COMMENTS

"The Entire History of You": Privacy and Security in the Face of Smart Contact Lens Technology

Jessica Dennis*

I. INTRODUCTION

Imagine an alternate reality, where each individual has what is known as a "grain" implanted behind his or her ear. This grain records everything that the individual does, sees, or hears.[1] It also allows memories to be played back either in front of the individual's eyes or on a screen, a "re-do."[2] This technology could be a wonderful solution to the problem of the imperfect human memory.

For example, imagine a young attorney who attends a work evaluation.[3] She feels that the interaction did not go well.[4] With her grain, she performs a re-do and plays back the interaction to see where she went wrong.[5] She analyzes her behavior and responses as well as

* © 2017 Jessica Dennis. J.D. candidate 2018, Tulane University Law School; B.A. 2015, Psychology and Sociology, University of Louisville. Senior Managing Editor, Volume 20, *Tulane Journal of Technology and Intellectual Property*. The author would like to thank her friends and family for their support and suggestions in writing this Comment, as well as the members of the *Journal* for their hard work and dedication.

1. *Black Mirror: The Entire History of You* (Channel 4 television broadcast Dec. 18, 2011).
2. *Id.*
3. *See id.*
4. *See id.*
5. *See id.*

those of the people with whom she interacted.[6] Later that evening, she projects this re-do of the performance evaluation on a screen for her friends to see, getting their feedback on the interaction.[7]

The previously mentioned grain technology is a creation of the cult television show *Black Mirror*, which addresses many of the problems and concerns that arise out of the advancement of technology in the world today. While the fictional *Black Mirror* technology is far more advanced than that which currently exists, these advancements may be nearer than one would think. Recently, innovators have filed patents for contact lenses with a built-in camera (smart lenses).[8] These smart lenses would be capable of taking pictures and even videos with just the blink of an eye.[9] While there are many different kinds of smart lens technology out there—with functions such as monitoring health (specifically blood sugar),[10] amplifying games via augmented reality,[11] and enhancing and even providing zoom to one's current vision[12]—recent patents have pushed the technology closer to the futuristic grain technology of *Black Mirror*.[13]

Wearable technology that is small and easily accessible will likely lead to wider usage. This increase in usage also brings the enticement to use these technologies to gather a massive amount of data about a person's life. By snapping a picture or recording a video discreetly with the blink of an eye and then storing this information for future use, the individual has opened herself up to the potential for this data to be observed, analyzed, and/or shared (potentially without their knowledge).[14]

---

6. *See id.*

7. *See id.*

8. There are many competitors and different goals and patents for Smart Lenses, but for the purpose of this Comment, Sony's version is the closest to what will be discussed. U.S. Patent Application No. 14/785249 (filed Feb. 12, 2014) [hereinafter Sony Patent].

9. *Id.*

10. Luke Edwards, *Google Is Developing Smart Contact Lenses that Detect Health and Autofocus Eyes,* POCKET-LINT (July 16, 2014), http://www.pocket-lint.com/news/129912-google-is-developing-smart-contact-lenses-that-detect-health-and-autofocus-eyes.

11. Luke Edwards, *Samsung Contact Lens Displays Will Put AR Video and Cameras in Your Eyes,* POCKET-LINT (Apr. 7, 2016), http://www.pocket-lint.com/news/137239-samsung-contact-lens-displays-will-put-ar-video-and-cameras-in-your-eyes.

12. Luke Edwards, *This Bionic Lens Could Give You 3 Times Better Vision than 20/20*, POCKET-LINT (May 19, 2015), http://www.pocket-lint.com/news/133945-this-bionic-lens-could-give-you-3-times-better-vision-than-20-20.

13. *See* Luke Edwards, *Sony Smart Contact Lens Will Record Everything You See, with the Blink of an Eye*, POCKET-LINT (May 5, 2016), http://www.pocket-lint.com/news/137527-sony-smart-contact-lens-will-record-everything-you-see-with-the-blink-of-an-eye.

14. *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH, no.. 2, 2015, at 1, 54, http://jolt.richmond.edu/v2li2/article6.pdf.

Moreover, this data can be very sensitive in nature, divulging information about an individual's daily life, including what stores she frequents, the route she normally takes, and even what she does in the privacy of her own home.

