UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30 | Issue 3 Article 6

Summer 2014

"Bring Your Own Glass": The Privacy Implications of Google Glass In the Workplace, 30 J. Marshall J. Info. Tech. & Privacy L. 607 (2014)

Anisha Mehta

"BRING YOUR OWN GLASS:" THE PRIVACY IMPLICATIONS OF GOOGLE GLASS IN THE WORKPLACE

ANISHA MEHTA*

I. INTRODUCTION

"Okay, Glass." With these two words, your employee has activated Google Glass in your office, captured crucial business strategies that have been developed exclusively within your company, and distributed the confidential information to your top competitor within seconds. If whispering these two words were not subtle and easy enough for your employee to give away all of your secrets, she can more quickly and discretely activate the device by simply tilting her head up.[1] Even before you have an inkling of her possible misconduct, the damage has already been done. Even worse, you may have absolutely no proof of her misuse because any incriminating evidence is on her personal Google Glass device that is not work-issued. This once futuristic, wearable technology has infiltrated our homes, the public, and our places of work. Its swift and subtle activation makes it ready to record, capture, search, and translate information within the wearer's field of vision,[2] and more hazardously, within a business setting.

The concept of BYOD ("Bring Your Own Device")—the use of employee-owned devices in the workplace—has been growing at a rapid rate.[3] This blends and blurs the business and personal use of

---

* The author earned her B.A. in 2008 from Kent State University. She is expected to earn her J.D. from The John Marshall Law School in 2015.

1. Perkins Coie LLP, *Privacy Risks of Google Glass and Similar Devices*, 19 No. 11 OR. EMP. L. LETTER 7 (2013).

2. Lance Ulanoff, *This Is Why Google Glass is the Future*, MASHABLE (Apr. 30, 2013), http://mashable.com/2013/04/30/google-glass-future/.

3. Garry G. Mathiason, et al., *The "Bring Your Own Device" To Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, THE LITTLER REPORT, 1, 4-5 (2012), http://www.littler.com/files/press/pdf/TheLittlerReport-

technology at an equally rapid rate.[4] Employers implementing BYOD programs reap the benefits of cost reduction, worker satisfaction,[5] and increased productivity and efficiency; however, these benefits are not as prominent[6] as that of the concerns.[7] The introduction of wearable technology like Google Glass (sometimes referred to as "Glass") is among the many reasons[8] that the costs outweigh the benefits for employers in a BYOD environment.[9] An employer is burdened with higher risks of theft, fraud, and misappropriation of his private information.[10] The surreptitious nature of Glass complicates workplace technology by creating a "BYOG" environment.[11]

TheBringYourOwnDeviceToWorkMovement.pdf (citing a study conducted by the Aberdeen group in July 2011 that surveyed 415 companies—seventy-five percent allowed employees to use their personal mobile devices for business-related purposes).

4. Terri Rogers, *The Rise of the Machines: BYOD Realities for the Workplace*, NETSTANDARD (July 19, 2013), http://www.netstandard.com/the-rise-of-the-machines-byod-realities-for-the-workplace/. The rise of IT consumerization has blended together the personal and business uses of electronic devices and applications. Trending technologies in the workplace are orchestrated by the younger generations being a more mobile workforce. *Id.* The article discusses:

> These employees have grown up with the Internet, and they are less inclined to draw the line between corporate and personal technology—especially since so many of them have good technology at home. More than any other, this generation of workers expects to be able to leverage technology at work that is efficient, productive and always accessible. If businesses won't buy devices that meet these needs, then employees will bring them—for business owners, this means that the realities of BYOD are here to stay. *Id.*

5. Tony Bradley, *Pros and Cons of BYOD (Bring Your Own Device),* CIO (Dec. 21, 2011),
http://www.cio.com/article/696971/Pros_and_Cons_of_BYOD_Bring_Your_Own_Device_ (outlining the benefits of BYOD environments as: (1) giving advantages to a company over a competitor; (2) reduction of costs to the company due to the costs of devices shifting to employees; (3) worker satsifaction through the allowable usage of their preferred devices; and (4) employees investing in the latest technology and in turn bringing the latest cutting edge technology into the company).

6. Tom Kaneshige, *12 BYOD Disaster Scenarios*, CIO (Aug. 1, 2013), http://www.cio.com/slideshow/detail/113286#slide4.

7. Caroline Baldwin, *BYOD Increases Productivity, but IT Departments Need to be Prepared*, COMPUTERWEEKLY.COM (Aug. 2, 2012), http://www.computerweekly.com/news/2240160757/BYOD-increases-productivity-but-IT-departments-need-to-be-prepared (explaining that even though productivity in BYOD programs are there, companies must be forewarned about the dangers and obstacles it could cause).

8. *See, e.g.*, Bradley, s*upra* note 5; Kaneshige, *supra* note 6, at slides 2, 5-7, 9-11.

9. Scott Koegler, *The Next BYOD: Glass in the Enterprise*, FORBES (Oct. 22, 2013), http://www.forbes.com/sites/emc/2013/10/22/the-next-byod-glass-in-the-enterprise/.

10. Rogers, *supra* note 4; s*ee also* Bradley, *supra* note 5.

11. Mike Elgan, *BYOG: Why You NEED a Google Glass Policy*, FORBES (Aug. 13, 2013), http://www.forbes.com/sites/netapp/2013/08/13/google-glass-policy/.

Glass is a head-mounted display in the form of eyewear and a Wi-Fi or Bluetooth-enabled module.[12] The module is equipped with a five-megapixel camera that can record HD video, coupled with 12GB of internal storage that can be synced with Google's Cloud Storage.[13] Glass is different than other forms of wearable technology because of its redefined limits, or lack thereof, in capturing one's surroundings.

Wearable technologies that have entered the market, such as the Garmin Forerunner, Fitbit Fitness Tracker, and Samsung Galaxy Gear smart watch,[14] can monitor personal data.[15] Camera-enabled smartphones capture surroundings and actively broadcast users' "most mundane activities every moment of the day"[16] using social media. Dangerously, Glass embodies both a type of wearable technology and a form of capturing surroundings, achieving the ability to continuously record and transmit data within the wearer's surroundings. The discreet nature of wearable technology is combined with the aspect of instantaneous dissemination of information to create this surreptitious and privacy-intrusive device. Ever since cameras have been installed onto mobile phones, users have been increasingly worried about unauthorized surveillance.[17] Google Glass, a low-profile wearable technology, takes the apprehension of video surveillance incorporated within smartphones and movable devices to an entirely different level.

Information collected by the wearer of Google Glass is accessible through a site and application called MyGlass,[18] which is synced with other Google applications including Gmail, Google+, and Google Now.[19]

---

12. Perkins Coie LLP, *supra* note 1.

13. Julian Horsey, *Google Glass Road Show, Visiting US Cities Demonstrating Glass Features*, GEEKY GADGETS (Sept. 27, 2013), http://www.geeky-gadgets.com/google-glass-road-show-visiting-us-cities-demonstrating-glass-features-27-09-2013/.

14. *Samsung Galaxy Gear Review: How Smart Is This Watch?,* HUFFINGTON POST UK (Sept. 27, 2013), http://www.huffingtonpost.co.uk/2013/09/27/galaxy-gear-review_n_4003305.html.

15. Perkins Coie LLP, *supra* note 1.

16. *Id.*

17. *Id.* Smartphones have further escalated the concerns of unauthorized surveillance in cellphones. *Id.*

18. Letter from Susan Molinari, Vice President, Public Policy and Government Relations, Google, to The Honorable Joe Barton, Co-Chairman, Bi-Partisan Privacy Caucus Google (June 7, 2013), *available at* http://marketingland.com/wp-content/ml-loads/2013/07/Google_Glass_Response_2013_Letter.pdf (response to letter sent to Google's VP by Congress); *see generally Navigating the MyGlass Site,* GOOGLE, INC., https://support.google.com/glass/answer/2725957?hl=en (last visited May 6, 2014).

19. Letter from Susan Molinari, *supra* note 18 (suggesting that MyGlass will have access to the mentioned social networking platforms); *see also* Letter from Joe Barton, Co-Chairman, Bi-Partisan Privacy Caucus to Larry Page, Chief Executive Officer, Google (May 16, 2013), *available at* http://joebarton.house.gov/images/GoogleGlassLtr_051613.pdf

This discrete surveillance, coupled with widespread distribution of information across all of Google's platforms within seconds, is what makes Glass different from any wearable technology or recording device that precedes it. "With Glass, others may be unaware of when or whether their conversations are being recorded, giving rise to invasion-of-privacy claims for unauthorized surveillance, wiretapping, and eavesdropping."[20] A major concern for employers is the greater possibility of the dissemination of trade secrets, confidential documents, and other protected workplace correspondence.[21] Furthermore, the technology harbored within Google Glass could critically hinder a job seeker's prospects for employment.[22]

This form of wearable technology "may very well be the next smartphone or Facebook—in other words, the next creation to redefine our concepts of privacy rights, workplace productivity, and communications etiquette."[23] Google Glass will be more than just "shifting [societal] norms,"[24] but utterly manipulating the way business is conducted and the way a workplace operates. While it has the potential to transform business and social interactions in a positive way, the negative

---

(example of Google, Inc.'s response to the letter sent by Congress to Google. Inc.'s Vice President).

