Denver Law Review Forum

Volume 90 Article 2

2-24-2013

"Sexting" and Surveillance: How Smartphones Change Workplace Harassment

Nantiya Ruan

"Sexting" and Surveillance: How Smartphones Change Workplace Harassment

"SEXTING" AND SURVEILLANCE: HOW SMARTPHONES CHANGE WORKPLACE HARASSMENT

NANTIYA RUAN[1]

As technology evolves, its advancement challenges courts as they attempt to apply long-standing legal doctrines to modern workplace conflicts. Emerging technological advances, such as handheld computers, make the personal/professional divide disappear as smartphones and tablets become inexpensive investments for companies who want their workers available and accessible to their work around the clock.

Our workforce is increasingly mobile, with many workers able to do some or all of their work from virtually anywhere. In 2013, it is expected that 75.5% of the American workforce will be working from somewhere other than a standard office at some point of their workweek,[2] and by 2015, it is expected that 1.2 billion global employees will be considered mobile workers.[3] This "boundaryless workplace"[4] allows for work to be done outside the purview of managers and supervisors at the same time that workers have wide access to instant communications (by way of social network sites, texts, and instant messages). Employers attempt to stem the tide of unauthorized overtime, misuse of company data, and loss of trade secrets by implementing computer monitoring and surveillance.[5] This trend makes workplace relationships ripe for (and companies liable for) sexual harassment (or "textual harassment") and privacy violations claims.

TEXTUAL HARASSMENT

In 2012, when both the Fifth Circuit and a Southern state appellate court reversed trial courts' findings for employers in sexual harassment claims, a trend was in the making. Supervisors sexually harassing their

---

1. J.D., M.S.W., Lawyering Process Professor, Director of Workplace Law Program, University of Denver Sturm College of Law. A heartfelt thank you to Professor Chris Lasch for his helpful suggestions, and to my research assistant, Elizabeth Hutchinson, as well as DU Law Review Editor, Katy Raffensperger.

2. *More Than One Billion Mobile Workers Worldwide by Year's End, According to IDC*, BUS. WIRE (Feb. 19, 2010), http://www.businesswire.com/news/home/20100219005085/en/Billion-Mobile-Workers-Worldwide-Years-IDC.

3. *Id.*

4. Professor Kathy Stone is attributed as coining this phrase to represent the changing workplace norms. *See, e.g.*, KATHERINE V.W. STONE, FROM WIDGETS TO DIGITS: EMPLOYMENT REGULATION FOR THE CHANGING WORKPLACE (Cambridge Univ. Press 2004); Katherine V.W. Stone, *Employee Representation in the Boundaryless Workplace*, 77 CHI.-KENT L. REV. 773 (2002); Katherine V.W. Stone, *The New Psychological Contract: Implications of the Changing Workplace for Labor and Employment Law*, 48 UCLA L. REV. 519, 519 (2001).

5. See Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035, 1042 (2006).

subordinates through inappropriate texts provide a record of behavior that is hard to ignore.

The Fifth Circuit recognized the illegality of supervisors "sexting" subordinates and reversed the district court for failing to recognize that danger. In *Cherry v. Shaw Coastal, Inc*.,[6] the plaintiff was part of a survey crew for an engineering firm when his supervisor subjected him to crude, sexually explicit text messages.[7] After a jury verdict in the plaintiff's favor, the trial court entered judgment as a matter of law in favor of the employer on the Title VII sexual harassment claim.[8] Finding the texts to be explicit sexual propositioning and both severe and pervasive, the Fifth Circuit reversed, remanding the case to the district court to enter the jury verdict.[9]

Similarly, in Missouri, a McDonald's restaurant worker was subject to sexually explicit and threatening text messages from her supervisor.[10] In *Reed v. McDonald's Corp.*, the trial court had granted summary judgment without specifying its reasoning.[11] The Missouri Court of Appeals reversed the judgment in favor of the employer, finding that a reasonable jury could find the conduct "unwelcome."[12]

