Journal of Technology Law & Policy

Volume XVII – Spring 2017

ISSN 2164-800X (online)

DOI 10.5195/tlp.2017.197

http://tlp.law.pitt.edu

Wearable Evidence: Why the Pennsylvania Judiciary Should Require a Warrant to Search Wearable Technology

Pat Augustine

Wearable Evidence: Why The Pennsylvania Judiciary Should Require A Warrant To Search Wearable Technology

Pat Augustine*

INTRODUCTION

Wearable technology has revolutionized the lives of those who wear them.[1] New digital devices enable consumers to easily collect mass amounts of data pertaining to various aspects of their lives simply by wearing a watch, armband, or shirt.[2] Whether they are recording health statistics with their Fitbits,[3] sharing pictures through Google Glass,[4] or making calls from their Apple Watches,[5] wearable technology has allowed consumers to store, collect, and share information more conveniently than ever before.[6] While shopping for such cutting edge technology,[7] it is unlikely that consumers are considering the implications it might have when they encounter the police.

---

* J.D. Candidate, 2017, University of Pittsburgh School of Law, Staff Editor, *University of Pittsburgh Journal of Technology Law and Policy*.

[1] *See* Katherine Saphner, Note, *You Should Be Free to Talk the Talk and Walk the Walk: Applying Riley v. California to Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1690 (2016) (describing wearable technology as an "extension of the wearer").

[2] *See, e.g.*, Spela Kosir, *A Look at Smart Clothing for 2015*, WEARABLE TECHNOLOGIES (Mar. 23, 2015), https://www.wearable-technologies.com/2015/03/a-look-at-smartclothing-for-2015/.

[3] *See, e.g.*, *Fitbit Charge*, FITBIT, https://www.fitbit.com/charge (last visited Aug. 26, 2016).

[4] *See, e.g.*, *Google Glass*, GOOGLE, https://developers.google.com/glass/develop/gdk/reference/ (last visited Aug. 26, 2016).

[5] *See, e.g.*, *Apple Watch*, APPLE, http://www.apple.com/watch/more-to-love/ (last visited Aug. 26, 2016).

[6] Tristan M. Ellis, Note, *Reading Riley Broadly: A Call For a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest*, 80 BROOK. L. REV. 463, 487 (2015) (citing Zara Stone, *SmartWhat? Smartwatch. Just, Why?*, ABC NEWS (Sept. 5, 2013), http://abcnews.go.com/ABC_Univision/smartwatch-whats-deal-web-connected-wrist-candy/story?id=20168783 (discussing the ease of access to messages, applications, and other data on a smart watch)).

[7] *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 31 (2015) (discussing both fitness applications and other uses of wearable fitness tracker devices).

Journal of Technology Law & Policy

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

The success of wearable devices has been incredible.[8] Experts estimate that the market for wearable technology is currently worth around $14 billion, a valuation that is expected to double by 2020.[9] More significant than the success of the industry is the growing interdependent relationship between consumers and wearable technology,[10] and the value of information stored on such devices.[11] For example, wearable technology may take the form of a bracelet or watch[12] and can be worn throughout the day and night.[13] The device follows the consumer closely, collecting data about the consumer's every move,[14] painting a picture of everything that happens to the consumer throughout their day.[15] Considering that someone may automatically put on their smart watch as a part of their daily routine, they may not be thinking of any legal ramifications which may follow. The consumer may not realize that their device essentially serves as the perfect eyewitness that can be seized, searched, and used against the consumer in court.

The law already recognizes the importance of information collected by wearable technology by requiring warrants to search similar sources of information.[16] The United States Supreme Court has held that the type of information stored on wearable technology is part of the consumer's "virtual home"[17] and should

---

[8] *See* Paul Lamkin, *Wearable Tech Market To Be Worth $34 Billion By 2020*, FORBES (Feb. 17, 2016, 9:31 AM), http://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#78e0658c3fe3 (discussing the growth potential in the wearable technology industry).