20. Freeland, Cooper, Foreman LLP, *Productivity, Privacy Risks of Google Glass and Similar Devices*, 23 No. 5 CAL. EMP. L. LETTER 10 (2013).

21. Perkins Coie LLP, *supra* note 1.

22. Mark Hurst, *The Google Glass Feature No One is Talking About*, CREATIVE GOOD (Feb. 28, 2013), http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/ (painting a picture of a very real dilemma that a prospective employee could have in the future due to the direct impacts of Google Glass). For example, Mark Hurst explains:

> Ten years from now [a company] takes an interest in you, wants to know if you've ever said anything they consider offensive, or threatening, or just includes a mention of a certain word or phrase they find interesting. A single search query within Google's cloud – whether initiated by a publicly available search, or a federal subpoena, or anything in between – will instantly bring up documentation of every word you've ever spoken within earshot of a Google Glass device.

Id.; s*ee also* Lena Sullivan, *Teacher Ashley Payne Fired for Posting Picture of Herself Holding Beer on Facebook*, GA DAILY NEWS (Feb. 7, 2011, 6:41 PM), http://www.gadailynews.com/news/61845-teacher-ashley-payne-fired-for-posting-picture-of-herself-holding-beer-on-facebook.html (describing how a Georgia teacher, Ashley Payne, was fired in 2011 for posting a picture of herself holding beer and wine on Facebook). Ashely Payne's experience is an example of a person in front of the camera posting her own picture, but Google Glass brings the reality of a person in front of a camera having similar photographs posted onto social media without notice of neither the capture nor the post. The wearer would be able to do this instantaneously and with ease, while the onlooker's employment could be quickly and significantly impaired.

23. Perkins Coie LLP, *supra* note 1.

24. Steve Henn, *Google Fights Glass Backlash before It Even Hits the Street*, NPR (May 13, 2013), http://www.npr.org/blogs/alltechconsidered/2013/05/13/183468218/google-fights-glass-backlash-before-it-even-hits-the-street.

implications must be recognized and regulated so they do not outweigh the positive attributes.[25]

The positive characteristics include embracing innovation, technological growth, business developments, and increased productivity in the workplace. For these reasons, an outright ban on the use of wearable technology is undesirable. If devices incorporating cameras or other technological advances were banned in the workplace, this would include smartphones, iPads, and Kindles. While these devices have some risks in the workplace, they have also aided and strengthened workplace productivity from quicker e-mail response times to accessing information on the go.[26] It is apparent that banning devices with cameras is simply not a feasible solution. It is more impractical to simply allow such technologies to be incorporated without any regulation, especially when devices are becoming more intrusive and unpredictable. At this rate, it is not inconceivable to imagine an inconspicuous technology like Google Glass to be produced in an utterly undetectable form: contact lenses.[27] Balancing measures must be implemented to ensure the protection of an employer's business strategies and confidential information as well as an employee's reasonable expectation of privacy when using personal devices, like Google Glass, in the workplace.[28]

Section II of this Comment will provide a history of how an employee's reasonable expectation of privacy has evolved over time, and the scope of protection for both employers and employees under the Electronic Communications Privacy Act ("ECPA") and the Computer Fraud and Abuse Act ("CFAA"). Section III will address how Google Glass and BYOD policies lower an employee's expectation of privacy. Section III will also illustrate, through new trends and case law, how BYODs create an unintended gap in ECPA and CFAA protection laws for employers, and how Google Glass only widens the gap for employers seeking protection of its business information. This Comment encourages the integration of new technology in the workplace while strongly advocating for a narrowly tailored exception to federal regulations of such technology. This solution will assist in protecting employers from employee

---

25. Perkins Coie LLP, *supra* note 1.

26. Steve Lander, *How to Use an iPhone in the Workplace*, AZCENTRAL, http://yourbusiness.azcentral.com/use-iphone-workplace-11185.html (last visited May 6, 2014).

27. Rachel Metz, *Google Glass Today, Smart Contact Lenses Tomorrow?*, MIT TECH. REVIEW (July 25, 2013), http://www.technologyreview.com/view/517476/google-glass-today-smart-contact-lenses-tomorrow/.

28. Sara Angeles, *Wearable Tech at Work Poses Challenges for Businesses*, BUS. NEWS DAILY (June 24, 2013), http://www.businessnewsdaily.com/4677-wearable-tech-at-work.html (explaining the growth of the bring-your-own-device concept and how its combination with wearable technology could greatly impact the way business is conducted).

misconduct, and protect employees' privacy of information in transit or stored on the device when it is unrelated to the workplace. This Comment proposes expansions and limitations for federal surveillance laws to balance the needs of employers and employees in a BYOD workplace.

II. BACKGROUND

A. REASONABLE EXPECTATION OF PRIVACY

1. Fourth Amendment Protection

The Fourth Amendment protects against certain types of government intrusion and unreasonable searches and seizures.[29] In *Katz v. United States*, the Supreme Court held that the Fourth Amendment applies to wiretapping,[30] and established a reasonable expectation of privacy test.[31] A person's reasonable expectation of having a particular right to privacy is determined by a two-prong test as follows: (1) a person must display an actual, subjective expectation of privacy; and (2) the expectation must be one that society recognizes as reasonable.[32] Varying degrees of privacy protection have been ascertained depending upon the environment.

2. Expectation of Workplace Privacy

Workplace privacy has evolved in the past few decades due to the rapid growth of technology. In 1987, the United States Supreme Court held that searches and seizures of an employee's private property are subject to Fourth Amendment restrictions.[33] Because there is no

---

29. U.S. CONST. amend. IV.; s*ee also* Katz v. United States, 389 U.S. 347, 353 (1967).

30. *Katz*, 389 U.S. at 361 (citing Silverman v. United States, 365 U.S. 505 (1961)).

31. *Katz*, 389 U.S. at 361.

32. *Id.* (describing how a person's home would be a place of a significantly reasonable expectation of privacy, but when certain activities or statements are made in public the reasonableness of any expectation of privacy diminishes considerably, making said statements and activities less protected); s*ee also* Oliver v. United States, 466 U.S. 170, 177 (1984).

33. O'Connor v. Ortega, 480 U.S. 709, 715 (1987). The court discusses:

> Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. The workplace includes those areas and items that are related to work and are generally within the employer's control. At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board. *Id.*

talisman to determine exactly which privacy expectations may or may not be "reasonable" to society, the Court has reasoned that factors, such as one's location and the Framers' intent while drafting the Fourth Amendment, should be used to form decisions pertaining to expectations of privacy.[34]

The basic understanding is that certain places and settings deserve a rigorous protection of privacy, while other locations may only deserve a milder protection of privacy.[35] This concept has evolved over time. *O'Connor v. Ortega* involved an employee who had a reasonable expectation of privacy under the Fourth Amendment with respect to his desk and file cabinets located in his office. The employee did not share his desk or file cabinets with any other employees, and the desk and file cabinets contained only personal items.[36] When addressing situations like this one, the Court states that the issue is whether government intrusion "infringes upon personal and societal values protected by the Fourth Amendment."[37] While the expectation of an employee's privacy was quite reasonable within the workplace during that era, our societal norms have changed with the introduction of different technologies.[38]

As these norms evolved, employers began to provide their employees with electronic devices for business purposes. Employers had protection with respect to those devices due to the ratification of the Electronic Communications Privacy Act ("ECPA"), which included a "provider" exception.[39] The ECPA's three employer-oriented exceptions lowered the reasonable expectations of privacy within a workplace to

---

34. *Id.* (citing *Oliver*, 466 U.S. at 178).

35. *Ortega*, 480 U.S. at 715.

36. *Id.* at 718 (discussing that intrusions by employers onto constitutionally protected privacy interest of their employees for "noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances"). This standard requires that both the development and scope of the intrusion be reasonable. *Id.* at 725-26.

37. California v. Ciraolo, 476 U.S. 207, 212 (1986) (citing *Oliver*, 466 U.S. at 181-83).

38. Stephen Wu, *Employee Privacy in the Dawn of the Mobile Revolution; The Prevalence of BYODs in the Workplace Signals a Need for Companies to Revise Their Monitoring Policies*, RECORDER, Feb. 25, 2013 (illustrating how new technologies and monitoring policies can "significantly reduce the expectation of employee privacy").

39. Wiretap Act, 18 U.S.C. § 2511(2)(a)(i) (1986); David Halpern, Patrick Reville, & Donald Grunewald, *Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace*, J. BUS. ETHICS 176 (2008); Jeremy U. Blackowicz, Comment, *E-Mail Disclosure to Third Parties in the Private Sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80, 91 (2001); Larry O. Natt Gantt, II, Comment, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 359 (1995).

some extent.[40] The intersection of the privacy rights in a workplace and electronic surveillance of devices has led the Court to reason that an employee's use of an employer-issued device does not have a very high threshold for any reasonable expectation of privacy.[41]

B. ELECTRONIC COMMUNICATIONS PRIVACY ACT

1. The ECPA's Three Sections

The Electronic Communications Privacy Act of 1986 ("ECPA") provides individuals with protection pertaining to the use of or access to electronic communications.[42] The ECPA encompasses three areas of electronic communication using federal surveillance laws that govern wiretapping and forms of electronic eavesdropping.[43] Title I, the Wiretap Act, [44] prohibits the intentional interception and disclosure of wire, oral, or electronic communications.[45] This Comment will focus primarily on Title I of the ECPA. The other two sections are Title II, the Stored Communications Act ("SCA"),[46] and Title III, the Pen Register Act.[47] Title II will be a secondary focus pertaining to the ECPA analysis within this Comment. However, Title III is outside the scope of this Comment.

