the name or likeness of another." *Id.* § 652C.

problems as highly offensive invasions into a person's hidden world.[80] This leaves little room for any notion of privacy relating to information a person self-publishes on the Internet, whether in a social networking profile or a blog.

B. Constitutional Right to Privacy

The constitutional right of privacy is derived from the Fourth Amendment, which creates "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[81] Since the Fourth Amendment prohibits unreasonable searches and seizures, in determining whether there has been an invasion of this constitutional right to privacy, the Supreme Court examines whether an individual has a subjective expectation of privacy, reasonable under the given circumstances.[82]

For example, when authorities, without a warrant, used an electronic tracking device inside a container of chemicals to track that container during its travels over the road, the Supreme Court found no violation of the Fourth Amendment.[83] The Court believed the agents obtained no more information than they would have through physical surveillance, concluding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[84] In more general terms, the Court's attitude is that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[85]

---

80. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1431 (2001).

81. U.S. CONST. amend. IV. Warrants authorizing a search or seizure must be based on probable cause and must describe with particularity the place to be searched, and the persons or things to be seized. *Id.* The Fourth Amendment applies to the states through the Fourteenth Amendment. O'Connor v. Ortega, 480 U.S. 709, 714 (1987). The Fourth Amendment regulates conduct by the state, and therefore, it applies to public employers. *Id.* While the Fourth Amendment does not apply to private employers, in many respects its application parallels private rights of privacy. *See id.* at 715.

82. Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967)).

83. United States v. Knotts, 460 U.S. 276, 285 (1983).

84. *Id*. at 281. *But see* United States v. Karo, 468 U.S. 705, 714 (1984) (holding a warrant was required under the Fourth Amendment when authorities used an electronic tracking device to track a container after it was located inside a suspect's home). "[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Id.*

85. *Katz*, 389 U.S. at 351 (1967) (citing Lewis v. United States, 385 U.S. 206, 210 (1966);

C. Privacy Equals Secrecy

Privacy protection in America, whether civil or constitutional, focuses on keeping information secret. But keeping information secret is difficult because U.S. law has taken an "opt-out" approach regarding privacy.[86] In other words, failing to take affirmative steps to prevent disclosure of information (i.e., to keep it secret) equates to implied consent for the publication and dissemination of that information.[87] This appears to be the approach taken by courts regarding warrantless searches. For example, in *U.S. v. Barrows*,[88] the Tenth Circuit Court of Appeals concluded that an employee who connected his personal computer (in a public work area) to his employer's computer network which allowed file sharing, left the computer running, and did not password-protect any files, had no expectation of privacy in any files observed by co-workers.[89] The court ruled that while the employee may have had "a subjective expectation of privacy, his failure to take affirmative measures to limit other employees' access makes that expectation unreasonable."[90] Similarly, in *Commonwealth of Pennsylvania v. Sodomsky*,[91] the Superior Court of Pennsylvania found

United States v. Lee, 274 U.S. 559, 563 (1927)).

86. *See, e.g.*, 15 U.S.C. § 6802(b) (2000); *see also* Solove, *supra* note 80, at 1458 (describing how the default rule for an "opt out" system allows "personal data [to] be collected and used unless the individual expressly states a preference not to have information collected or used").

> [F]inancial institution[s] may not disclose nonpublic personal information to a nonaffiliated third party unless— (A) [the] institution[s] clearly and conspicuously disclose[] to the consumer . . . that such information may be disclosed to such third party; (B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party . . .

§ 6802(b)(1). "[N]onpublic personal information" is defined as personally identifiable financial information, however obtained by a financial institution (including both the information a consumer personally provides to a financial institution and the information relating to any transactions with the institution) that is not otherwise publicly available. § 6809(4)(A)-(B). In other words, financial institutions may share nonpublic personally identifiable information with third parties unless consumers take the affirmative step of notifying the institutions to not share the information.