Those who do not use smart lenses may also have cause for concern. These individuals may find themselves in a situation or environment where they are surrounded by people who are using these technologies. These nonusers are neither able to control how others use smart lenses, nor what actions or data the users capture about the individual.[15] Further, providing consent to collect this type of data from an individual who does not use these technologies could prove to be impossible.[16]

While they were once only the ideas of science fiction writers, smart lenses now introduce the real world to the potential for an individual to not only gather data about their daily lives but also the lives of every person with whom they come into contact. Any sense of privacy that an individual has will be tossed out in the cold, ushering in this new big brother-esque reality. Further, any sense of confidence that an individual has about the security of his or her information when using smart lenses will go by the wayside. Smart lenses will open up a whole new world to cybercriminals, allowing vulnerable information about users and nonusers alike.

Thus, technological advancement of this kind does not come without a cost. This Comment will focus on the legal implications of this type of technology in two major realms: the workplace and criminal investigations. First, this Comment will discuss the rise of wearable technologies and how smart lenses came to be in existence. Next, it will look at security concerns implicated by this technology in the workplace. This type of discreet technology causes concern for both employers and employees in the workplace. While an employee's privacy rights are very important, there is also a growing concern for employers who wish to keep their data safe from competitors. Finally, this Comment will examine the use of this technology in the criminal realm. The use of smart lenses in the criminal justice system will create many concerns.

---

15. *See id.* at 55.

16. *See* Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, at 4, 14/EN WP 223 (Sept. 16, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("[C]lassical mechanisms used to obtain individuals' consent may be difficult to apply in [this case], resulting in a 'low quality' consent based in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals.").

This Comment will look at the concerns raised both when law enforcement seeks to access information during an investigation, as well as when law enforcement uses smart lenses.

II. THE RISE OF WEARABLE TECHNOLOGY AND SMART LENSES

Wearable technology, or "networked devices that can collect data, track activities, and customize experiences to users' needs and desires,"[17] have been used in our society for years. These technologies have largely been composed of health and fitness trackers and other smart devices.[18] However, it is now cheaper than ever to incorporate technology, such as microchips, sensors, and cameras, into devices.[19] Advances in both circuits and software have made it possible to make a web server that fits on the tip of a finger at an extremely cheap price.[20]

As a result, once mundane objects such as refrigerators, vehicles, and watches have now become "smart" and use these advanced technologies.[21] CEO and founder of SmartThings, Alex Hawkinson, refers to this as a shift to a "programmable world," where "things will become intuitive [and] connectivity will extend even further, to the items we hold most dear, to those things that service the everyday needs of the members of the household, and beyond."[22] Old iterations of wearable technologies that are comparable to smart lenses are clunky and unattractive, which likely has limited their otherwise broad adoption.[23] Now it appears that this "programmable world" will extend to contact lenses, allowing instant (and arguably constant) data collection.

Smart lenses are the epitome of discreet smart technology. Smart lenses ultimately will make the clunky, unattractive wearable technologies obsolete and irrelevant. They provide the same technology and capabilities of a camera or camcorder in the size of an ordinary

---

17. Thierer, *supra* note 14, at 1.

18. For example, many of the wearable technologies include the smart watches (e.g., the Apple watch), fitness trackers (e.g., Fitbit), and Google Glass.

19. Thierer, *supra* note 14, at 5.

20. *Id.* at 6.

21. *See id.*

22. Alex Hawkinson, *What Happens When the World Wakes Up*, MEDIUM (Sept. 23, 2014), http://medium.com/@ahawkinson/what-happens-when-the-world-wakes-up-c73a5c931c17#.94ngx03ct

23. *See* Connie Guglielmo & Parmy Olson, *The Case Against Wearables, or Why We Won't All Look Like the Borg This Year*, FORBES (Mar. 3, 2014), http://www.forbes.com/sites/connieguglielmo/2014/02/12/the-case-against-wearables; *see also* Nick Warnock, *Wearable Tech: Fashion Will Rule*, INFORMATIONWEEK (June 18, 2014, 9:06 AM), http://www.informationweek.com/strategic-cio/digital-business/wearable-tech-fashion-will-rule/a/d-id/1278629?piddl_msgorder=thrd.

contact lens. This type of discreet technology will likely result in the increased usage of smart lenses, allowing for the "programmable world" to be as prevalent as ordinary contact lenses.