[9] *Id.*

[10] *See* Saphner, *supra* note 1, at 1690–91 (citing Sara M. Watson, *Stepping Down: Rethinking the Fitness Tracker*, ATLANTIC (Sept. 25, 2014), http://www.theatlantic.com/technology/archive/2014/09/hacking-the-fitness-tracker-to-move-less-not-more/380742 (claiming that the author's Fitbit was an "extension of [her] awareness of distance, of quantified movement through space")).

[11] Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 127 (2014) (discussing the private nature of the information collected by wearable technology and its value to insurers, creditors, and employers of the wearer).

[12] *See, e.g.*, *Samsung Gear S2*, SAMSUNG, http://www.samsung.com/us/explore/gear-s2/ (last visited Aug. 28, 2016); *Up2*, JAWBONE, https://jawbone.com/store/buy/up2 (last visited Sept. 1, 2016).

[13] *See* Saphner, *supra* note 1, at 1690–91.

[14] Peppet, *supra* note 11, at 88 (explaining that these devices count every step the wearer takes).

[15] Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J.L. & TECH. 9, 14 (2016) (explaining that a litigant's Fitbit was used to gauge her daily physical fitness levels after an accident).

[16] Riley v. California, 134 S. Ct. 2473, 2489 (2014) (detailing the private nature of the types of information held on cellphones such as pictures, location information, and addresses).

[17] Ellis, *supra* note 6, at 469–70 (describing the collection of information as the user's "virtual home").

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

be entitled to a wide degree of privacy.[18] The law is unsettled as to what degree of protection the Fourth Amendment affords to consumers who encounter police while in possession of wearable technology.[19] For example, it is unclear whether police can search through an arrestee's Fitbit data or the information stored in their smart watch. While the U.S. Supreme Court has ruled that law enforcement must obtain a warrant before searching an arrestee's cellphone,[20] it has not yet considered other forms of wearable technology.[21] In a recent Pennsylvania trial court case, the Lancaster County Court of Common Pleas discovered that the information on a woman's Fitbit may have invalidated her rape claim.[22] In the investigation of the rape, police discovered the alleged victim's Fitbit, which revealed numerous inconsistencies in her testimony.[23] This case has brought to light the search and seizure implications that can result if it is the defendant, rather than a victim, whose device is searched.

This Article examines the issue of search and seizure law in Pennsylvania as it pertains to wearable technology. Part I provides a survey of existing search and seizure law in the digital age, including the erosion of privacy interests. Part II discusses how Federal and Pennsylvania courts have exhibited shared concerns for privacy in the digital age, but stresses that the former has diminished privacy interests while the latter has not. The role of changing technology is included in this discussion. Part III considers precedential, historical, and policy reasons why the Pennsylvania judiciary should require law enforcement to obtain a warrant before searching wearable technology, and predicts that the Supreme Court of Pennsylvania will uphold this requirement if it is imposed by lower courts.

---

[18] *See generally* Peppet, *supra* note 11.

[19] *See* Ellis, *supra* note 6, at 489 (explaining that the Fourth Amendment does not secure any general right to privacy and cautioning that protections could erode in the future).

[20] *Riley*, 134 S. Ct. at 2491 (explaining the "privacy interests at stake" when searching a cellphone).

[21] *See* Ellis, *supra* note 6, at 491 (explaining that the Supreme Court has laid the ground work for mobile devices but has not had occasion to deal with one other than a cellphone).

[22] *See* Myles Snyder, *Police: Woman's Fitness Watch Disproved Rape Report*, ABC 27 NEWS (June 19, 2015, 2:03 PM), http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/; *see also* Commonwealth v. Risley, Criminal Docket: CP-36-CR-0002937-2015 (Lancaster Cty., Pa., printed Nov. 16, 2015) (an alleged victim's claim of sexual assault was undermined by discovery of her Fitbit at the scene, she was subsequently prosecuted).