87. *See, e.g.*, Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 133 (2003) (noting the argument that consumers' failure to "opt out" of data collection or sharing may "constitute[] implied consent to the collection and sharing of personal information").

88. 481 F.3d 1246 (10th Cir. 2007).

89. *Id*. at 1247, 1249.

90. *Id*. at 1249 (citing O'Connor v. Ortega, 480 U.S. 709, 718 (1987); United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002)). The *Barrows* court further explained, "[t]hose who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably expect their personal materials to remain private." *Id*.

91. 939 A.2d 363 (Pa. Super. Ct. 2007).

no privacy interest in computer files when employees of Circuit City, while performing routine diagnostic tests to verify whether their installation of a DVD drive on the appellant's computer was successful, discovered what appeared to be child pornography video files on the appellant's computer and notified police.[92] The *Sodomsky* court ruled the appellant did not have a reasonable expectation of privacy in his video computer files since he was informed that Circuit City employees would test the operability of the installed DVD drive and he took no steps to restrict access to any of his computer's files.[93] Again, reflecting the "opt-out" attitude, the court summarized what it considered a basic rule of law regarding privacy: "If a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents."[94] Courts have also extended this attitude to information published on the Internet: "[I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, *without taking any measures to protect the information*."[95]

The same attitude is reflected in civil protections of privacy. "Certainly no one can complain when publicity is given to information about him which he himself leaves open to the public eye . . . ."[96] Current privacy law suggests that a job applicant who posts embarrassing or personal information on a blog or within a social networking site which can be accessed by anyone with an Internet connection should have no expectation of privacy, and therefore, no recourse, when that publicly-available information is viewed, and potentially used, in an employment decision.[97]

---

92. *Id*. at 368.

93. *See id*. (citing United States v. Barth, 26 F. Supp. 2d. 929, 937 (W.D. Tex. 1998)).

94. *Id*. at 369-70 (citations omitted).

95. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) (holding that stop of vehicle was legal where police officer used picture downloaded from the Internet to initially identify and then follow suspect), *vacated*, 90 F. App'x 3, 4 (1st Cir. 2004).

96. Prosser, *supra* note 48, at 394.

97. *See, e.g.*, Dexter v. Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 & n.4 (Ohio Ct. App. May 25, 2007) (upholding custody for father where mother had posted on her MySpace page, among other online statements considered by the court, that "she was on a hiatus from using illicit drugs [during the trial] but that she planned on using drugs in the future . . . . [T]hese writings were open to the public view. Thus, she can hardly claim an expectation of privacy regarding these writings"); Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 78 (2007) ("Categorically, everyone would agree that those who carelessly post shameful pictures of themselves or incriminating information on profiles

Just as extreme circumstances in the early privacy cases may have contributed to the added requirement of offensiveness for the tort of invasion of privacy,[98] extreme facts may have contributed to the binary notion of privacy—that "private" facts must be hidden, kept secret, and once they are publicly accessible are no longer private. Recall that the information discovered in *Sodomsky* was child pornography,[99] as was also the case in *Barrows*.[100] Courts have denied civil claims of invasion of privacy against employers in similar circumstances.[101] It is arguable that when facing evidence of child (or other types of) pornography, courts are reluctant to allow claims of privacy to protect what some in society consider prurient interests. The classic maxim provides that "bad facts make bad law."[102] Rights to privacy protections in these cases stand on their own—they are not conditioned on the content of the information (i.e., child pornography) that is at risk of disclosure.