Communications such as e-mail and text messages are protected by Title I of the ECPA only when these communications are in transit from one party to another.[48] Once delivered or in electronic storage for back-up, the communications are governed by the SCA.[49] This Comment will focus on the ways in which the electronic communications and electronic storage will be utilized by wearable technology in the workplace, altering the scope of protection for employers and the scope of privacy

---

40. *See infra* Part II.B.1.

41. City of Ontario, Cal. v. Quon, 560 U.S. 746, 747 (2010).

42. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-3127 (1986).

43. *Id.*; *see* CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2012), *available at* http://www.fas.org/sgp/crs/misc/R41733.pdf.

44. 18 U.S.C. §§ 2510-22.

45. *Id.* at § 2511.

46. Stored Communications Act, 18 U.S.C. § 2701-11 (1986).

47. Pen Register Act, 18 U.S.C. § 3121-27 (1986).

48. Susanna Knutson Gibbons, *Recent Court Case Tests Privacy of Employee E-Mails and Text Messages*, POYNER SPRUILL LLP (Aug. 25, 2008), http://www.poynerspruill.com/publications/Pages/RecentCourtCaseTestsPrivacyofEmployeeE-MailsandTextMessages.aspx.

49. *Id.*; s*ee generally* 18 U.S.C. § 2701-11; *see also* Julie J. McMurry, Comment, *Privacy in the Information Age: The Need for Clarity in the ECPA*, 78 WASH. U. L. REV. 597, 598 (2000) (explaining the prohibitions of unauthorized access and disclosure of stored electronic communications).

rights for employees.

2. Exceptions under Title I and Title II of the ECPA: Employer's Permitted Interceptions and Access

The ECPA provides some leeway for employers to access certain information that would normally be impermissible under the Act. These exceptions tend to complicate the employer-employee relationship.[50] Furthermore, employers in the private sector must comply with these federal and state surveillance laws as well.[51] The first exception afforded to the employer is generally known as the "Prior Consent" rule.[52] This rule allows an employer to intercept or access an electronic communication when one party to the communication has given prior consent.[53] However, many states now have statutes requiring the consent of all parties when recording a phone call or conversation.[54] Courts and scholars have reasoned that privacy policies regarding the use of certain electronic devices could satisfy consent.

The second exception allowing an employer to intercept a communication is known as the "Provider" exception.[55] If an employer furnishes

50. *See infra* Part III.B.1 (illustrating case law relating to the Electronic Communications Privacy Act and the employer-employee, ever-evolving relationship).

51. *See* DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/state-law-recording (last updated Mar. 2, 2008). "Many statutes govern the extent to which employers can intrude into an employee's life." Gail E. Mautner, Nancy W. Anderson, & Sarah E. Haushild, *Privacy in the Workplace*, 4 (2001), *available at* http://www.lanepowell.com/wp-content/uploads/2009/04/mautnerg_002.pdf. Federal and state statutory provisions do not expressly protect privacy in general, but do provide for certain privacy interests in particular matters. Many statutory provisions direct employers to comply with certain workplace-specific privacy concerns. Employers must also comply with more general laws protecting individual privacy, such as federal wiretap legislation that limits nonconsensual tape recording of phone calls. *Id.*

52. *See* Wiretap Act, 18 U.S.C. §§ 2511(2)(c)-2511(2)(d); *see e.g.,* Gantt, *supra* note 39, at 356; Blackowicz, *supra* note 39, at 93 (explaining the exception and providing an opposing view on employee privacy); Halpern, Reville, & Grunewald, *supra* note 39 (naming the exception the "One Party Consents" rule, but providing the same background); s*ee* McMurry, *supra* note 49, at 597 (providing a deeper analysis into the exceptions and distinctions between Title I and Title II of the Electronic Communications Privacy Act).

53. *See, e.g.*, 18 U.S.C. § 2511(2)(c)-2511(2)(d) ("It shall not be unlawful . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent. . . ."); Stored Communications Act, 18 U.S.C. § 2702(b)(3) ("A person or entity may divulge the contents of a communication . . . with the lawful consent of the originator or an . . . intended recipient. . . ."); *see, e.g.*, Gantt, *supra* note 39, at 356; Blackowicz, *supra* note 39, at 93; Halpern, Reville, & Grunewald, *supra* note 39; McMurry, *supra* note 49.

54. DIGITAL MEDIA LAW PROJECT, *supra* note 51.

55. *See, e.g.*, Halpern, Reville, & Grunewald, *supra* note 39; Blackowicz, *supra* note 39; Gantt, *supra* note 39.

a device to an employee, then the employer's interception or accession is exempt from the ECPA's restrictions pertaining to electronic communications in transit or stored on that device.[56] The exception under Title II, governing access, is triggered when an employer merely provides the device, whereas Title I, governing interception, requires that the device be employer-owned, that the intercepted messages relate to the business, and that the acts are necessary to protect company property.[57] The likelihood that Google Glass will be provided by employers is slim due to the rising trend in employee-owned devices.[58] However, employees' usage of Google Glass will still relate to business purposes, and the data collected within it will contain a company's intellectual property.[59]

The third exception, governed only by Title I of the ECPA, is called the "Ordinary Course of Business" exception.[60] This exception is afforded to employers in order to protect certain rights or property of the particular business if "telephone equipment or facilities [are] used within the ordinary course of business."[61] Currently, Google Glass works by connecting to smartphones; therefore, it may fall under this section of the Act when used in a BYOD workplace. Consequently, communications that do not fall under the ECPA exceptions are inaccessible to employers and are protected, in favor of employees, under these regulations.

3. Societal Norms Narrows ECPA's Scope of Employer Protection

The exceptions to the ECPA protect employers from employees' wrongdoings. Since 1986, when the ECPA was first enacted, there have been no considerations of how new technologies or simply new concepts and societal norms could impact the scope of the ECPA's protection for employers. By incorporating certain concepts pertaining to technology within the workplace, such as the "Bring Your Own Device" to work trend, an unintended gap has been created for employers and the protection of their businesses. There are currently no bright line rules or regulations to bridge this gap, and Google Glass is only widening it.

---

56. *See* 18 U.S.C. § 2511(2)(a)(i) (affording this protection pertaining to business-related information); *see also* 18 U.S.C § 2701(c)(1) (providing broader accession under Title II than that of Title I).

57. Blackowicz, *supra* note 39, at 90.

58. Mathiason, et al., *supra* note 3.

59. *See* Perkins Coie LLP, *supra* note 1.

60. *See* 18 U.S.C. § 2510(4), 2510(5)(a); *see also* Blackowicz, *supra* note 39, at 90.

61. *See* Blackowicz, *supra* note 39, at 90 (citing Gantt, *supra* note 39, at 364) (explaining that this is because the definition of an intercepting device required under Title I specifically excludes telephone and telegraph devices as well as facilities that are used in the ordinary course of business); *see* Halpern, Reville, & Grunewald, *supra* note 39.

C. COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act[62] is principally a computer trespass statute.[63] 18 U.S.C § 1030(a)(2)(C) poses an issue for the employer, pertaining to employee-owned devices. This provision punishes those who "intentionally [access] a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[64] The elements of this provision can be broken down into the following: (1) intentionally accessing a computer, without authorization or exceeding authorized access; (2) obtaining information; and (3) doing so through the means of a protected computer.[65] Any kind of information, whether it is private or not, is subject to this provision.[66] A "computer" is defined as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.[67]

In interpreting the CFAA, the U.S. Court of Appeals for the Eighth Circuit in *United States v. Kramer*[68] reasoned that even "basic" cellular phones are included within the definition of a computer.[69] The Court stressed that it is bound to the definition given in Section 1030(e)(1).[70]

---

62. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).

63. *Investigating and Prosecuting 21st Century Cyber Threats Before the H. Subcomm. on Crime, Terrorism, Homeland Security and Investigations*, 113th Cong. 1, 1 (2013) (written statement of Orin S. Kerr, Fred C. Stevenson Research Professor, George Washington Univ. Law Sch.), *available at* http://www.loc.gov/law/opportunities/PDFs/KerrCFAATestimony2013.pdf.

64. *Id.* at 3.

65. *Id.*

66. *Id.* (stressing the very scary fact that the statute doesn't require the information to be valuable or private in any way; therefore, "*any* information of *any* kind is enough" to satisfy this requirement, such as even innocent conduct when visiting a website or opening an e-mail).

67. 18 U.S.C. § 1030(e)(1).

68. United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).

69. *Id.* at 902-04 (delineating the arguments for and against the interpretation of a cellular phone being a computer, and recognizing the sheer fact that it cannot be excluded from the definition).

70. The Court explains that new technology is constantly being developed and the definition within this statute could further encompass additional devices that were not foreseen. The definition seems to have the effect of sweeping much more broadly than intended. Moreover, this Court reasons this is a problem for Congress to rectify, not the courts. *Id.* at 903-04 (citing 18 U.S.C. § 1030(e)(1)).

More specifically, the Court held that the defendant's cellular telephone, used only to make "voice calls and send text messages" to the victim, was deemed to be a "computer" within the definition of the CFAA.[71] This poses an intricate issue of employer access to company information on employee-owned devices.