Wearable technologies gather a massive amount of information, raising a number of unique privacy concerns.[24] Whether these concerns arise depends on the access to the device, the information that the device shares with other devices, or the information transmitted to any remote storage system.[25] Smart lenses would go beyond this to allow a user to not only take pictures and record videos with the blink of an eye, but store those videos and images for future playback and use.[26] These pictures and videos stored for future playback give cybercriminals, such as hackers, the opportunity to gain access to valuable information. Not only would the hackers be able to find pictures and videos that a person has stored, but it would essentially allow the hackers to piece together things about a person's life, such as his or her daily schedule or favorite places to shop.

Researchers have proven that with enough determination and the right codes, it is possible to hack the devices that we wear on our bodies every day.[27] Current wearable technologies have proven to be more work than they are worth.[28] The information gained from hacking current devices is not worth the amount of time and effort that it would take an individual to perform such a feat.[29] However, with the advancement of these technologies, like smart lenses, cybercriminals are more likely to target them.[30] It is likely that smart lenses will have a cloud-based storage system, providing a prime target for cybercriminals who wish to hack the lenses for valuable information about an individual.[31] It is equally likely that smart lenses will also have capabilities to link to third-party applications or devices, thus creating another likely target for cybercriminals.[32] Therefore, the present circumstances, where new

---

24. *See* Patrick Thibodeau, *The Internet of Things Could Encroach on Personal Privacy*, COMPUTERWORLD (May 3, 2014, 7:45 AM), http://www.computerworld.com/s/article/9248086/The_Internet_of_Things_could_encroach_on_personal_privacy.html.

25. *See* Al Sacco, *Fitness Trackers Are Changing Online Privacy—And It's Time To Pay Attention*, CIO (Aug. 14, 2014, 8:31 AM), http://www.cio.com/article/2465142/wearable-technology/fitness-trackers-are-changing-online-privacy-and-its-time-to-payattention.html.

26. Casey Williams, *Sony Filed a Patent for Video-Recording Contact Lens*, HUFFINGTON POST (Apr. 28, 2016), http://www.huffingtonpost.com/news/digital-contact-lens/.

27. David Nield, *Wearables Are Only Secure Until They Become Worthwhile Hacking*, WAREABLE (July 21, 2016), http://www.wareable.com/wearable-tech/wearable-security-8865.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

technology has become prolifically ingrained in the collection and storage of information, have reached a point where a light must be shone on the legal abyss protecting smart lens privacy—a light this Comment seeks to shine.

III. PRIVACY AND SECURITY IN THE WORKPLACE

The Supreme Court has interpreted the Fourth Amendment to establish individual privacy with the reasonable expectation of privacy (REOP) test.[33] The Court laid out the test in two prongs: (1) an individual must display an actual, subjective expectation of privacy and (2) that expectation must be recognized as reasonable by society.[34] This is a flexible test that yields different privacy expectations in different underlying circumstances. Thus, varying degrees of protection for one's privacy have been determined depending upon the situation.[35]

An individual's REOP is dependent upon the situation.[36] In 1987, the Supreme Court held that Fourth Amendment protections applied to searches and seizures of an employee's private property.[37] The Supreme Court determined that individuals in the workplace are granted a lesser expectation of privacy within the boundaries of the workplace than they would be in other situations.[38] Due to this determination that an individual's REOP is lower in the workplace, the Court found it essential to delineate the boundaries of the workplace.[39] The Court determined the workplace to include "those areas and items that are related to work and are generally within the employer's control."[40] This lower REOP does not apply to an individual's closed private property, such as a purse or luggage, which happens to be on the premises of the workplace.[41]

When presented with a REOP issue in the workplace, courts must first determine whether the governmental intrusion "infringes upon

33. Katz v. United States, 389 U.S. 347, 361 (1967).

34. *Id.* (describing how a person's home would be a place that held a 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).

35. Anisha Mehta, Comment, *"Bring Your Own Glass:" The Privacy Implications of Google Glass in the Workplace*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 607, 612 (2014).

36. *Id.*

37. O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

personal and societal values protected by the Fourth Amendment."[42] New technology, specifically wearable technology like smart lenses, creates a new societal norm regarding one's expectation of privacy in the workplace. Therefore, as societal values and norms change, so too would the protections that the Fourth Amendment provides to an employee in the workplace.