This all-or-nothing approach to privacy may be outmoded.[103] New forms of communication allow others to view what are intended to be at least somewhat private conversations. Protecting these conversations requires an attitudinal shift towards acceptance of the idea that just because a few people have access to information does not mean it is no longer private.[104] Privacy law will have to adapt to the notion that

that are accessible to everyone on the Internet cannot reasonably claim privacy in their posting."); Krysten Crawford, *Have a Blog, Lose Your Job?*, CNN MONEY.COM, Feb. 15, 2005, http://money.cnn.com/2005/02/14/news/economy/blogging (citing four cases of employees being fired for what they had posted online, observing that most non-contract employees are at-will, meaning they can be fired at any point for any or no reason at all without any recourse, and are therefore extremely vulnerable to such employment actions); Ellen Simonetti, *I Was Fired for Blogging*, CNET NEWS.COM, Dec. 16, 2004, http://www.news.com/2102-1030_3-5490836.html?tag=st.util.print ("[T]he official reason for my suspension [and eventual termination]: 'inappropriate' pictures. The unofficial reason (implied through an intimidating interrogation): blogging.").

98. *See supra* notes 59-67 and accompanying text.

99. *Sodomsky*, 939 A.2d at 365-66.

100. United States v. Barrows, 481 F.3d 1246, 1247 (10th Cir. 2007).

101. *See, e.g.*, TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 163-64 (Cal. Ct. App. 2002) (holding employee had no right to privacy in content stored on employer-provided computer employee was allowed to use at home, including content from sexually-explicit Web-sites, based in large part on fact employee consented in writing to company policy statement that allowed for monitoring of computer use).

102. *See* Haig v. Agee, 453 U.S. 280, 319 (1981) (Brennan, J., dissenting).

103. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 143 (2004).

104. Even though information published on the Internet is potentially accessible by millions of people, from a practical standpoint, only a few people may actually view the information. And that is often the intent of the publisher of the information. *See infra* note 114 and accompanying text.

information can still be private even if it is not concealed.[105] Just because we share confidential information with someone does not mean it is automatically "public" (i.e., no longer private). U.S. privacy law will have to abandon the attitude that "privacy" means "secret."[106]

As noted above, Warren and Brandeis' *The Right to Privacy* moved U.S. privacy law away from the notion of confidentiality.[107] Confidentiality allows limited disclosure, while privacy law demands near-total non-disclosure.[108] Confidentiality is a better fit for modern communications in which, for example, social networks are a primary venue for social interactions among teens.[109] One method of communication is to post a message on a social network friend's page or "wall," (rather than, say, send an e-mail message), the accessibility of which is controlled by the recipient, not the sender.[110] Under current privacy law, exposing information to the recipient means a loss of privacy because the sender passes control of the information to the recipient—the recipient can then expose the information to the world.[111]

The notion of confidentiality at least recognizes some disclosure of information without loss of privacy protection.[112] Strictly speaking,

105. *See, e.g.*, Solove, *supra* note 103, at 143-45.

106. *See* Richards & Solove, *supra* note 48, at 174.

107. *See supra* notes 51-56 and accompanying text.

108. *See* Richards & Solove, *supra* note 48, at 174.

109. *See* AMANDA LENHART ET AL., TEENS AND SOCIAL MEDIA i (2007), http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf ("Some 93% of teens use the internet, and more of them than ever are treating it as a venue for social interaction . . . .").

110. *See, e.g.*, Abril, *supra* note 97, at 74 ("[Online Social Networking (OSN) profiles] are linked together by real-world relationships and OSN ties to form a network of 'friends.' Through these networks of associated profiles, OSN participants can . . . leave notes on their friends' profiles that are visible by anyone with access to the profile."); MySpace.com, MySpace Safety Tips & Settings, http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pagetips&sspage=4 (last visited Feb. 23, 2008) (detailing how to change from the default setting, in which comments posted to a profile do not have to be approved before appearing). While e-mail continues to fall into disfavor among young adults as a mode of communication, with only 14% of all teens sending daily e-mails to friends, among those who use social networking sites, 84% post messages to a friend's page or wall to communicate on these sites. LENHART ET AL., *supra* note 109, at iv, tbl.6.

111. *See, e.g.*, Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1-2 (D. Mass. 2002) (citing Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. 1999)) (holding plaintiffs could not have a reasonable expectation of privacy in messages they sent using the defendant company's e-mail system because the messages could have been forwarded to or accessed by third parties).