III. ANALYSIS

A. GLASS LOWERS PRIVACY EXPECTATIONS

The privacy protection afforded to people under the Fourth Amendment must be analyzed in the context of a workplace, using the two-prong approach from *Katz*: (1) the employee has a subjective expectation of privacy; and (2) society recognizes workplace privacy as reasonable.[72] While courts have acknowledged an expectation of privacy for employees within the workplace,[73] the level of protection is much lower in comparison to the expectation of privacy and protection afforded to people within their homes or other private settings.[74]

1. How Google Glass will Deteriorate the Expectation of Privacy

Glass is one of the most advanced personal devices that will be available for the public to buy and use in their daily activities. The integration of this new technology into our societal norms raises potential concerns. For example, capturing a picture or video with Google Glass is considerably less noticeable to onlookers rather than taking a photograph with a traditional lens camera. An even more intrusive concern is that the connection from a person's smartphone, via Bluetooth, to his or her personal Glass device allows the possibility of real-time facial recognition[75] to be incorporated within the picture-taking and

---

71. Kramer, 631 F.3d at 901-02; *see also* Cheryl Orr, *Employer's BYOD dilemma: With Employees Using their Personal Electronics for Business, the Contours of Expectation of Privacy are Blurred; Privacy*, RECORDER, July 30, 2012, at 15.

72. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that while the court's majority opinion says "the Fourth Amendment protects people, not places," the two-prong test infers that certain places afford higher expectations of privacy than others).

73. *See id*.

74. *Id.* (stating that one's home is a place where privacy is expected).

75. "Naturally, hackers have thumbed their noses at Google's announcement, reportedly building their own unauthorized software with facial recognition features." Gabriel Meister & Benjamin Han, *Peering Into the Future: Google Glass and the Law,* SOCIALLY AWARE (Sept. 9, 2013), http://www.sociallyawareblog.com/2013/09/09/peering-into-the-future-google-glass-and-the-law/ (citing the letter sent to Google on May 16, 2013 by the bipartisan caucus of congressmen inquiring about a variety of privacy matters, and in response to that inquiry, Google announced on June 3, 2013 that it would not allow ap-

video-recording experiences.[76]

More specifically, in the context of a workplace, Google Glass would be able to capture and record a private conversation of the wearer and an onlooker, relating to the business, or of the private conversations of colleagues that the wearer has no part in. Meetings with clients would be subject to unknown surveillance of privileged speech, confidential data, and even nonverbal conduct. An employee in this type of workplace could be fired for simply saying something that is disliked by his employer and within an earshot of Google Glass.[77] This device has the potential to change the very environment of a workplace into a 24/7 surveillance area, where everyone is always on edge about being recorded and is watching what he or she says. Company policies can prevent these extremities, but the mere entrance of Glass into the workplace will lower the standards of privacy expectations.

Google, Inc. has recently asserted that users of its Gmail service do not have any "legitimate expectation of privacy."[78] Furthermore, Google, Inc. has received increased requests for user information and data from governments and courts around the world.[79] Not only does Google, Inc. have access to its users' information, but it has also complied with these requests.[80] Therefore, the wearer of Google Glass, or the employee in this analysis, will have no reasonable expectation of privacy in using Google Glass itself because of Google, Inc.'s access to it across all of Google, Inc.'s information sharing platforms. A decrease in

---

plications with facial recognition on the Google Glass wearable device); *see also New Facial Recognition Technology*, YOUTUBE (Mar. 25, 2012), http://www.youtube.com/watch?v=EVSkhYHk6TQ.

76. The more society adapted to cameras, the more they have been used in almost every setting in our lives today. Meister & Han, *supra* note 75 (analogizing with Kodak cameras and when they were first a huge uproar to lawmakers and society, banning them from certain settings such as beaches, the Washington Monument, and other locations).

77. Hurst, *supra* note 22.

78. Jamie Court, *Google Glass: "No Legitimate Expectation of Privacy" Either?,* HUFFINGTON POST (Sept. 5, 2013), http://www.huffingtonpost.com/jamie-court/google-glass-no-legitimat_b_3872270.html.

79. *Transparency Report*, GOOGLE, INC., http://www.google.com/transparencyreport/userdatarequests/ (last visited May 6, 2014) (illustrating the drastic increase in percentage of requests for user information since 2009). Seventy-four different countries have demanded user information via social media. Facebook, specifically, received requests concerning 38,000 of its users in only the first half of the year 2013. Furthermore, the author verifies that Microsoft and Google have similarly made these requests for information on its users. Associated Press, *Governments Demanded Data on 38,000 Users, Facebook Reveals*, FOX NEWS (Aug. 27, 2013), http://www.foxnews.com/tech/2013/08/27/facebook-governments-demanded-data-on-38k-users/.

80. *Transparency Report*, *supra* note 79.

privacy within Glass itself coupled with its prospective customary use in the workplace creates a significantly lowered expectation of privacy inside and outside of Glass. This Comment, therefore, seeks to allow employers access to the wearable technology when business-related information is at issue, without infringing on an expectation of privacy of personal data stored on the device.

2. Courts' Acknowledgment of Lowered Privacy Expectations in the Workplace

Operational realities of the workplace must be considered in order to determine whether an employee's Fourth Amendment rights are implicated.[81] Justice Scalia's concurring opinion in *O'Connor v. Ortega*[82] inquires into the operational realities and reasons "that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the Fourth Amendment."[83] "Reasonableness" and "normal" are the operative terms within the standard set out in Scalia's opinion.

As time moves forward, societal norms and public policy concerns are constantly evolving, resulting in newfound perspectives on what constitutes "reasonable" and "normal" behavior in our society as well as within specific circumstances. Legal analyses and processes of reasoning turn on how these terms are interpreted and perceived within the relevant time period. The rise of wearable technologies is no exception. Wearable technologies used in a BYOD environment will significantly alter what is perceived to be "reasonable" privacy constraints and "normal" societal behavior within a workplace.

Courts have looked to company privacy policies when assessing the "reasonableness" of employer and employee conduct in the workplace.[84] Some courts have said that employers are not limited to choosing the "least intrusive method of meeting their legitimate monitoring objectives" when certain privacy policies are put in place.[85] Courts and

---

81. City of Ontario, Cal. v. Quon, 560 U.S. 746, 746 (2010) (citing O'Connor v. Ortega, 480 U.S. 709, 717 (1987)).

82. *O'Connor*, 480 U.S. at 729-32.

83. *Quon*, 560 U.S. at 757 (citing *O'Connor*, 480 U.S. at 732).

84. *See infra* Part III.B.2; "The California Supreme Court recognized that employers have some latitude to impose reasonable computer and Internet use policies and discipline employees for violating them." Wu, *supra* note 38 (citing Hernandez v. Hillsides, 211 P.3d 1063, 1073-74 (Cal. 2009).

85. Wu, *supra* note 38 (citing Hernandez, 211 P.3d at 1073) (explaining further that the courts will not second-guess monitoring policies that have been put into place by employers within their business environments and that the courts will not require employers to limit themselves in choosing the "least intrusive method" of meeting their legitimate

scholars have suggested that whether employee-monitoring policies and programs are put in place determines whether there is a reasonable expectation to be monitored.[86] An employer's lack of these policies would equally impact this designation, causing a reasonable expectation of privacy for the employee.[87] The application of this concept has not been uniformly acknowledged or applied, and the courts have employed these analyses on a case-by-case basis.[88] These incongruous applications give more deference to some company policies over others, blurring the lines of both employee privacy expectations and employer protections.[89]

Courts and scholars have reasoned that many places of employment that implement the use of new technologies, such as smartphones, have diminished expectations of privacy, but that *some* privacy expectations still exist.[90] With Google Glass being the next level of privacy-intrusive technology, that expectation could be decreased even further, or possibly cease to exist.[91] When a reasonable expectation of privacy is found, an employee may have a form of recourse under federal surveillance laws, such as the ECPA, which provides sanctions for violating that privacy.[92] However, it follows that no invasion of privacy can be found if there is no reasonable expectation of privacy established. Glass, a more discreet and surreptitious form of smartphone technology, will be predominantly employee-owned within the workplace, and expectations of privacy will differ from that of smartphones.[93]

Moreover, the "legitimacy of an expectation of privacy depends, in part, on the ability of persons to control their circumstances."[94] The privacy expectations when using Glass may be "nonexistent" due to

---

monitoring objectives).

86. Wu, *supra* note 38.

87. *Id*.

88. *Id*. (explaining that "[a determination of] the expectation of privacy requires an analysis of the facts and circumstances in each case").

89. *Id*.

90. *Id*.

91. *See infra,* Part III.A.1; *see* Court, *supra* note 78.

92. *See infra,* Part II.B.2.

93. *See generally* Orr, *supra* note 71, at 15 (describing the fluctuating dynamics of a BYOD workplace); *see* Michael Bosnar, *Google Glass and the Future of BYOD*, ABC TECHNOLOGY (Apr. 3, 2013), http://www.abc.net.au/technology/articles/2013/04/03/3728650.htm (explaining how Google Glass further complicates an already complex BYOD workplace).

94. Rod Dixon, Comment, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age,* 4 J. TECH. L. & POL'Y 1, 47 (1999). "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Katz v. United States*,* 389 U.S. 347, 351 (1967).