A. An Employee's Rights to Privacy

One key component of the workplace operations is the privacy aspect. While the expectation that an employee had of her privacy within the workplace used to be quite reasonable, emerging societal norms have changed that expectation with the introduction of different technologies (e.g., smart lenses).[43] As a result of this shift and evolution in societal norms, Congress passed the Electronic Communications Privacy Act (ECPA) to protect workplace privacy rights for employers that provide their employees with electronic devices and different technologies for business purposes.[44] Thus, there is a low threshold in regards to an individual's expectation of privacy within the workplace.[45] This low threshold will likely continue to exist with the emergence of smart lenses.

The ECPA provides individuals with protection concerning the use of or access to electronic communications. Title I of the ECPA protects the transmission of communications, such as e-mail or text messages, between two parties.[46] Title I only protects these communications from anyone who intercepts or attempts to intercept them.[47] Thus, Title I of the

---

42. California v. Ciraolo, 476 U.S. 207, 212 (1986) (quoting Oliver v. United States, 466 U.S. 170, 181-83 (1984)).

43. *See* Stephen Wu, *Employee Privacy in the Dawn of the Mobile Revolution*, RECORDER (Feb. 22, 2013), http://www.law.com/therecorder/almID/1202588380082/?slreturn=20170930155718 (illustrating how new technologies and monitoring policies can "significantly reduce the expectation of employee privacy").

44. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986); David Halpern, Patrick Reville & Donald Grunewald, *Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace*, 80 J. BUS. ETHICS 175, 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).

45. Mehta, *supra* note 35, at 614; *see also* City of Ontario v. Quon, 560 U.S. 746, 747 (2010).

46. Mehta, *supra* note 35, at 614; *see* Electronic Communications Privacy Act, §§ 101-111 (codified as amended at 18 U.S.C. §§ 2510-2521 (2012));.

47. Mehta, *supra* note 35, at 614; *see* Electronic Communications Privacy Act, § 101(b) (codified as amended at 18 U.S.C. § 2511(2)(a)(i)).

ECPA does not apply to communications prior to being sent or to communications once they have reached their recipient.[48]

Once these communications reach the recipient or are put in electronic storage for backup, these communications are then governed by Title II of the ECPA, the Stored Communications Act (SCA).[49] The SCA provides privacy protections to both files stored by the service providers and records about subscribers held by the service providers.[50] This subscriber information would include information such as subscriber name, billing records, or IP addresses.[51]

The ECPA affords employers three exceptions, providing some flexibility to access certain information that would normally be impermissible under the ECPA.[52] The first of these exceptions is known as the "prior consent" rule.[53] It allows the employer to intercept and/or access electronic communication when *one* party involved in the communication has given prior consent.[54] This means that an employer need not have the consent of both the sender and the recipient, so long as one of them has provided the employer with consent.

Strong concerns exist about prior consent in workplace privacy. Recognizing this reality, many states have enacted statutes that require the consent of all parties involved when recording a phone call or conversation.[55] Nevertheless, both courts and scholars have reasoned that privacy policies dealing with the use of certain electronic devices could easily satisfy the consent element.[56] For example, an employer could

---

48. 18 U.S.C. § 2511.

49. *Mehta, supra* note 35, at 614; *see* Electronic Communications Privacy Act, §§ 201-202 (codified as amended at 18 U.S.C. §§ 2701-2711); *see also* Julie 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).

50. Mehta, *supra* note 35, at 614; *see* 18 U.S.C. §§ 2701-2711; *see also* McMurry, *supra* note 49, at 598.

51. *See* 18 U.S.C. §§ 2701-2712.

52. Mehta, *supra* note 35, at 615.

53. *Id.*

54. *See, e.g.*, 18 U.S.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) (providing an exception when given "the lawful consent of the originator or an . . . intended recipient"); Halpern, Reville & Grunewald, *supra* note 44; Blackowicz, *supra* note 44, at 93; Gantt, *supra* note 44, at 356; McMurry, *supra* note 49, at 598 (explaining the prohibitions of unauthorized access and disclosure of stored electronic communications).