112. SOLOVE, *supra* note 11, at 173 ("[C]onfidentiality involves sharing one's secrets . . . . When we tell others intimate information, we expect them to keep it confidential.").

confidentiality does not extend to fully public disclosures.[113] But it leans toward the possibility that a person could publish personal information on their blog or social networking profile, retaining its privacy even though the information may be available to anyone with an Internet connection. The intent in publishing the information is often only to share it with a few friends; the fact that it is widely accessible is an indirect consequence.[114] Anyone else's access of that information (such as a prospective employer) is tantamount to electronic eavesdropping, and therefore an invasion of privacy.[115]

Our society already recognizes selective exposure of personal information.[116] For example, one expects a level of privacy within a gym's locker room, although it is not completely private, at least as to the people simultaneously using the locker room.[117] If someone were to surreptitiously take pictures of others within that locker room, there would be a strong argument for an invasion of privacy.[118] In a society in which substantial numbers of people carry (and use) camera phones and have the means to post photos and videos on the Internet (through a blog or social networking profile)—meaning anyone can be a paparazzo and anyone can be the subject of these citizen paparazzi—notions of what is private will have to evolve, just as in 1890, to accommodate these new technologies.[119]

---

113. *See* Richards & Solove, *supra* note 48, at 181-82.

114. *See, e.g.*, SOLOVE, *supra* note 11, at 50-54 (describing a young woman's blog chronicling her life, including names and detailed descriptions of sexual exploits, "to keep a few of her friends informed about her escapades," but which became widely known and read); *see also* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 968-69, 969 n.197 (2005) (equating the vast amount of information on the Internet with noise, allowing private conversations on the Internet similar to face-to-face conversations remaining private in noisy bars or restaurants).

115. *See* Daniel Benoliel, *Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125, 182 & n.343 (2005) (discussing methods of eavesdropping, most notably interception of electronic communications, including e-mail, as invasions of privacy).

116. *See* SOLOVE, *supra* note 11, at 173-74 (discussing confidentiality and the inconsistent protection it receives in American courts, and giving examples of instances where information is shared but expected to be kept private).

117. *Id*. at 167.

118. There are specific laws prohibiting such types of voyeurism. *See* Marjorie A. Shields, Annotation, *Criminal Prosecution of Video or Photographic Voyeurism*, 120 A.L.R. 5TH 337, 342-49 (2004) (discussing several state statutes criminalizing the use of video cameras or photography as a part of voyeuristic activities that constitute an invasion of privacy and the cases interpreting them).

119. Thomas L. Friedman, Op-Ed., *The Whole World is Watching*, N.Y. TIMES, June 27, 2007, at A23 (discussing the prevalence of blogs, online social networks and camera cell phones and how these conditions make everyone both a paparazzo and a public figure); Andrew Jay McClurg,

IV. PROTECTING LAWFUL CONDUCT FROM EMPLOYMENT DECISIONS

One attitudinal shift, which also specifically applies in an employment context, is reflected in a number of states which restrict employers from considering private aspects of applicants' lives in employment decisions.[120] Most of these statutes prohibit discrimination against employees, as well as applicants, based on tobacco use.[121] A few of the statutes restrict employment decisions based on the more general "use of lawful consumable products."[122] These statutes refer to off-site, off-duty conduct, and are limited to activities which have no employment-related consequences.[123]

These laws could potentially restrict, in certain circumstances, employers' use of Internet searches in making hiring decisions. For example, in 2006, Stacy Snyder, a twenty-five-year-old senior at Millersville University, was denied her teaching credential and dismissed from the student teaching program after staff members of the high school she was working at came across a photograph on her MySpace profile.[124] The photograph in question, captioned "Drunken Pirate," showed Snyder in a pirate costume and drinking an

Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places, 73 N.C. L. REV. 989, 990-92 (1995) (pointing out the "no privacy in public" rule, under which there is little recourse in tort law for intrusions into privacy that occur in public places, and arguing that such a restrictive view is outdated in the face of "a modern technological society").