Both appellate cases showcase the danger instant communications can bring to workplace relationships. From the employees' viewpoint, they are increasingly vulnerable to unwanted sexual predatory advances even when they are away from the workplace, and they feel powerless to stop it without losing their jobs. For employers, harassing supervisors and co-workers are handed this potential avenue for illegal behavior with (often) company-owned equipment, while that same smartphone technology is capturing a record of harassing behavior that previously remained witness-less. Many employers are responding to such potential legal liability with technology monitoring and surveillance of their workers.

PRIVACY EXPECTATIONS IN A PEEPING TOM WORLD

Given the potential liability evidenced on employees' smartphones, an era of unprecedented employer monitoring and surveillance has begun. While employees mistakenly believe they enjoy a privacy right in their smartphone communications, the law is far from clear.

The traditional judicial approach of protecting purely personal matters, while allowing employer scrutiny of work-related activities, is prov-

6. 668 F.3d 182 (5th Cir. 2012).
7. *Id.* at 185–86. The supervisor also subjected the worker to unwelcome touching. *Id.*
8. *Id.* at 186–87 (citing Title VII, 42 U.S.C. § 2000e-2(a)(1)).
9. *Id.* at 188–90.
10. 363 S.W.3d 134, 137 (Mo. Ct. App. 2012).
11. *Id.* at 138.
12. *Id.* at 141.

ing unworkable in the current workplace dynamic. The line distinguishing the personal from the professional is difficult to draw when employees use the same hand-held technology to email work colleagues, text family members, and call doctors. Meanwhile, employers are authorizing IT technicians to install software that capture texts and other data onto the company server.

When it comes to privacy rights, public employees enjoy greater freedom than their private counterparts by enforcing their Fourth Amendment right against unreasonable searches done by their government employer.[13] The Supreme Court's most searching and relevant decision on this issue is *O'Connor v. Ortega*,[14] a twenty-five-year-old opinion without a majority decision, established in a time when hand-held technology was only a promise of things to come. In *Ortega*, the plaintiff was a state hospital physician asserting a privacy right in his desk and file cabinets in his office.[15] The plenary decision established a balancing test, testing the "operational realities of the workplace" against an employee's privacy interests to determine whether an employee has a reasonable expectation of privacy.[16]

In essence, the "operational realities of the workplace" balancing asks courts to evaluate office policies and actual employer practices as *the* measure for evaluating the reasonableness of an employee's privacy expectations.[17] This provides employers with a perverse incentive to adopt a practice of regular electronic surveillance and policy of "no privacy"; accordingly, an employer alone determines the employee's reasonable expectation of privacy.

The Supreme Court had the opportunity to revisit employee privacy in a more modern workplace in *City of Ontario v. Quon* (*Quon III*).[18] In *Quon*, a SWAT team member asserted that he had a reasonable privacy expectation in his text messages sent from his government pager.[19] The police department had a "no privacy" policy, but evidence revealed an unofficial policy of allowing personal use of pagers.[20] Unfortunately, the *Quon* Court left unanswered the central issue of whether public employees have a reasonable expectation of privacy in text messages sent on employer-issued devices (by assuming that the plaintiff did have a priva-

13. U.S. CONST. amend. IV.
14. 480 U.S. 709 (1987).
15. *Id.* at 712, 719.
16. *Id.* at 721.
17. *See id.* at 718–19.
18. 130 S. Ct. 2619 (2010).
19. *Id.* at 2626–27. As Justice Scalia commented during oral argument, these texts were "spicy" and not work related. *See* Transcript of Oral Argument at 49, *Quon III*, 130 S. Ct. 2619 (No. 08-1332).
20. *Quon III*, 130 S. Ct. at 2626-27.

cy expectation), and side-stepped an opportunity to revise *Ortega's* employer-centric focus.[21]

Meanwhile, until recently, employees that work for private employers have been left with only common law tort privacy claims. These causes of action look at whether there was an intentional intrusion "upon the solitude or seclusion of another or private affairs or concerns" that is "highly offensive to the reasonable person."[22] These claims provide very limited relief for private employees, because courts often look to Fourth Amendment case law for guidance on what is objectively reasonable in the workplace, resulting in failed claims. Moreover, this limited relief is all the more unhelpful to at-will employees for risk of termination is not worth pursuing any perceived invasions of privacy claims.