[23] *Id.*

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

I. FOURTH AMENDMENT JURISPRUDENCE AND THE DIGITAL WORLD

The Fourth Amendment of the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution prohibit unreasonable searches and seizures.[24] The constitutional protections against unreasonable search and seizure are firmly rooted in the "principles of humanity and civil liberty."[25] The protections established by the Fourth Amendment provide a baseline for which state constitutions may expand upon, but may not encroach.[26] To that end, the Pennsylvania Constitution has a long history of affording its citizens increased protections against governmental intrusion than the protections afforded by the federal government.[27] Pennsylvania has tied the right to be free from unreasonable searches and seizures to the implicit right of privacy.[28] Conversely, the same right to privacy that the Pennsylvania Constitution has expanded has been eroded under the Federal constitution.[29]

The robust protections afforded by the Pennsylvania Constitution have not been met on a federal level. Over time our nation's Supreme Court has held that more and more situations do not mandate the exclusionary rule as a constitutional remedy.[30] For example, the Fourth Amendment of the United States Constitution allows for a "good faith exception"[31] which the Pennsylvania Constitution does not.[32] Similarly, the Pennsylvania Constitution limits the third-party exception that the Fourth amendment allows for government searches.[33] All in all, the reluctance of Pennsylvania courts to adopt the same exceptions that the Federal courts have

[24] U.S. CONST. amend. IV; PA. CONST. art. I, § 8.

[25] Bram v. United States, 168 U.S. 532, 544 (1897).

[26] Commonwealth v. Henderson, 437 A.2d 387, 390 (Pa. 1981).

[27] Commonwealth v. Gayle, 673 A.2d 927, 931 n.9 (Pa. Super. Ct. 1996); Commonwealth v. Wright, 672 A.2d 826, 829 n.5 (Pa. Super. Ct. 1996); Commonwealth v. Edmunds, 586 A.2d 887 (Pa. 1991).

[28] Commonwealth v. Moore, 928 A.2d 1092 (Pa. Super. Ct. 2007) (a prisoner had no Fourth Amendment or Article I, Section 8 right to privacy in his non-privileged prison mail); Commonwealth. v. Viall, 890 A.2d 419 (Pa. Super. Ct. 2005) (unreasonable expectation of privacy in objects recovered from a common area in the back seat that was not shielded from view of the many others occupying the same small space); Commonwealth v. DeJohn, 403 A.2d 1283 (Pa. 1979).

[29] Louis A. Smith, II, *Pennsylvania's Constitutional Right to Privacy: A Survey of its Interpretation in the Context of Search and Seizure and Electronic Surveillance*, 31 DUQ. L. REV. 557, 562 (1993).

[30] *Id.*

[31] United States v. Hoffa, 385 U.S. 293, 302 (1966).

[32] *Edmunds*, 586 A.2d at 896.

[33] *DeJohn*, 403 A.2d at 1292.

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

adopted shows a clear difference in which interests each constitution seeks to advance.[34]

Though an individual's right to privacy in Pennsylvania is fundamental, courts have held that in certain situations, it can be abridged.[35] These situations exist where there is a government interest that is so compelling, it warrants the diminishment of one's right to privacy in order to achieve some greater societal objective.[36] The determination of whether individual privacy rights trump the interests of society as a whole involves the balancing of both interests by the court.[37]

The constitutional right of privacy is significant, however it is not unqualified.[38] Accordingly, one instance where the U.S. Supreme Court has held that state interests trump an individual's expectation of privacy is in the context of arrest.[39] When there is probable cause to arrest someone, that person has a diminished expectation of privacy.[40] The government's interest in preventing the destruction or concealment of evidence and maintaining the arresting officer's safety outweigh an arrestee's expectation of privacy, and a search incident to arrest is an exception to the warrant requirement.[41] Though the scope of this exception has been historically disputed across jurisdictions,[42] the arresting officer maintains the right to search the arrestee and the area within their immediate control.[43]

A. From Riley v. California *Onward*

There is tension between the slow pace at which the law adapts and the rapid development of technology.[44] The U.S. Supreme Court is cognizant of advancing

---

[34] Smith, *supra* at note 29, 567–68.

[35] Pa. Soc. Servs. Union, Local 688 v. Commonwealth, 59 A.3d 1136, 1145 (Pa. Commw. 2012).

[36] *Id.*

[37] Commonwealth v. Brundidge, 620 A.2d 1115, 1118 (Pa. 1993).

[38] Stenger v. Lehigh Valley Hosp. Center, 609 A.2d 796, 800 (Pa. 1992).

[39] Arizona v. Gant, 556 U.S. 332, 338 (2009) (citing Weeks v. United States, 232 U.S. 383, 398 (1914)).