120. *See* Jason Bosch, *None of Your Business (Interest): The Argument for Protecting All Employee Behavior With No Business Impact*, 76 S. CAL. L. REV. 639, 654 (2003) (explaining how these so-called "lifestyle protection laws" generally protect three types of employees, including employees who use lawful products on their own time as well as employees who engage in lawful behavior unrelated to their jobs).

121. *E.g.*, WYO. STAT. ANN. § 27-9-105(a) (2007) ("It is a discriminatory or unfair employment practice: . . . (iv) For an employer to require as condition of employment that any employee or prospective employee use or refrain from using tobacco products outside the course of his employment . . . ."); *see* Marisa Anne Pagnattaro, *What Do You Do When You are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625, 641 n.86 (2004) (listing tobacco-specific statutes from nineteen different states); *see also* Bosch, *supra* note 120, at 654-58 (describing the nature and benefits of "lifestyle protection laws," including those protecting tobacco users, which are "by far the most widespread of the various lifestyle protection laws").

122. *See, e.g.*, 820 ILL. COMP. STAT. 55/5(a) (2007); MINN. STAT. § 181.938, subdiv. 2 (2006); MONT. CODE ANN. § 39-2-313(2) (2007); NEV. REV. STAT. § 613.333(1) (2005); N.C. GEN. STAT. § 95-28.2(b) (2006); TENN. CODE ANN. § 50-1-304(e) (2005); WIS. STAT. § 111.31(3) (2006).

123. *See, e.g.*, Pagnattaro, *supra* note 121, at 642 (examining the North Carolina statute, which explicitly disqualifies from protection any use of lawful products that interferes with an employee's ability to do their job or adversely affects the safety of co-workers).

124. Stross, *supra* note 20.

unidentifiable beverage from a plastic cup.[125] It is arguable that an employer could not refuse to hire someone such as Snyder based on a similar photo if the employer were located in a state with a statute prohibiting discrimination based on off-duty use of lawful consumable products.[126]

However, if a job applicant in one of these states were to argue that a prospective employer violated the lawful consumable products statute based on what was said on a blog or a social networking profile—under the theory that the applicant's use of the blog or social networking profile (a lawful consumable product) was the basis of the employer's adverse decision—there is a strong likelihood the argument would fail. For example, in *McGillen v. Plum Creek Timber Co.*,[127] the plaintiff, who was employed by the defendant, was fired after he decided to play a practical joke on his supervisor, who had reported the plaintiff for sleeping on the job, by placing a classified ad in a local paper for the sale of a truck, indicating that interested parties should call the supervisor's home number late at night.[128] The plaintiff claimed his firing violated Montana's statute because his taking out the ad was a use of a lawful product off the employer's premises during nonworking hours.[129] The Montana Supreme Court denied the plaintiff's claim, noting that in defining "lawful product," the statute "means a product that is legally consumed, and includes food, beverages, and tobacco."[130] In other words, protection only applies for a product "that can literally be consumed."[131]

A few of these "off-duty" statutes (in California, Colorado, Connecticut, New York, and North Dakota) go beyond just lawful consumable products and protect off-duty conduct in general.[132]

125. *Id.*

126. *See, e.g.*, MINN. STAT. § 181.938, subdiv. 2 (2006) (specifically identifying alcohol as a lawful consumable product).

127. 964 P.2d 18 (Mont. 1998).

128. *Id.* at 20.

129. *Id.* at 23 (quoting MONT. CODE ANN. § 39-2-903(5) (2007) ("The legal use of a lawful product . . . is not a legitimate business reason [that would give an employer an opportunity to dismiss for 'good cause'] . . . ."); *see also* MONT. CODE ANN. § 39-2-313(2) (2007) ("[A]n employer may not refuse to employ . . . an individual . . . because the individual legally uses a lawful product off the employer's premises during nonworking hours.").