Google's ability to access personal data stored on the device itself.[95] Furthermore, increased usage and integration of Glass in work environments will simultaneously increase the perception of Glass as a normal part of one's everyday routine.[96] Glass will reasonably be seen to lower an employee's subjective expectation of privacy within the business uses of his or her device. Therefore, employers should be allowed to intercept or access information within the confines of an employee's device when an employer has a legitimate business interest in the protection of a company's property or intellectual property.

Currently, employers are unable to protect such property or intellectual property in most BYOD scenarios. Business-related information is unreachable to an employer because employees predominantly own these types of devices. People using personal devices have been deemed to have an expectation of privacy. The rationale is that the devices are bought and owned by an individual rather than by companies, and contain personal data.[97] However, the rising trend in personal devices used for business purposes, and personal data intermingled with business data, gives employees an unjustified protection from employers seeking access to that business data.[98]

B. EMPLOYER'S SCOPE OF PROTECTION UNDER FEDERAL LAWS WITH THE RISING TREND OF BYOD WORKPLACES

Corporations, law firms, small business organizations, hospitals, and other places of employment are starting to see real benefits in employees bringing their own devices.[99] The trend of employee-owned devices in the workplace has nearly replaced employer-issued technologies.[100] A benefit of the BYOD trend is lowered costs for employers

---

95. Court, *supra* note 78 (citing Defendant Google Inc.'s Motion to Dismiss Plaintiff's Consolidated Individual and Class Action Complaint; Memorandum of Points and Authorities in Support Thereof at 19, In Re Google Inc., No. 5:13-md-02430-LHK) (analogizing with Google, Inc. statement in court concerning Gmail users' privacy expectations: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties").

96. Perkins Coie LLP, *supra* note 1; *see also* Angeles, *supra* note 28.

97. Wu, *supra* note 38.

98. Erika Collins & Michelle Gyves, *"BYOD" – Potential Pitfalls for the Global Employer,* N.Y. L.J. (Aug. 8, 2013), http://www.newyorklawjournal.com/id=1202614311187/'BYOD'---Potential-Pitfalls-for-the-Global-Employer?slreturn=20140118213517 (describing the rising trend of BYODs, the ways in which employers are not adequately covered, and the benefits that BYOD policies can provide for both employers and employees).

99. Nancy M. Barnes, *BYOD: Balancing Employee Privacy Concerns against Employer Security Needs,* LEXOLOGY (Sept. 26, 2013), http://www.lexology.com/library/detail.aspx?g=1109490a-6895-40f0-a7a3-afc714316165.

100. *Id.*; *see* Maureen Minehan, *Is Your Workplace Ready for the Bring Your Own*

because they can purchase fewer devices and service plans.[101] For example, employers today do not have to provide BlackBerrys to their employees when they want the employees to have access to e-mail on the go because most employees already have that feature on their personal smartphones.[102]

Employee efficiency and productivity within the workplace are significant additional benefits.[103] For example, hospitals that have incorporated certain devices, such as iPads, have increased the efficiency of doctors and nurses throughout the nation, and provided quicker responses to patients, remarkably altering the healthcare field.[104] A hospital may seem boring and sluggish to a visitor or a patient, but to the physicians and other healthcare employees, it is a fast-paced environment requiring an extremely minimal amount of error, quick decisions, and rapid responses to patients. For these employees, technological advancements, such as Google Glass, that aid in decreased paperwork and increased efficiency could mean life-altering results.[105]

Device (BYOD) Movement?, 30 No. 12 EMP'T ALERT 1 (2013).

101. Minehan, *supra* note 100.

102. Barnes, *supra* note 99.

103. Most businesses recognize that boosts in employee productivity and customer response time are attributable to allowing employee-owned devices into the workplace. According to a study by Dell Software, including about 1,500 IT decision-makers worldwide, sixty-four percent of businesses felt they would be at a disadvantage without BYODs because they believed a BYOD environment would only deliver benefits when correctly implemented. The survey noted that employees would also reap benefits, such as more flexible working hours, ability to foster creativity, innovation, increased morale and collaboration. Scott Campbell, *Study: BYOD Brings Employee Productivity Gains*, CRN (Jan. 22, 2013), http://www.crn.com/news/mobility/240146736/study-byod-brings-employee-productivity-gains.htm.

104. In a research letter in an issue of the Archives of Internal Medicine, it was stated that providing medical residents with personal mobile computers increases their overall efficiency. The research letter stated that it would also reduce delays in the process of their patient care as well as enhance their continuity of care. When they were surveyed, three out of every four of the residents noted that they felt the ability to accomplish certain tasks quicker. This allowed them to allocate more time for educational activities and direct patient care. Press Release, Univ. of Chi. Medicine, Personal Mobile Computing Increases Doctors' Deficiency, (Mar. 12, 2012), *available at* http://www.uchospitals.edu/news/2012/20120312-ipad.html.

105. *See id.* Desktop computers were the first to reduce the exhaustive amount of paperwork and files that healthcare providers would have to sift through. Portable devices, such as pagers, smartphones, and iPads, followed desktop computers. Brandon Glenn, *Five ways Hospitals are Using the iPad,* MEDCITY NEWS (Nov. 7, 2011 1:38 PM), http://medcitynews.com/2011/11/5-ways-hospitals-are-using-the-ipad/. This is a remarkable example of Google Glass's benefits on a global scale. The next big technological advancement for hospitals throughout the world is Google Glass. Physicians can live stream surgeries, employ new levels of sharing medical research and practices, and empower their hospital staff. *Chennai Doc Airs Surgery Live via Google Glass*, DECCAN CHRONICLE

Employee productivity must be balanced against the legitimate concerns for employer security. These concerns are increasing due to BYOD workplaces, diminishing an employer's capability to access and monitor devices.[106] A flat ban on these devices would not be feasible because there are highly desirable qualities of BYOD and wearable devices, such as convenience and efficiency.[107] Additionally, a flat ban would be impractical with the rapid growth of smartphones, iPads, Google Glass, and similar products in today's society and workplaces.[108] While Google Glass should be incorporated into workplaces, it must not go unregulated. Establishing employer protections for legitimate business interests residing in employees' personal devices will aid this workplace problem. This can be incorporated into the exceptions within the ECPA, by way of amendment.

1. The ECPA's Exceptions and the Unintended Gap

The ECPA prohibits the intentional, unauthorized interception of or access to an employee's personal device.[109] Exceptions to the ECPA were codified to protect employers from misappropriation of their trade secrets, intellectual property, confidential documents, and business strategies. However, there are no exceptions permitting employers to intercept or access an employee's personal device even when used for work-related purposes, similar to that of any other device within the workplace.

Today, the permitted use exceptions for employers are inadequate because of the rise of new technologies coupled with new ways of conducting business in the workplace. The regulations must comport with

---

(Sept. 21, 2013), http://www.deccanchronicle.com/130921/lifestyle-offbeat/article/chennai-doc-airs-surgery-live-google-glass (describing how a doctor in Chennai, India was able to live stream a surgery using Google Glass).

106. Barnes, *supra* note 99.

107. *See* Ken Hess, *Five Essential BYOD Accessories*, ZDNET (Oct. 21, 2013), http://www.zdnet.com/five-essential-byod-accessories-7000022161/ (discussing the advantages to portable power sources); *see* Bradley, *supra* note 5.

108. Mathiason, et al., *supra* note 3.

109. In *Lazette v. Kulmatycki*, the Northern District of Ohio denied the defendant's motion to dismiss the plaintiff's complaint. The plaintiff's complaint was for invasion of privacy and violation of several federal laws. The employer had issued a company-owned BlackBerry mobile device to the plaintiff-employee, and the defendant-supervisor used that device to access the employee's personal e-mail. The court held that the Stored Communications Act had applied, and that the supervisor, and possibly the employer, could be liable for accessing the personal information because the defendant-supervisor did not have authority to do so. In analyzing this case, Barnes advocates for clear and specific company policies, outlining an employer's exact authority over employer-issued devices as well BYODs. Barnes, *supra* note 99; *see generally* Lazette v. Kulmatycki, 2013 U.S. Dist. LEXIS 81174 (N.D. Ohio June 5, 2013).

new societal norms in order to revive the initial reasons for allotting such protections. After all, an individual's reasonable expectation of privacy is that which society deems to be reasonable.[110] Google Glass, as a BYOD, creates a lowered expectation of privacy in the workplace, forming a reason to permit employers to access or intercept company-related information on personal devices.

Under the first employer exception to the ECPA, the "Prior Consent" rule, [111] it is not unlawful for a person to intercept a wire, oral, or electronic communication in which one of the parties has consented to the interception of the communication.[112] It follows that a person recording his or her own conversation with someone else, without the other person knowing, is acceptable and does not violate the law under the ECPA.[113] Applying this to the usage of Google Glass at work allows an employee to wear the device and record her own conversations with others throughout the day, not in violation of any laws. Further, the device is her own personal piece of equipment that nobody is entitled to access absent any company policies (which are still not a guarantee of access).[114]

Another application of the use of Google Glass in this context is when a wearer records a private conversation of which the wearer is not a party. Without consent, the wearer is not authorized to record the private conversation. If Google Glass is so frequently used in the workplace, a wearer may not even realize he or she is recording someone else's private conversation while trying to capture an unrelated matter.[115] Moreover, the wearer's intentional, unauthorized, and unnoticed recording is difficult for an employer to prove or gain access to because it will be sitting in the confines of the employee's personal Glass, similar to that of other BYODs. However, Glass is easier and more furtive to use than that of other BYODs. Therefore, an employee can quickly and illicitly capture surveillance of private conversations in an office without being detected or sanctioned.