[40] United States v. Mitchell, 652 F.3d 387, 405 (3d Cir. 2011).

[41] *See Gant*, 556 U.S. at 339 (citing Chimel v. California, 395 U.S. 752, 763 (1969)).

[42] *Cf.* Commonwealth v. White, 669 A.2d 896 (Pa. 1995); New York v. Belton, 453 U.S. 454 (1981).

[43] *Gant*, 556 U.S. at 339 (*citing Chimel*, 395 U.S. at 763); *accord* Commonwealth v. Bess, 382 A.2d 1212, 1214 (Pa. 1978).

[44] Ellis, *supra* note 6, at 467–68 (explaining that by the time a case has reached upper level appellate review, the technology in question is often obsolete).

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

technological developments,[45] and the nefarious purposes for which law enforcement may use them to see inside the private lives of those suspected of wrongdoing.[46] The Court's sudden rush to protect privacy interests in the wake of rapidly changing technology conflicts with the historical degradation of privacy interests in federal search and seizure law.[47] The Court's shift is likely the result of the widespread use of technological advancements and their importance in everyday life.[48] With this progressive perspective,[49] the Supreme Court in *Riley v. California* examined the issue of whether the Fourth Amendment requires law enforcement to obtain a warrant before searching a suspect's cellphone.[50] The Court accepted that cellphones are large digital data storage devices, the likes of which have never been seen.[51] It acknowledged that private information is regularly stored on cellphones and therefore deserves protection.[52] The Court explained that the mass and quality of information stored on a cellphone is more akin to that which is stored in a house than anything that a person would carry around with them.[53] In doing so, the Court reasoned that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him."[54] The Court did not stop at likening the cellphone to a house, it explained that a search of a cellphone would typically expose much more

---

[45] *Cf.* Kyllo v. United States, 533 U.S. 27, 36 (2001) (When examining police use of thermal imaging on the home, the Court explains that "the rule [the Court] adopt[s] must take account of more sophisticated systems that are already in use *or in development*") (emphasis added); *see also* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (noting that the government may develop ways to reproduce documents in court without "removing papers from secret drawers").

[46] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (In the context of wiretapping, Justice Brandeis discusses the future of police intrusion in stating "our contemplation cannot be only of what has been *but of what may be*. The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping") (emphasis added).

[47] *See* Ellis, *supra* note 6, at 466 (discussing the continued expansion of exceptions to the warrant requirement and suggesting *Riley* is a break from this trend).

[48] Riley v. California, 134 S. Ct. 2473, 2484 (2014) (explaining that cellphones are a "pervasive and insistent part of daily life").

[49] Ellis, *supra* note 6, at 467–68 (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[50] *Riley*, 134 S. Ct. at 2494.

[51] *Id.* at 2490 (discussing storage capacity and explaining that people carry large amounts of data on their cellphones and that ordinarily a person does not carry an expansive collection of records like this in document form).

[52] *Id.* (discussing that a simple search of a cellphone's internet history can reveal a person's most private interests or concerns such as symptoms of a disease).

[53] *Id.*

[54] United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926).

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

information about a person than a search of a house would.[55] *Riley* laid the groundwork of constitutional protection[56] that could be expanded to wearable technology.[57] However, the Court's limited holding in *Riley*[58] is merely the beginning of the analysis on wearable technology.[59]

B. Pennsylvania's Heightened Protection Against Intrusion

When considering searches in the digital age, Pennsylvania courts have echoed the response of the *Riley* Court: "Get a warrant."[60] This response was not merely created by an obligation to follow precedent.[61] Pennsylvania courts have repeatedly guaranteed a heightened level of privacy in the context of the Fourth Amendment and Article I, Section 8 of the Pennsylvania Constitution than the U.S. Supreme Court.[62] This guarantee is not limited to digital-age technology.[63] The Pennsylvania Constitution, though similarly worded to the U.S. Constitution,[64] has historically guaranteed rights under the law of search and seizure that the Fourth Amendment has not.[65]

The test for determining whether an unreasonable search has occurred is the same under both Article I, Section 8 of the Pennsylvania Constitution and the Fourth Amendment of the U.S. Constitution.[66] The difference is that Article I, Section 8 implicitly extends constitutional protection to those areas where a person has a reasonable expectation of privacy.[67] Mere phraseology becomes inconsequential, as

---

[55] *Riley*, 134 S. Ct. at 2491 (acknowledging that "Indeed, a cellphone search would typically expose to the government far more than the most exhaustive search of a house").