55. *Monitoring Employees' Off-Duty Conduct*, NOLO, https://www.nolo.com/legal-encyclopedia/monitoring-employees-off-duty-conduct-29994.html (last visited Nov. 2, 2017) ("In the private sector, a number of laws prohibit employers from intruding into their employees' lives outside of work.").

56. Mehta, *supra* note 35, at 615.

have a provision in their privacy policy stating that, by agreeing to the policy, all communications shared can be intercepted at any time. This would essentially allow the employer to use their privacy policy to satisfy the prior consent rule.

The second exception under the ECPA is known as the "provider" exception.[57] The provider exception allows an employer who furnishes the employee with a device to intercept or access information pertaining to the electronic communications that are either in transit or stored on that device.[58]

The third exception that is afforded to employers is known as the "ordinary course of business" exception.[59] This exception protects employers' rights and business property when the technology being used is "telephone equipment or facilities used within the ordinary course of business."[60] This exception applies when an employee is engaged in any activity that is a necessary part of their job. For example, a young associate who makes a call or sends an email to a client is performing a necessary part of their job during the course of her employment. Therefore, under the ordinary course of business exception, the employer would have the right to intercept the call or email.

As mentioned above, the exceptions to the ECPA provide employers with certain protections. As smart lenses become more prevalent in society, it is not unthinkable that an employee would want to be able to use their lenses while at work. It is also equally likely that an employer would want to be able to access any information that may be transmitted from these lenses while in the office. However, in order to gain access to the transmission of communications, an employer would need to satisfy one of the exceptions to the ECPA.

For example, with the first exception, the prior consent rule, scholars and courts have reasoned that privacy policies could effectively satisfy this consent.[61] This may allow an employer to use privacy policies to regulate the use of smart lenses within the parameters of the company.

---

57. Halpern, Reville & Grunewald, *supra* note 44; Blackowicz, *supra* note 44, at 91; Gantt, *supra* note 44, at 359.

58. *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).

59. *See* 18 U.S.C. §§ 2510(4), 2510(5)(a); *see also* Blackowicz, *supra* note 44, at 90.

60. *See* Blackowicz, *supra* note 44, at 90 (citing Gantt, *supra* note 44, 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 44.

61. Mehta, *supra* note 35, at 615.

Short of using privacy policies to allow access to the transmissions made by the smart lenses, companies may begin to ban them all together.

The second exception to the ECPA, the provider exception, would apply if an employer furnished, or provided, his or her employees with certain technologies.[62] It is highly unlikely that smart lenses will start being supplied to employees as readily as other technology, such as laptops and cell phones. It is hard to believe that an employer would require or force his or her employee to wear contact lenses. Thus, this exception is unlikely to affect smart lenses.

The third exception to the ECPA, the ordinary course of business exception, would apply if an individual were using technology and transmitting information as a necessary part of their job.[63] Therefore, smart lenses could be used as a part of an individual's job. For example, it is extremely likely that smart lenses will connect to a mobile device, such as a cell phone, to enhance the user's experience. An employee could then use this same device during the course of business, utilizing the connection to the smart lenses. If this type of use were to occur, it is likely that the use would fall under the ordinary course of business exception as well.

B. An Employer's Rights to Privacy

The concerns for workplace privacy do not stop with employees. Now that smart lenses are in the works and are potentially more likely to be used by the average citizen than the bulky wearable technologies that already exist, there is potential that the individuals that use smart lenses will use them at work. This could present a scary reality for employers who wish to keep their work product protected.[64] The exceptions to the ECPA were created to protect employers from potential wrongdoing by their employees.[65] Since the ECPA was enacted in 1986, there have been no considerations of how new technology or concepts would impact the scope of the protection that the ECPA provided for employers.[66]

If these new technologies are incorporated into the workplace, an unintended gap will emerge between the protections that employers seek

---

62. *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).

63. *See* 18 U.S.C. §§ 2510(4), 2510(5)(a); *see also* Mehta, *supra* note 35, at 616.