---

110. *See infra* Part III.A.

111. *See infra* Part II.B.2.

112. 18 U.S.C. §2511(2)(d); *see* Halpern, Reville, & Grunewald, *supra* note 39.

113. Halpern, Reville, & Grunewald, *supra* note 39.

114. *See infra* Part III.C.2.

115. "The human ear has a marvelous ability to pick one voice out of a crowd and focus on it, ignoring all other conversations. Recording devices don't do that. They pick up everything within earshot, even the confidential conversations that someone wearing a recording device may not even realize they're hearing." Brian Wassom, *Does Your Workplace Have a Sousveillance Policy?*, WASSOM.COM (Apr. 12, 2013), http://www.wassom.com/does-your-workplace-have-a-sousveillance-policy.html.

The second permitted interception for employers, the "Provider" exception, allows the interception of communications by an employer when they furnish a piece of electronic equipment.[116] However, the typical way of conducting business is moving away from employer-provided devices and towards employee-owned devices.[117] The rapid advancement of employee-owned devices incorporated into the workplace, coupled with the ever-evolving mobile device landscape, is escalating security risks for businesses.[118] Google Glass, a product that is interconnected with one's smartphone, can and will impact the BYOD phenomenon in ways that can disrupt business practices across the board. Therefore, it must be handled with care. Furthermore, the "Provider" exception should be expanded to encompass all devices used within the normal course of business.

However, this Comment in no way suggests that all devices used within the normal course of business should be examined without any filters. The courts have found ways to sift through the personal data and business data when investigating technologies that have been furnished by both companies and employees,[119] but the courts have not done so consistently. The courts have not laid out any bright line rules for a company's access, interception, or disclosure of information within BYODs even when those companies have privacy policies that address this. Congress should therefore amend the ECPA to allow a business-related extension to BYODs when BYOD policies are put in place, along with limitations on their access, interception, and disclosure. This would ensure that the information retrieved is used in the normal course of business, is of legitimate interest to the employer, and is obtained only after the employee has been given notice through the implementation of BYOD workplace policies.

Sitton v. Print Direction, Inc. is a recent case in which the Court of Appeals of Georgia analyzed an action by an employee against an employer's access and alleged trespass to the employee's personal laptop.[120] This case involves an employer-issued laptop and a personal laptop computer, blurring the lines of the employee's expectation of privacy and of the employer's scope of authority to access and monitor the employee's devices.[121] Here, the plaintiff-employee, Larry Sitton, filed a lawsuit against his employer, Print Direction Inc. ("PDI"), alleging

---

116. Halpern, Reville, & Grunewald, *supra* note 39.

117. Rogers, *supra* note 4.

118. *Id.*

119. *See infra* Part III.B.2 (analyzing Sitton v. Print Direction, Inc., 718 S.E.2d 532, 535 (Ga. Ct. App. 2011).

120. *Sitton*, 718 S.E.2d at 535-36.

121. *Id.* at 534-35.

computer theft, trespass, and invasion of privacy.[122] Sitton was terminated from his employment because he was conducting a competing business while simultaneously working for PDI.[123] PDI provided Sitton with a laptop for work-related tasks, but Sitton chose to use his own computer and connected to PDI's network to conduct his work.[124] The employees of PDI were also provided with an employee manual, prohibiting employees from obtaining outside jobs with competitors of PDI.[125]

While working for PDI, Sitton was able to broker more than $150,000 in print jobs for a competitor print brokerage business that was run by his wife and managed by Sitton himself.[126] After learning about Sitton's competing business, the PDI employer went into Sitton's office where Sitton's personal laptop was located.[127] His employer moved the computer's mouse to find Sitton's e-mails on his laptop's screen, and he printed certain e-mails relating to outside, competing printing companies.[128] The e-mails were located in a separate e-mail account from that of Sitton's employer-issued account, and the content had confirmed Sitton's violations as an employee of PDI.[129]

The Court reasoned that the employer had proper authority to inspect Sitton's personal computer pursuant to the computer usage policy located in PDI's employee manual.[130] "The policy was not limited to PDI-owned equipment."[131] The employer for PDI was allowed to inspect the contents of the electronic device, which was not owned by the employer but rather by the employee, "in the course of an investigation triggered by indications of unacceptable behavior."[132]

---

122. *Id.* at 534.

123. *Id.*

124. *Id.* at 535; *see* Jeffrey S. Klein, Nicholas J. Pappas, & Kendra Okposo, *Privacy Challenges in Drafting "Bring Your Own Device" Policies*, N.Y. L.J. 1, 2 (Dec. 3, 2012).

125. Klein, Pappas, & Okposo, *supra* note 124 (citing Sitton v. Print Direction, Inc., 718 S.E.2d 532, 534 (2011)).

126. *Sitton*, 718 S.E.2d at 535.

127. *Id.*

128. *Id.* at 536.

129. *Id.* at 535.

130. *Id.*

131. Klein, Pappas, & Okposo, *supra* note 124 (explaining that because this Court held that there was protection for the employer's access, this analysis could be applied to smartphone technologies and other employee-owned devices).

132. Sitton v. Print Direction, Inc., 718 S.E.2d 532, 536 (2011) (discussing that Sitton also sued the employer, PDI, for a common law invasion of privacy, alleging intrusion upon his seclusion and solitude into his private affairs). In order to prove that an unreasonable intrusion has occurred, a plaintiff must show an actual physical intrusion. However, Courts have reasoned that this requirement can be met by showing that the defendant monitored Sitton's activities or conducted a type of surveillance of him in some way. *Id.* at 537. Unfortunately for Sitton, the court concluded that no such intrusion took place be-

The Court's leniency towards the investigation of an employee-owned device, where there is no exception permitted by federal laws, illustrates that an expansion of the "Provider" exception is reasonable. Furthermore, it hones in on the original intent that the drafters of the ECPA had when they created these exceptions for workplace environments: to protect the employer. The application of *Sitton* to all employee-owned devices can and should be incorporated into the federal regulations, especially when certain employee-owned devices, such as Google Glass and other forms of wearable technology, are on the brink of becoming mainstream in today's society. Additionally, with the technological advancements that have come forth in just the past few decades, it is not an exaggeration to contemplate the possibilities of even more discrete wearable technology being created, such as smart contact lenses.[133] The workplace realm should be prepared for these possibilities.

The ECPA's third exception, the "Ordinary Course of Business" exception,[134] needs to be addressed. This exception provides a remedy for employers, permitting the interception of electronic surveillance when it is in furtherance of protecting certain confidential business information through telephones or communications within the facilities.[135] The exclusion of employee-owned devices from this exception creates a blind spot for employers due to the fact that BYODs are personal devices that are also used in the ordinary course of business.

The scope of this third exception is unclear to lower courts. At its inception, the third exception was meant to protect employers from employees' mishandling of business information through communication channels during the ordinary course of business. The exception was afforded to employers for this purpose but did not establish any bright line rules as to the scope of its protection, even though it is namely a workplace exception.

Generally, if the issue deals with interception of surveillance, or employers' access to workplace devices, courts apply one of the first two exceptions to the ECPA. The third exception is not normally examined because it is a vague regulation that is inadequate in providing

---

cause, even if the process of reviewing Sitton's e-mails was deemed to be a type of "surveillance," it was reasonable in light of the situation. The president of the company in fact acted specifically in response to an investigation of an improper employee behavior on the part of Sitton. *Id.* at 536-37.

133. Metz, *supra* note 27; s*ee* Katherine Bourzac, *Contact Lens Computer: Like Google Glass, Without the Glasses,* MIT TECH. R. (July 7, 2013), http://www.technologyreview.com/news/515666/contact-lens-computer-like-google-glass-without-the-glasses/.

134. Wiretap Act, 18 U.S.C. § 2510(5)(a) (1988).

135. Halpern, Reville, & Grunewald, *supra* note 39, at 2.

guidelines or clear remedies for such workplace issues.[136]

2. Ambiguities of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") has traditionally been a tool for employers to use when an employee takes part in "knowingly [causing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer," in violation of the CFAA.[137] The CFAA was put in place in favor of employers and for the protection of their corporate information technology ("IT") systems because of employee misconduct and dishonesty.[138] However, the ambiguities within this law have started to "expose the often-secret reality that the statute was not structured for an era when most employees have company-issued computing devices and are permitted remote BYOD access to corporate IT systems."[139]

When the CFAA was created, computers were generally very rare,[140] and now computers are everywhere and in many forms.[141] The CFAA makes it a criminal offense to obtain unauthorized access to a computer, which now includes smartphones.[142] The definition could in fact apply to many different technological devices.[143] The statute further says that the trespass must be on a "protected computer." However, the definition of "protected computer" does not seem to narrow down

---

136. Little guidance or explanation has been provided as to what Congress intended by enacting the business-extension exception. Gantt, *supra* note 39, at 364.

137. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A), 1030(e)(2), 1030(e)(3); *see* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006); There are similar state regulations that have been enacted. *See* Mathiason, et al., *supra* note 3, at 14 ("All fifty states have enacted 'computer trespass' laws, which largely parallel the CFAA."); *see, e.g.,* ARIZ. REV. STAT. § 13-2316(A)(8) (2012); 720 ILL. COMP. STAT. § 5/17-51(a) (2012); NEV. REV. STAT. § 205.4765 (2011).