130. *McGillen*, 964 P.2d at 23-24 (citing § 39-2-313).

131. Pagnattaro, *supra* note 121, at 645-46 (discussing the *McGillen* court's interpretation of §39-2-313).

132. *E.g.*, N.D. CENT. CODE § 14-02.4-03 (2004) ("It is a discriminatory practice for an employer to fail or refuse to hire a person; to discharge an employee; or to accord adverse or unequal treatment . . . because of . . . participation in lawful activity off the employer's premises

However, these statutes have been interpreted by the courts infrequently and, despite their broad language, their actual applications reveal their limitations.

In California, section 96(k) of the California Labor Code authorizes the Labor Commissioner to take assignments of "[c]laims for loss of wages as the result of demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer's premises."[133] A plain reading of California's "lawful conduct" statute indicates there is no limitation to the type of lawful conduct protected.[134] In *Barbee v. Household Automotive Finance Corp.*,[135] the California Court of Appeal rejected an employee's claim that his employer violated his (state) constitutional right of privacy when the employer discharged him as a result of his intimate relationship with a co-worker.[136] The court concluded that the employee had no reasonable expectation of privacy as to the relationship once the employer became aware of it in large part because he was on notice of the employer's policy discouraging such relationships.[137] The employee in *Barbee* claimed that his employer's conduct violated section 96(k) because the intimate relationship with the co-worker took place during nonworking hours away from the employer's premises.[138] The court rejected this claim, holding that section 96(k) "does not set forth an independent public policy that provides employees with any substantive rights, but rather, merely establishes a procedure by which the Labor Commissioner may assert, on behalf of employees, recognized constitutional rights."[139] With no expectation of privacy, the employee had no invasion of privacy claim—and hence no claim—despite the action involving allegedly lawful conduct occurring during nonworking hours away from the employer's premises.

Colorado has enacted legislation which also prohibits an employer from terminating "the employment of any employee due to that

during nonworking hours which is not in direct conflict with the essential business-related interests of the employer.").

133. CAL. LAB. CODE § 96(k) (West 2003).

134. See *id.*

135. 6 Cal. Rptr. 3d 406 (Cal. Ct. App. 2003).

136. *Id.* at 408 (citing CAL. CONST. art. I, § 1; § 96(k)). *See generally* CAL. CONST. art. I, § 1 (guaranteeing privacy as an inalienable right). California's constitutional privacy provision applies to actions against both private and governmental parties. *Barbee*, 6 Cal. Rptr. 3d at 409-10 (quoting Hill v. NCAA, 865 P.2d 633, 644 (Cal. 1994)).

137. *Barbee*, 6 Cal. Rptr. 3d at 412 (citing Hill, 865 P.2d at 655).

138. *See id.* at 412 (citing § 96(k)).

139. *Id.*

employee's engaging in any lawful activity off the premises of the employer during nonworking hours . . . ."[140] However, Colorado's "lawful activity" restriction does not apply if the activity "[r]elates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee . . . ."[141] Therefore, in *Marsh v. Delta Air Lines, Inc.*,[142] the U.S. District Court ruled that an employer did not violate Colorado's statute when it dismissed an employee who had written a letter critical of management that was published in a newspaper.[143] The court held that the employee owed his employer a duty of loyalty, which the employee breached by trying to settle publicly a private dispute with management.[144]

Connecticut's "off-duty" statute is limited to protecting employees who exercise state or federal first amendment rights.[145] At least as applied to free speech rights, courts have limited application of Connecticut's statute to speech relating to matters of public concern,[146] and "internal employment policies are not a matter of public concern."[147]

The state of New York has adopted legislation that prohibits employers from discriminating against employees on the basis of their legal political activities, legal use of consumable products, and legal recreational activities—all off-site, during non-work hours and without the use of the employer's property.[148] The statute specifically excludes, however, any activity which "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest . . . ."[149] To date, the majority of cases dealing with the "recreational activities" portion of the statute have defined recreational activities as not including romantic relationships or extramarital affairs,[150] although the Supreme Court, Appellate Division

140. COLO. REV. STAT. § 24-34-402.5(1) (2007).

141. *Id.* § 24-34-402.5(1)(a).