However, recent federal legislation has changed employee privacy law. The Electronic Communications Privacy Act (ECPA) has two major parts relevant to employees.[23] Title I is the Wiretap Act, which prohibits interception of electronic communication, while Title II is the Stored Communication Act (SCA), providing civil liability for intentional access into stored electronic communications without authorization of "a facility through which an electronic communication service is provided" or which "intentionally exceeds an authorization to access that facility."[24] Exceptions to a valid privacy claim include consent to the interception and access by the provider of the communication service.[25]

A few test cases reveal the ECPA's limitations. In *Shefts v. Petrakis*,[26] the president of a telecommunications company filed suit pursuant to the EPCA (and state privacy law) against corporate stakeholders for authorizing installation of "spyware" software on his company computer, laptop, and BlackBerry, which captured all his email and texts on the company server.[27] The spyware was installed after senior management received complaints of the plaintiff's sexual harassment of co-workers.[28] The district court denied summary judgment for the plaintiff, holding he implicitly consented to the interception because: the company's employee handbook made a policy of "no employee privacy," which specifically referenced text messages; his BlackBerry device was a piece of company equipment; and his decision to connect his BlackBerry to the company server, which he should have known could log com-

21. *Id.* at 26, 30–31; *see also* Marissa Lalli, *Spicy Little Conversations: Technology in the Workplace and a Call for a New Cross-Doctrinal Jurisprudence*, 48 AM. CRIM. L. REV. 243, 254 (2011).
22. Restatement (Second) of Torts § 652(B) (1977).
23. 18 U.S.C. §§ 2510–2522, 2701–2711 (2012).
24. 18 U.S.C. § 2701(a) (2012).
25. *Id.*
26. 758 F. Supp. 2d 620 (D. C.D. Ill. 2010).
27. *Id.* at 625–27.
28. *Id.* at 625.

munications sent from his BlackBerry, provided him with notice that all of his messages could be archived.[29]

The SCA has been found equally unavailing for employees looking for privacy in their smartphone use.[30] In *Garcia v. City of Laredo, Texas*,[31] a police dispatcher sued the police department under the SCA for accessing her texts and photos on her smartphone.[32] For employers to be liable under the SCA, they must have gained unauthorized access to a facility through which electronic communication services are provided (or the access must have exceeded the scope of authority given) and thereby must have accessed electronic communications while in storage.[33] The plaintiff argued that her smartphone is a "facility" in which electronic communication is kept in electronic storage in the form of text messages and pictures stored on the cell phone.[34] The Fifth Circuit held that the smartphone does not provide an "electronic communication service" just because the device enables use of electronic communication services, and there was no evidence that the employer ever obtained any information from the cellular company; accordingly, the text messages and photos stored on her phone were not in "electronic storage" as defined by the SCA and therefore outside the scope of the statute.[35]

Together, the most recent cases involving smartphone usage reflect the dissonance between employees' expectations about their "private" communications and what the law protects. While mobile workers are quickly becoming the norm in today's workplace, and the whole notion of what constitutes a "workplace" is being challenged continually in our courts, the law struggles to keep up, especially in the field of workplace sexual harassment.

---

29. *Id.* at 631.
30. *See generally* Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901 (2012).
31. 702 F.3d 788 (5th Cir. 2012).
32. *Id.* at 790.
33. *Id.* at 791.
34. *Id.*
35. *Id.* at 792–93.