138. *See* Troutman Sanders LLP, *More CFAA Uncertainty*, INFO. INTERSECTION (Aug. 8, 2012), http://www.informationintersection.com/2012/08/more-cfaa-uncertainty/.

139. *Id.*

140. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010).

141. *Id.*

142. Orr, *supra* note 71, at 15; *see* United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011) (stating that cellular phones are within the definition of a computer).

143. Kramer, 631 F.3d 902-03 (citing Kerr, supra note 140) (explaining that common household items that include microchips and electronic storage devices will satisfy the statutory definition of "computer," such as "coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers").

the scope of the CFAA very much when looking at how it is used today.[144] The shocking truth is that *any* "computer" within the definition of the statute that has access to the Internet is deemed a "protected computer,"[145] subjecting it to the criminal offenses described when violating the CFAA. This is because protected computers are those that are simply used in, or affect interstate commerce.[146] Any device connected to the Internet is used in or affects interstate commerce.[147] Google Glass is a computer, connected to a smartphone, and most of its functions are infused, bounded, and so intricately linked with multiple uses of the Internet that it is undoubtedly a "protected computer" within the meaning of the CFAA.[148]

The problem with Google Glass being deemed a protected computer within the meaning of the CFAA arises when employees own and operate their personal Google Glass devices in a BYOD work environment. In this type of workplace, "[the] challenge arises from the fact that the employer's confidential information and intellectual property moves outside the corporate firewall and is stored on a device the company does not own."[149] In this situation, an employer's access to company's confidential business information would be a criminal violation without the prior permission from its employee,[150] which was not the protection that the CFAA was originally created to provide.[151]

The Seventh Circuit Court of Appeals provides an example of the kind of corporate espionage relating to employee behavior that the CFAA was created to help prevent.[152] The Court held in *International Airport Centers, LLC v. Citrin* that the computer accessed by the

---

144. Computer Fraud and Abuse Act, 18 U.S.C. §1030 (1986); *see generally* Kerr, *supra* note 140.

145. Kerr, *supra* note 140, at 1568.

146. *See* 18 U.S.C.A. §1030(e)(2)(B) ("[T]he term 'protected computer' means a computer . . . which is used in or affecting interstate or foreign commerce or communication. . . .").

147. Kerr, *supra* note 140, at 1568 (explaining the relationship between the Internet and interstate commerce as well as the conclusion that every computer with Internet access is a protected computer under 18 U.S.C. § 1030).

148. *See Setting up Glass*, GOOGLE, INC., https://support.google.com/glass/answer/3064121?hl=en (last visited May 6, 2014).

149. PHILIP GORDON, MANAGING THE EVOLVING CHALLENGES OF WORKPLACE PRIVACY AND INFORMATION SECURITY 4 (2013).

150. *Id.*

151. Michael Z. Green, Comment, *Against Employer Dumpster-Diving for E-mail*, 64 S.C. L. REV. 323, 347 (2012) ("The law was originally designed to respond to juvenile hackers by prohibiting them from attacking the federal government's computers. However, the CFAA has also been used to deter industrial espionage efforts related to the hacking of a business computer to obtain trade secrets.").

152. *See generally* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

employee was deemed protected by the definition within the CFAA.[153] The employee caused the "transmission" of a program that resulted in damage to the protected computer, and the employee "intentionally accessed" the computer "without authorization," or "exceeding authorization," which is a violation of the CFAA.[154]

The employee's authorized access to the computer terminated when he quit his employment in violation of his employment contract and resolved to destroy the files.[155] The employee had installed a program onto the computer that permanently deleted the employer's files.[156] This was a violation of the CFAA because the key elements outlined by the Act were met. The employer's computer was a protected computer, the "command"[157] was the result of the damage, and the employee was the trespasser.

When the CFAA was enacted, employees were not roaming their places of work with their own pieces of technology and recording devices. Arguably, the scope of the CFAA and environment in which it is used has changed tremendously. Therefore, the laws should change in order to support new workplace norms as well. In fact, now the CFAA simply creates a barrier in the context of employee-owned devices (i.e., BYODs).

Upon review of the *Sitton* analysis,[158] it is important to note that the suit that was filed alleged computer trespass and invasion of privacy under state law, and the invasion of privacy was based on an unreasonable intrusion upon seclusion under the common law tort analysis.[159] Sitton brought his cause of action under state law, the Georgia Computer Systems Protection Act (OCGA), which provides civil liability as

---

153. *Id.* at 419.

154. *Id.* at 419-20.

155. *Id.* at 419-20. The program was installed, either by downloading it from the Internet and installing it onto the employer's computer, or by copying the program from a disk and installing it onto the employer's computer. *Id.*

156. *Id.* at 419.

157. *Id.* Citrin's argument was based on the contention that merely erasing a file from a computer cannot constitute a valid "transmission." However, this was not a successful argument because the Court reasoned that pressing a "delete" or "erase" key in fact transmits a "command." *Id.* at 419. This may be a far stretch for the statute, considering the statute provides criminal as well as civil sanctions for its violation, but moreover because under this analysis any typing on a computer keyboard could be deemed to be a form of "transmission" just because it transmits a "command" to the computer. *Id.*

158. *See supra* Part III.B.1.

159. Procedurally, a judgment was entered against Sitton and awarded damages to PDI at the trial court level. Sitton appealed this judgment, and the Court of Appeals of Georgia affirmed the lower court's decision. Klein, Pappas, & Okposo, *supra* note 124, at 2.

well as a civil remedy for criminal offenses.[160] Under the OCGA, computer theft, invasion of privacy, and computer trespass all require that the action at issue be taken "with knowledge," and that the use of the computer or examination of another's data be "without authority."[161] It also requires that the actions be taken with the "requisite intent to take, obtain or convert personal property, delete data, obstruct or interfere with data or examine any personal data."[162] The Court had reasoned that the employer did have the authority to examine his employee's personal laptop because policies were put in place at the company, and the ongoing investigations were due to indications of misbehavior.[163] This case illustrates the support behind privacy policies within companies that allow the use of employee-owned devices. However, the precise scope of the CFAA and similar state regulations in the context of using employee-owned devices in the workplace has recently become the subject of a split among the federal circuit courts of appeal.[164]

C. COMPANY POLICIES ONLY PROVIDE A *MERE POSSIBILITY* OF PROTECTION FOR EMPLOYERS INCORPORATING BYODS

"Employees' right to privacy with respect to mobile devices turns in part on whether they are owned by the company and in part on the agreements reached between the employer and the employee."[165] The entrance of mobile devices followed by smartphones and iPads, and now trumped with wearable technologies, such as Google Glass, is constantly altering the way in which an employee interacts with others in the workplace. These new technologies tend to act as catalysts to the process of employee interference with and distortion of confidential

160. *Id.*

161. *Id.*

162. *Id.*

163. *Id.*

164. "The majority of the circuits have ruled that employers can, by issuing a policy, establish the scope of an employee's permissible authorization to access corporate information." Gordon, *supra* note 149, at 5. Accordingly, if an employee downloads confidential company information to a personal device when his or her employer's policy allows employees to access company information only for authorized purposes and to advance the company's legitimate business interests, the employer can take the position that the employee has violated the CFAA. *Id.* However, in *United States v. Nosal*, the Ninth Circuit rejected the majority view, holding that employers' policies cannot establish the scope of permissible authorization for purposes of the CFAA. United States v. Nosal, 676 F.3d 854, 859-61 (9th Cir. 2012). The court reasoned that allowing employers' policies to make up the boundaries of authorized access with respect to the CFAA would "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved," which could not have been Congress' intent when it enacted the CFAA. Gordon, *supra* note 149, at 5; *see Nosal*, 676 F.3d at 859-61.

165. Wu, *supra* note 38.

business information.

1. How Company Policies have been Incorporated into the Laws of Surveillance

In *United States v. Simons*, the Court held that an employee lacks any reasonable expectation of privacy with regard to his use of the Internet when the employer has official policies regarding such use.[166] In this case, the official policy provided, in part, that "official business use, incidental use, lawful use, and contractor communications" were permitted.[167] The Court relied on *O'Connor v. Ortega* to find that the employee's reasonable expectation of privacy should be analyzed in the context of the employment relationship.[168] This case illustrates the ways in which a company's privacy policy can define the scope of any expectation. In *Simons*, as well as in *Sitton*, an employer can significantly reduce an employee's expectation of privacy by communicating a policy that clearly describes the form and scope of employer monitoring. Employers should inform employees that they simply do not have an expectation that their monitored conduct will be private. "Indeed, a review of the case law suggests that the presence or absence of a clear policy communicated to employees is the key factor in distinguishing between facing or avoiding liability."[169]

Businesses have been increasingly narrowing their policies regarding employees' conduct within the workplace while using certain technology. In *Sitton*, the policies put in place allowed the employer to receive a much higher level of protection, showing a decline in the reasonable expectation of privacy for an employee within his or her personally-owned technologies as long as they are simultaneously used for business purposes.[170] However, not all cases are afforded the same leniency as in *Sitton*, and that is why the scope of authority governing employee-owned devices must be redefined in order to apply federal regulations uniformly.