142. 952 F. Supp. 1458 (D. Colo. 1997).

143. *Id.* at 1464 (citing § 24-34-402.5(1)(a)).

144. *See id.* at 1463 (citing § 24-34-402.5(1)(a)).

145. CONN. GEN. STAT. § 31-51q (2007); *see also* Pagnattaro, *supra* note 121, at 669 ("Unlike the broader state statutes addressing off-duty conduct . . . [§ 31-51q] simply protects employees who exercise certain federal and state constitutional rights from adverse action by their employers.").

146. *See, e.g.*, Daley v. Aetna Life & Cas. Co., 734 A.2d 112, 122 (Conn. 1999) (citing Connick v. Myers, 461 U.S. 138, 147 (1983); Schnabel v. Tyler, 646 A.2d 152, 162-63 (Conn. 1994)).

147. *Id.* at 123 (citations omitted).

148. N.Y. LAB. LAW § 201-d(2)(a)-(c) (McKinney 2002).

149. *Id.* § 201-d(3)(a).

150. *See, e.g.*, McCavitt v. Swiss Reinsurance Am. Corp., 237 F.3d 166, 168 (2d Cir. 2001)

has ruled that an employee who was "terminated as a result of a discussion during recreational activities [dinner at a restaurant] outside of the workplace in which her political affiliations became an issue, stated a cause of action for a violation of [§ 201-d]."[151]

North Dakota's statute prohibits discrimination by an employer, in part, based on an employee's "participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer."[152] In the only case interpreting this language, the Supreme Court of North Dakota ruled it was a disputed issue of fact whether a chaplain who was discovered engaging in unseemly behavior in a Sears store bathroom was terminated for participating in lawful activity off the employer's premises during nonworking hours.[153]

As can be seen, even the few states that seem to promise protection of lawful, off-duty conduct from employment decisions are severely limited in application. For example, one may have an argument for protection if information associated with matters of public concern or politics were used in a hiring decision, but this only applies in Connecticut or New York.[154] Importantly, all of these statutes also condition the conduct on not having any connection with the employer's business concerns.[155] An employer could argue that information derived about a candidate, from the Internet, had a direct correlation to the employer's business since it was used in the hiring decision. Henry Ford reportedly would send investigators to managers' homes to investigate "the employee's religion, spending and savings patterns, drinking habits

("[N]othing in logic, the language of § 201-d, its legislative history, or New York state case law . . . leads us to conclude that the New York Court of Appeals would hold that romantic dating is a 'recreational activity' under . . . § 201-d(1)(b) . . . ." (citing State v. Wal-Mart Stores, Inc., 621 N.Y.S.2d 158, 159-60 (App. Div. 1995)); *Wal-Mart*, 621 N.Y.S.2d, at 159-60 (citations omitted) (finding that "the voluminous legislative history" of § 201-d excluded dating relationships from the definition of leisure activities).

151. Cavanaugh v. Doherty, 675 N.Y.S.2d 143, 149 (App. Div. 1998) (citations omitted).

152. N.D. CENT. CODE § 14-02.4-03 (2004).

153. Hougum v. Valley Mem'l Homes, 574 N.W.2d 812, 820-21 (N.D. 1998) (citing N.D. CENT. CODE § 12.1-20-12.1 (2004) (prohibiting masturbation in public places); § 14-02.4-03).

154. *See supra* notes 128-47 and accompanying text.