[56] *See* Ellis, *supra* note 6, at 469.

[57] *Id.* at 467–68.

[58] *See Riley*, 134 S. Ct. at 2494–95.

[59] Ellis, *supra* at note 6, at 466–67.

[60] Commonwealth v. Stem, 96 A.3d 407, 413 (Pa. Super. 2014) (citing Riley v. California, 134 S. Ct. 2473 (2014)).

[61] *Id.*

[62] Smith, *supra* note 29, at 557 (discussing Pennsylvania's history of increasing rights against governmental intrusion); *see also* Commonwealth v. DeJohn, 403 A.2d 1283 (1979).

[63] *See* Commonwealth v. Chaitt, 112 A.2d 379 (1955) (acknowledging a specific right to privacy before the U.S. Supreme Court recognized this right in *Griswold v. Connecticut*, 381 U.S. 479 (1965)).

[64] Commonwealth v. McCree, 924 A.2d 621, 627 (Pa. 2007).

[65] *See* Smith, *supra* note 29, at 557–58 (citing Commonwealth v. Edmunds, 586 A.2d 887 (Pa. Super. Ct. 1991); *see also* Barasch v. Pa. Pub. Util. Comm'n, 576 A.2d 79 (Pa. Commw. 1990)).

[66] Commonwealth v. Russo, 934 A.2d 1199, 1211 (Pa. 2007).

[67] In Interest of B.C., 683 A.2d 919, 926 (Pa. Super. Ct. 1996).

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

Pennsylvania state courts have clearly demarcated the focus of both constitutions.[68] The U.S. Supreme Court has held that the U.S. Constitution, with an eye for the wrongs done by the government, aims to deter police misconduct.[69] The Pennsylvania Supreme Court has interpreted that its Constitution has deep roots in the principles of individual liberty, and emphasizes the protection of privacy.[70] These diverging approaches produce two different results when determining the privacy rights of citizens. While the U.S. Constitution gives way to an increasing number of situations in which the exclusionary rule does not apply,[71] Article I, Section 8 remains stalwart in its defense of privacy, protecting many areas and situations from governmental intrusion which are no longer recognized on the federal level.[72]

The effect of Article 1, Section 8's implicit right to privacy takes form in a court's determination of reasonableness.[73] As previously stated, when determining whether a search or seizure is unreasonable under Article I, Section 8, Pennsylvania courts use the same two-part test as the federal courts.[74] In determining whether society is willing to accept a privacy interest as reasonable and legitimate, state and federal courts balance the weight of an individual's privacy interests versus competing government interests.[75] However, Pennsylvania courts have placed a much heavier emphasis on an individual's privacy interest when balancing these

[68] Commonwealth v. Hughes, 836 A.2d 893, 903 (Pa. 2003).

[69] *Id.*

[70] *Id.*

[71] Pa. Soc. Serv. Union, Loc. 688 v. Commonwealth, 59 A.3d 1136, 1144 (Pa. Commw. 2012).

[72] *See* Smith, *supra* note 29, at 557–58; *see also* Commonwealth v. Berkheimer, 57 A.3d 171 (Pa. Super. 2012) (declining to follow the inevitable discovery rule in Pennsylvania); Commonwealth v. DeJohn, 403 A.2d 1283, 1292 (Pa. 1979) (limiting the third party exception and requiring police to seek a warrant for bank records); Commonwealth v. Sell, 470 A.2d 457, 467 (Pa. 1983) (granting automatic standing to those charged with possessory offenses); Commonwealth v. Edmunds, 586 A.2d 887, 896 (Pa. 1991) (declining to adopt a "good faith" exception to the exclusionary rule); *but see* Commonwealth v. McCree, 924 A.2d 621, 630 (Pa. 2007) (acknowledging that Pennsylvania has adopted a "*limited* automobile exception") (emphasis added).