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

65. Mehta, *supra* note 35, at 616.

66. *Id.*

for their business and those they actually receive.[67] No new bright line rules or regulations that could help bridge this gap have emerged, and new wearable technologies, like smart lenses, will only serve to widen this gap until it is essentially a cavern between the employers and the rights they want (and arguably deserve).[68]

IV. PRIVACY IMPLICATIONS IN CRIMINAL LAW

The workplace is not the only place that smart lenses raise concerns. It is not an obscene concept that government and law enforcement officials will use this technology, raising a number of concerns in the criminal justice system. As a result, the use of smart lenses by law enforcement should receive special scrutiny as well as additional precautions.[69] This additional protection and scrutiny should also extend to law enforcement seeking to tap into private data that is stored within these smart lenses or their corresponding external storage.[70]

A. Police Seizing Information

When the government seeks to access privately held data that is collected from wearable technologies, strong constitutional and statutory protections should apply. The Fourth Amendment provides protections against invalid searches and seizures.[71] The Supreme Court has further reasoned that this Fourth Amendment protection extends to locations and items where an individual has an REOP.[72] The Court came up with a two-prong test to determine an individual's REOP in a location or an item.[73] First, an individual must display an actual, subjective expectation of privacy.[74] Second, that expectation must be recognized as reasonable by society.[75] There are a number of exceptions and nuances to the Fourth Amendment and *Katz* protections.

In addition to the Fourth Amendment, the ECPA is the primary federal statute that governs when law enforcement agencies may compel private entities to divulge information held on behalf of third-party subscribers.[76] It is unlawful to use illegally obtained communications as

---

67. *See id.*
68. *See id.*
69. *See* Thierer, *supra* note 14, at 115.
70. *See id.*
71. U.S. CONST. amend. IV.; *see* Katz v. United States, 389 U.S. 347, 353 (1967).
72. *Katz*, 389 U.S. at 361.
73. *Id.*
74. *Id.*
75. *Id.*
76. Thierer, *supra* note 14, at 116.

evidence.[77] Title I of the ECPA also provides procedures for government and law enforcement officials to obtain such communications.[78] Currently, under the ECPA, a judge may issue a warrant for the interception of information for up to thirty days.[79] This warrant may be issued upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in § 2516.[80] Congress should reform the ECPA to address smart lens concerns by requiring any government entity to acquire a warrant that has been issued upon the basis of probable cause before the government entity can access the privately held information, data, and communications.[81]

Smart lenses are likely to hold, or store on an external device, an individual's private data and information. It is also likely that during a police investigation, law enforcement would want to access this information. This would cause a search and seizure of both an individual's privately held information and their private technological devices. In so doing, an individual's Fourth Amendment rights against unreasonable search and seizure must be respected. Assuming that not every search and seizure during an investigation is done with a warrant, it is likely that this will occur in regards to smart lenses and the information that they hold.

Therefore, when looking to the reasonableness of a search and seizure, when a warrant is not present, the *Katz* REOP test applies.[82] The test focuses on both a subjective and objective right to privacy.[83] In the case of smart lenses, it is highly likely that an individual will have an expectation of privacy in the information that is collected and stored on his or her smart lenses and the storage device. This is privately held information that could potentially be very sensitive in nature. This would satisfy the subjective, actual expectation of privacy prong of the *Katz* test.

The second prong is the objective prong. This prong considers what expectations of privacy society has deemed to be reasonable.[84] In the

---

77. 18 U.S.C. § 2515 (2012).

78. Electronic Communications Privacy Act of 1986, §§ 101(c)(1)(A), 101(c)(8), 101(e), 104-05, 18 U.S.C. §§ 2516-2518.

79. 18 U.S.C. § 2518.

80. *Id.*

81. *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 129-30, 154 (2011).

82. *See generally* Katz v. United States, 389 U.S. 347 (1967).

83. *Id.* at 361.

84. *Id.*

case of smart lenses, it is extremely likely that society will find a reasonable expectation of privacy in an individual's smart lenses and the companion storage device. As mentioned above, the lenses and the storage device will likely contain sensitive information from an individual's life. Therefore, society will likely hold the smart lenses to the higher standard of privacy, thus satisfying the objective prong of *Katz*.[85]

Thus, in the event that law enforcement would like to gain access to the information stored or the data collected on an individual's smart lens, then a warrant would be required, pursuant to the Fourth Amendment.[86] However, absent a warrant, an individual's REOP would need to be assessed before gaining access to this information. It would be good practice for both law enforcement agencies and courts to require a warrant when searching and seizing privately held information that is collected and stored on technology such as smart lenses. This would prevent much dispute over REOP and Fourth Amendment violations in practice, as well as provide the protections to individuals who are using these lenses in their daily lives.