155. *See, e.g.*, COLO. REV. STAT. § 24-34-402.5(1) (2007) ("It shall be a discriminatory or unfair employment practice for an employer to terminate . . . any employee due to . . . lawful activity off the premises of the employer during nonworking hours unless such a restriction: (a) Relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or . . . group of employees . . . or (b) Is necessary to avoid a conflict of interest with any responsibilities to the employer or the appearance of such a conflict of interest.").

and how the worker 'amused himself.'"[156] Today's employer may argue it has a legitimate business interest in whether its employees are publishing pictures on the Internet of themselves drinking excessively.

Since current privacy laws will not protect Internet information, perhaps the "lawful conduct" statutes provide a good start to protect that information. Many of these statutes are incorporated into states' antidiscrimination prohibitions.[157] The Internet provides employers the opportunity to learn a substantial amount of information they would otherwise be prohibited from asking (such as religion, disability, marital status) in a typical employment interview. Even if an employee were to volunteer such information during an interview, the employer is still prohibited from using it in the hiring decision.[158] But there is no way to know if an employer has used the same information gleaned from an Internet search in deciding whether to even interview an applicant.

One way to protect job applicants from the content of their Internet information would be to amend "lawful conduct" statutes to prohibit employers from using publicly-available personal information that could be obtained through an Internet search in their hiring decisions. As an alternative, or in addition, personal information obtained by employers through an Internet search could be treated as credit reports.[159] Under this model, employers could be prohibited from acquiring personal information that could be obtained through an Internet search without first informing the applicant in writing, and would be required to inform the applicant if this information was used as part of an adverse decision, as well as to provide the applicant with a copy of the information found and used. This latter requirement would at least inform the applicant there was possibly damaging information on the Internet so steps could be taken to remove, alter, or correct the information.

CONCLUSION

Millions of people have embraced the Internet as a means of

156. Stross, *supra* note 20.

157. *See, e.g.*, N.D. CENT. CODE § 14-02.4-03 (2004) (codifying North Dakota's "lawful conduct" statute within a section entitled "Employer's discriminatory practices" in Chapter 14-02.4, entitled "Human Rights," which contains policies addressing several other types of discrimination); WYO. STAT. ANN. § 27-9-105(a)(iv) (2007) (codifying Wyoming's statute within a section entitled "Discriminatory and unfair employment practices enumerated; limitations").

158. *See* 42 U.S.C. §§ 2000e-2(a), 12112(a)-(b) (2000).

159. *See supra* notes 41-42 and accompanying text (discussing similar restrictions and procedures for the use of credit reports in employment decisions).

communication and social interaction. Employers have found this information to be very helpful in learning more about job applicants. For the most part, however, people are not publishing information about themselves on the Internet for prospective employers. Although most of this information is accessible by anyone with an Internet connection, the information is usually intended only to be disseminated among a few individuals. Under current U.S. law, even this "limited" dissemination destroys any right to privacy in the information, since it can be accessed by others.[160] In effect, information cannot be kept private unless it is also kept secret. This eliminates any sort of privacy protection for a fast-growing form of social communication.

In the late nineteenth century, technological changes drove a need for updated privacy laws.[161] Early twenty-first century technologies are doing the same. It takes time for new legal theories to evolve and be adopted, so no quick fix is in sight. In the meantime, some protection could be provided by expanding current state statutes which prohibit employers from considering off-site, off-work, lawful conduct in hiring decisions. These statutes could be used (with some amendment, as well as enactment by the states lacking such statutes) to specifically restrict the ability of prospective employers from considering information gleaned from Internet searches. Without such protection, job candidates may never know that they missed an opportunity to interview for their dream job because of some questionable comments they shared with friends through a social networking site.

160. *See supra* notes 83-99 and accompanying text (discussing the "all or nothing" approach U.S. law takes to the right to privacy).

161. *See, e.g.*, *supra* notes 48-56 and accompanying text (discussing the concerns of Warren and Brandeis over expanding technologies of their time–most notably that of the press–and the related developing need for privacy protections against public disclosure).