[73] *See* Commonwealth v. Enimpah, 62 A.3d 1028, 1032 (Pa. Super. 2013); *see also* Commonwealth v. Beaman, 880 A.2d 578, 582 (Pa. 2005).

[74] Commonwealth v. Gary, 91 A.3d 102, 127 (Pa. 2014).

[75] Commonwealth v. Bostick, 958 A.2d 543, 552 (Pa. Super. 2008).

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

concerns against their competing state interests.[76] Thus, Article I, Section 8 has been interpreted in a manner that gives greater protection than the Fourth Amendment.[77]

In *Commonwealth v. Edmunds*, the Pennsylvania Supreme Court made, what is arguably, its most astounding showing of its continued commitment to provide increased protections under Article 1, Section 8.[78] The Pennsylvania Supreme Court examined whether adding a good faith exception to Pennsylvania's Article I, Section 8 would be consistent with the Commonwealth's jurisprudence.[79] Though this exception was present in the Federal Constitution,[80] this broadens the protections of Article I Section 8.[81] The Court established four factors that enable litigants to invoke the state right of privacy, both offensively and defensively, to combat excessive governmental intrusion.[82] Conversely, the Court also allows the government to use the factors in *Edmunds* to argue for an exception to the warrant requirement.[83] In doing so, the Court emphasized that they would look to textual, historical, precedential, and policy considerations that warrant greater protection than the Fourth Amendment.[84] The Court's strong federalist philosophy[85] and its continued commitment to safeguarding the right to privacy[86] are reasons for which wearable technology should be protected by the warrant requirement.

II. PENNSYLVANIA'S NEXT STEP: EXTENDING *RILEY* TO COVER WEARABLE TECHNOLOGY

The next step for the judiciary to take in defense of Pennsylvania's constitutional right to privacy, is extending the decision in *Riley v. California* to cover all high-tech, wearable devices and the data they store. Such a holding is the

[76] *See* Smith, *supra* note 29, at 568–72 (discussing the emphasis that Pennsylvania courts have placed on this interest and the importance of raising privacy concerns when challenging a search and seizure issue).

[77] *Id.*; *see also Edmunds*, 586 A.2d at 896 (creating a test to allow for areas not covered under federal law to be recognized as private in Pennsylvania).

[78] *See Edmunds*, 586 A.2d at 896.

[79] *Id.* at 894.

[80] *Id.* at 898.

[81] *Id.* at 894.

[82] Smith, *supra* note 29, at 580–81.

[83] *See e.g.*, Commonwealth v. Edmunds, 586 A.2d 887, 895 (Pa. 1991).

[84] Commonwealth v. Gary, 91 A.3d 102, 124 (Pa. 2014) (citing *Edmunds*, 586 A.2d at 895).

[85] Smith, *supra* note 29, at 567–68.

[86] *See id.*

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

natural antecedent of not only the jurisprudence of Pennsylvania,[87] but also that of the Fourth Amendment in the wake of vast technological advances.[88] In order to make a solid argument for the expansion of *Riley*, an *Edmunds* analysis and a discussion of the policy considerations surrounding wearable technology are necessary.

A. The Factors in Edmunds *Support Protecting Wearable Technology*

The first factor in *Edmunds* requires a consideration of the text of Article I, Section 8.[89] The Pennsylvania Supreme Court has noted that the text in Article I, Section 8 is similar to that of the Fourth Amendment on numerous occasions.[90] Textual similarities between Article 1, Section 8 and the Fourth Amendment do not require identical interpretation.[91] However, there is nothing in the text of Article 1, Section 8 that suggests additional protection for technological advances is warranted. Though this factor does not affirmatively support requiring a warrant, the remaining factors do require such.

The second *Edmunds* factor requires a historical and precedential analysis.[92] This analysis can be difficult because wearable technology is new and does not have the benefit of extensive historical legal analysis or use.[93] Therefore, a consideration of Pennsylvania's treatment of technological advances in general may be most persuasive in this area. There is no question that Pennsylvania courts have strongly supported the constitutional right to privacy in regards to rapid advances in technology.[94] On several occasions the courts have shown a willingness to provide increased protections to technological advances under Article I, Section 8.[95] The judiciary's willingness to provide increased protections accompanies its awareness

---

[87] *See id.* at 33 (explaining that it has been the continuing trend of Pennsylvania to increase privacy rights).