Another method that law enforcement may use to gain access to the data and information stored on smart lenses or another storage medium is the "third-party doctrine." The third-party doctrine holds that when an individual voluntarily divulges information to a third party, even when that party has promised to safeguard the data, the individual sacrifices their Fourth Amendment interest in that information.[87] It could be argued that once an individual captures an image or records a video and places it in cloud (or some other third-party) storage, the individual has voluntarily divulged this information to a third party, thus triggering the third-party doctrine. If this doctrine were to apply to the information that is gathered via smart lenses, then there would be no protection for information and insight into the most intimate details of a person's life. This does not seem to comport with the protections granted under the Fourth Amendment by the Supreme Court.

Smart lenses will likely have some form of external storage medium, whether it is an application linked to a smart phone or a cloud-based storage system. Depending on the storage medium used, one could argue that a user has divulged their once privately held information to a third party. Once this occurs, the REOP that an individual had in the

---

85. *See id.*

86. *See* U.S. CONST. amend. IV.

87. *See, e.g.*, Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1401-02 (2008).

information no longer exists; law enforcement can access the data and information, and the individual no longer has standing to challenge the Fourth Amendment violation (if one so exists).[88] This would be a slippery slope, allowing law enforcement to gather data and information about the very personal and private details of an individual's life, violating his or her REOP, without acquiring a warrant to do so.

B. Use of Technology by Law Enforcement

In addition to law enforcement agencies wishing to access information and data held on smart lenses, it is likely that law enforcement will use smart lenses during the course of their job. Currently many law enforcement agencies are now using technologies, such as "body cams."[89] Body cams are cameras worn by the police officer and used to record the interactions between the officer and a member of the public.[90] Body cams provide a unique insight into an officer's interactions with an individual and can often be used during criminal proceedings (by both prosecution and defense).

Body cam footage can provide details surrounding an investigation, arrest, or some other interaction between law enforcement and an individual. It is often used during a trial or criminal proceeding. The details learned from body cam footage could be essential to proving a key element in either the prosecution's or the defense's case in chief. Further, this footage can either build up or tear down the credibility of a witness in a case. Generally, this impeachment evidence is used by the defense team to discredit or challenge the credibility of the prosecution's witnesses.

With the use of body cams, a defendant typically has an idea of whether this type of evidence exists. It is easily discernible to an individual if a law enforcement agent is wearing a body cam. Therefore, an individual will generally be able to inform his or her attorney of the potential evidence that could be gained from the body cam footage.

However, smart lenses are not as obvious as body cams because they are much more discreet, but they are just as likely to be used by law enforcement in the future. Unlike body cams, smart lenses can be worn

---

88. *Id.* at 1402.

89. *See* JAY STANLEY, AM. CIVIL LIBERTIES UNION, POLICE BODY-MOUNTED CAMERAS: WITH RIGHT POLICIES IN PLACE, A WIN FOR ALL (2015), http://www.aclu.org/sites/default/files/assets/police_body-mounted_cameras-v2.pdf (updating JAY STANLEY, AM. CIVIL LIBERTIES UNION, POLICE BODY-MOUNTED CAMERAS: WITH RIGHT POLICIES IN PLACE, A WIN FOR ALL (2013)).

90. *Id.* at 1.

without an individual being aware of their existence. Smart lenses could be used during the course of an investigation to interview suspects, interview witnesses, or just take stock of a scene. Similar to body cams, smart lenses can gather this data and information to be used during a trial or other criminal proceeding. However, unlike body cams, it is much more difficult to see if this type of information or data exists. Further, it is highly unlikely that an individual would be able to tell if a law enforcement agent they had an encounter with was wearing smart lenses or not. This would mean that smart lenses could pose problems to an individual and his or her defense team when trying to locate any data or information from the individual's interaction with law enforcement.