---

166. The Court held that no reasonable expectation of privacy existed for the employee's Internet use and the Court looked to the language of the company's policy in its analysis. United States v. Simons, 29 F. Supp. 2d 324, 327 (E.D. Va. 1998) *aff'd in part, remanded in part,* 206 F.3d 392 (4th Cir. 2000).

167. Additionally, the policy had a section regarding audits, stating that audits would be implemented to support identification, termination, and prosecution of unauthorized activity, and that audits would be capable of recording web sites that are visited as well. *Id.*

168. *Id.* (citing O'Connor v. Ortega, 480 U.S. 709, 717-18 (1987)).

169. Wu, *supra* note 38.

170. Sitton v. Print Direction, Inc., 718 S.E.2d 532, 537 (2011).

2. Existing Policies are Often Inadequate[171]

Policies for electronic communications within places of work, such as corporations, government agencies, hospitals, law firms, and many more, have generally been crafted and based on the fact that companies own the computer, equipment, or other electronic device.[172] Furthermore, the employer pays for the technology, the access, the security, and other services, giving it broad control over its ownership rights to the property and only requiring the need to give employees appropriate notice of monitoring and access along with the device.[173]

The problem today lies in the fact that business is conducted not only with workplace computers, but also with portable devices.[174] Portable devices are more likely to be incorporated into the workplace than previously used non-portable devices, and the devices are increasingly employee-owned. Additionally, problems have emerged when employees regularly access their personal web-based e-mail and social media networks, such as Facebook, Twitter, and Google+, at work. Many electronic communication policies fail to address these issues, and now the concerns of intermingled business and personal uses of devices in the workplace will only complicate the matters more, and provide less recourse for employers.

"For example, many policies don't address whether and how employee-owned devices may access the corporate network."[175] Mobile devices, and smartphones in particular, give a company far less control than that of employer-owned equipment, making it significantly more important for any employer to have authority to access devices, monitor employee activity, and take appropriate action to prevent the misuse of confidential information. While the U. S. Supreme Court recognized the validity of computer usage policies, it failed to set parameters on an employee's expectation of privacy or limitations on a company's right to access an employee's device when such policies are implemented.[176] Giving recourse to only businesses that are able to come up with the most comprehensive policies against the misuse of devices disrupts the purpose of why the ECPA's employer-related exceptions were drafted in the first place.

---

171. Kathleen M. Porter, *Going Mobile: Are Your Company's Electronic Communications Policies Ready to Travel?*, BUS. L. TODAY 1 (2011).

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.*

176. *Id.* (citing City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010)) (explaining how the U.S. Supreme Court determined an employee's scope of rights within the specific situation laid out in City of Ontario, Cal. v. Quon, but did not go further to set adequate parameters for future examination).

D. PROPOSAL

1. Changes to the ECPA under the Provider Exception

A plausible form of refined protection for employers would be to narrowly tailor the "Provider" exception under Title I and Title II of the ECPA to apply to employee-owned devices that are used for business purposes, just as employer-owned devices are addressed within Title I.[177] Title II does not have a "type of use" requirement to trigger the exception, making it over-inclusive.[178] However, the lack of protection for employers in BYOD workplaces creates an under-inclusive feature to Title II as well.

An expansion that allows employers to access and intercept new technology along with a narrowly tailored purpose for that access or interception can protect employers from employee misconduct under all workplace devices, and simultaneously protect employees from unjustified invasions of their personal use of devices. First, the inclusion of employee-owned devices would allow employers to be protected from employee misconduct under all workplace devices. Second, the narrowly tailored regulation would ensure safeguards for employees' remaining privacy. This would be through the use of restrictions on employers' access or interception. In order to create this narrowly tailored regulation, the amended exception should be triggered only when: (a) a legitimate business purpose is present; and (b) BYOD privacy policies are established.

Requiring an employer to have a legitimate business purpose maintains employees' privacy within their personal use of the dual-use devices. Requiring the implementation of a BYOD policy eliminates any expectation of privacy within the business use of the dual-use device. These prerequisites trigger the exception, and allow for an appropriate and fitting analysis to apply to such problems in the workplace. This proposed amendment to the ECPA promotes adequate and reasonable means of access and interception to achieve the balanced ends of employer and employee protections. Therefore, this is the best way to amend the ECPA.

---

177. *See* Wiretap Act, 18 U.S.C. § 2511(2)(a)(i) (1986).

178. *See* Stored Communications Act, 18 U.S.C. § 2701(c)(1) (1986); *see* McMurry, *supra* note 49, at 621 (describing the over breadth of the liability exception for service providers and advocating for legitimate business purposes to be considered in the exception).

2. Tightening the Exceptions even Further

Furthermore, pertaining to the "Prior Consent" rule, if the requirement for a BYOD policy is implemented, it will give notice of the monitoring program to the employee and ensure that the employer has the employee's prior consent. This takes care of the problem of "two-party consent" that twelve states have thus far enacted.[179]

Another reasonable way to broaden employer protection in order to accommodate these new forms of technology would be under the third exception, known as the "Ordinary Course of Business" exception. Congress can use the same narrowly tailored test set out in section one of this proposal in order to ensure protection under this particular exception.[180] However, the "Ordinary Course of Business" exception is currently exclusive to Title I of the ECPA, and would therefore not be as effective as that of an amendment to the "Provider" exception, which is set forth under Title I and Title II of the ECPA.

3. Refining Workplace Policies

Until federal laws are amended and molded to shape our societal norms and current technological advancements, every business entity should have a thoroughly structured and detailed privacy policy regarding employee-owned devices. Furthermore, if changes are made to the ECPA to allow employers to access employee-owned devices, policies that at least give notice to the employee of monitoring will have to be put in place in order to satisfy a reasonable expectation to be monitored. Employers will need to show that the employee has no reasonable expectation of privacy within the business use of the dual-use device. Therefore, change or no change, the best practice to avoid liability is to implement strong BYOD policies into one's workplace as soon as possible.

Many companies have enacted strong mobile device management adoptions that a workplace should put in place.[181] These mobile device management tools can be used to create similar Google Glass management tools. Some of these tools are: identifying business goals and costs, investing in BYOD training programs, defining the segregation between personal and business data, and defining device requirements.[182] These should be integrated into company handbooks or into employee contracts, possibly along with a choice to opt in or opt out of

179. DIGITAL MEDIA LAW PROJECT, *supra* note 51.

180. *See* Wiretap Act, 18 U.S.C. §§ 2510, 2511 (1986) (using the same language of within the "ordinary course of business" as in the statute).

181. Rogers, *supra* note 4.

182. *Id.*

the BYOD program.[183]

IV. CONCLUSION

An employee's expectation of privacy has been refined and narrowed through court interpretation, and the implementation of Google Glass and similar wearable technologies will continue to shape the expectation of privacy within a workplace. Employees, instead of employers, predominantly own Glass and the smartphones with which it syncs to. Users of Glass do not have a very high expectation of privacy when their personal use of the device is intermingled with their employer's business purposes. A decrease in employees' expectation of privacy justifies an employer's reach into the device pertaining to their legitimate business interest.

Employee misconduct can occur through the uses of various technologies. One example includes the employee who used his personal laptop to access and misappropriate a company's private information from the confines of his home.[184] This misappropriation will only worsen with the use of more discreet devices, enabling misconduct to occur in the presence of colleagues during regular work hours. Google Glass embodies this very real possibility.

Wearable technologies are currently the biggest threat to a BYOD workplace due to the devices being "employee-owned." Google Glass is already utilized by many individuals and is hitting the public consumer market in the next few months. Therefore, it would be wise for private companies as well as governmental organizations to have policies addressing these wearable technologies, defining what they are, what they encompass, how they are to be used, and the scope of their use within the workplace before employees start to bring their own Glass, bringing disruptions or misconduct into the workplace as well.

The CFAA is overly broad and encompasses even rudimentary devices. Its application to the employer-employee context makes an employer's interest in obtaining business-related information impossible without the authorization of an employee. This reinforces the reasons for a change in the law in favor of employers. However, when analyzing the two federal regulations, the ECPA is a better fit for an exception to employers' access and interceptions of employee-owned devices.

---

183. *Id.*; *see* Taylor Chapman, *BYOD? Avoiding the Pitfalls of Employee Use of Personal Devices*, 24 No. 2 VA. EMP. L. LETTER 1 (2012) (explaining the U.S. Supreme Court's holding of an employer's right to access all communications on corporate-issued devices, and its failure to address that of employee-owned devices); *see* Koegler, *supra* note 9.

184. *See supra* Part III.B.2 (analogizing with the issues within Sitton v. v. Print Direction, Inc., 718 S.E.2d 532 (2011)).

Court interpretation of the ECPA coupled with analysis of company privacy policies has been successful in some cases. If Congress creates a clear federal regulation addressing this, then employers will not have to rely on the mere possibility of recourse due to incongruous court interpretations.

The best solution is to amend the ECPA's exceptions of an employer's permitted access and interception to include investigation of business uses of an employee's dual-use device. The exceptions should expand to protect business information in the hands of employees, as well as limit its application strictly when there is a legitimate business purpose behind the investigation. This will narrowly tailor the law in protecting the ends that it was created to secure without using means that are over-inclusive or under-inclusive. Therefore, the proposed amendments to the ECPA should be codified to reinstate protection for employers in a world where business is now being run by employees' BYODs, and soon enough, Google Glass.