The American Civil Liberties Union (ACLU) "best practices" for law enforcement agencies and officials may serve as a guide for proper smart lens usage.[91] The ACLU developed these practices for the use of body cams.[92] Some of the suggestions set forth by the ACLU include that the citizens be notified of the fact that they are being recorded, that the data "be retained no longer than necessary for the purpose for which it was collected," and "that this technology not become a backdoor for any kind of systematic surveillance or tracking of the public."[93]

Similarly, these best practices would be an ideal template for mapping out how officers wearing smart lenses conduct themselves in the line of duty. Following the guidelines laid out by the ACLU, a police officer wearing smart lenses should be required to tell an individual that they are being recorded by the smart lenses. This would provide the notice and protection that the ACLU has intended for the individual.

Further, the information that is recorded during such an encounter should not be kept for any longer than necessary, nor used for any other reason than that which a body cam would be allowed. The biggest concern and criticism of allowing police officers to use smart lenses in lieu of or in addition to body cams is the possibility that the technology will be used as a backdoor, or a discreet way to monitor and survey the public.[94] This would be an egregious violation of an officer's duty, breeding mistrust of the police in a time where tensions are already running high in that regard.

---

91. *See id.*

92. Adi Robertson, *The ACLU Wants Police Officers To Wear Cameras, but Only with Privacy Restrictions,* VERGE (Oct. 9, 2013, 2:09 PM), http://www.theverge.com/2013/10/9/4820600/aclu-issues-guidelines-for-police-officercameras.

93. STANLEY, *supra* note 89, at 5-7.

94. *See id.* at 7.

VI. CONCLUSION

Wearable and advanced technology has been used in our society for a number of years now. Once mundane objects have now become "smart," using advanced technology to make the objects more appealing, efficient, or user friendly.[95] This type of advanced technology, particularly wearable technology, constantly gathers massive amounts of data and information. This alone is enough to raise concerns regarding one's privacy.

However, smart lenses exemplify the type of discreet technology that is capable of constantly gathering data and information without an individual's knowledge, posing even greater concerns for one's privacy. Smart lenses will be capable of gathering and storing data and information about the intimate details of an individual's life, making it ripe for cybercriminals, such as hackers, to attack.[96]

With the right codes and determination, it is possible for a cybercriminal to gain access to the devices that we currently wear every day.[97] However, up to this point the technologies have been more trouble than they are worth.[98] Smart lenses will change this, causing cybercriminals to attempt to gain access to the information that is held on them.

Smart lenses are also likely to make an appearance in our daily lives. These lenses are much more attractive and less bulky than current, comparable technology, which will lead to more people wearing and using them. It is likely that smart lenses will be worn by both private citizens and law enforcement alike. This has the potential to pose a challenge to the current laws in place.

Employers may have increasing concerns regarding the use of smart lenses by their employees. It is likely that the protections provided to employers by the ECPA will apply to smart lenses, at least in some capacity, if not fully. The exceptions to the ECPA will provide employers with some flexibility when they wish to access information that is stored on their employees' smart lenses or storage device. Further, the increased use of smart lenses may completely shape how a workplace operates, implementing privacy policies or new workplace policies to govern the use or data collection of the smart lenses.

---

95. Thierer, *supra* note 14, at 4-5.
96. Sony Patent, *supra* note 8.
97. Nield, *supra* note 27.
98. *Id.*

Smart lenses are also likely to be used by law enforcement, whether in an official capacity or accessing the data used in an investigation. When gathering data for an investigation, the strong constitutional protections that currently exist should be upheld.[99] A court should consider an individual's REOP in the information and data contained on his or her smart lenses or storage medium.[100]

In addition to gaining access and using the information during the course of an investigation, law enforcement will likely use smart lenses on duty. While this technology is similar to the current use of body cams, it is distinguishable and should be treated as such. The ACLU's best practices for body cam usage should be extended to the use of smart lenses.[101] I would argue that best practices for smart lenses should go further, providing the utmost protection to individuals when the police are involved.

Smart lenses may not be at the forefront of technology today, but they will be in the near future. The current laws in place are not equipped to deal with this type of technology, creating a gap between the technology of smart lenses and the practical applications and concerns posed by them. We are, quite simply, legally behind the times, and it will take some serious changes before our current laws and jurisprudence are equipped to handle the new challenges that smart lenses will bring.

---

99. *See* U.S. CONST. amend. IV; *see also* Katz v. United States, 389 U.S. 347, 353 (1967).

100. *See Katz*, 389 U.S. at 361.

101. *See* STANLEY, *supra* note 89.