[88] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 36 (2001); Riley v. California, 134 S. Ct. 2473, 2494 (2014).

[89] Commonwealth v. Edmunds, 586 A.2d 887, 896 (Pa. 1991).

[90] Commonwealth v. Russo, 934 A.2d 1199, 1205 (Pa. 2004); Commonwealth v. Chase, 960 A.2d 108, 117 (Pa. 2008) (plurality); Commonwealth v. Gray, 503 A.2d 921, 926 (Pa. 1985).

[91] *See, e.g.*, Commonwealth v. Waltson, 724 A.2d 289, 291 (Pa. 1998).

[92] Commonwealth v. Gary, 91 A.3d 102, 125 (Pa. 2014).

[93] *See* Peppet, *supra* note 11, at 101–02 (explaining that certain wearables have come about only recently).

[94] *See*, *e.g.*, Barasch v. Pa. Pub. Utils. Comm'n, 576 A.2d 79 (Pa. Commw. 1990); Commonwealth v. Stem, 96 A.3d 407 (Pa. Super. 2014); Commonwealth v. Chaitt, 112 A.2d 379 (Pa. 1955).

[95] *See id.*; *see also* Commonwealth v. Murray, 223 A.2d 102, 105 (Pa. 1966).

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

of the effects that technology can have in the realm of search and seizure.[96] This ever-present cognizance of the effect technology may have on the rights of its citizens directly aligns with their continual granting of increased liberties and a more expansive right of privacy.[97] Therefore, it is clear that the law in Pennsylvania has displayed a willingness to adjust with the change in technology over its history and provide increased rights where it is constitutionally necessary.

The third *Edmunds* factor involves an analysis of how other jurisdictions address wearable technology in the context of search and seizure.[98] Similar to the analysis of the second Edmund's factor, a problem arises due to the minimal amount of cases pertaining to wearable technology. However, precedent involving high tech devices similar to wearable technology may be analogous or at the least persuasive, and provide overlapping rationales for why their wearable counterparts should be subject to increased privacy.[99] To that end, an examination into cases involving other high tech devices that contain similar information may be persuasive in justifying the need for a warrant to search wearable technology.

In the aftermath of *Riley*, other jurisdictions have exhibited mixed responses to increasing protections against governmental intrusion of high tech electronic devices.[100] For example, the Wisconsin Supreme Court interpreted *Riley* broadly, focusing on the private nature of the contents of a cellphone.[101] In doing so, the Court held that detained citizens have a legitimate expectation of privacy in regards to their electronic devices.[102] In *State v. Putrell*, the Wisconsin Supreme Court examined whether a warrantless search of a probationer's computer was lawful.[103] While the Court did find the search lawful, it did so solely because of the petitioner's status as a probationer.[104] The Court held that absent these probationary restrictions, ordinary citizens would be protected against this type of search.[105] The Court explained that absent probation conditions that render the device contraband, the computer holds

[96] Smith, *supra* note 29, at 557–58.

[97] *See id.* (explaining that in light of modern intrusions the court has displayed a continued willingness to adjust to technology while maintaining privacy rights).

[98] Commonwealth v. Gary, 91 A.3d 102, 128 (Pa. 2014).

[99] *See* Saphner, *supra* note 1, at 1710–11.

[100] *Id.* at 1704.

[101] State v. Purtell, 851 N.W.2d 417, 427 (Wis. 2014).

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

within itself private information about the user which are entitled to a reasonable expectation of privacy.[106]

The Indiana Court of Appeals also had an opportunity to review the warrantless search of an electronic device after *Riley*.[107] In the aftermath of the landmark decision in *Riley*, the Indiana Court of Appeals examined whether the warrantless seizure of a GPS device was constitutionally permissible.[108] The Court discussed the ability of the GPS to store a massive amount of data, between 16 to 28 gigabytes.[109] Additionally, the Court explained that data describing an individual's location is private in nature and may reveal a plethora of details about a person's life which they would not readily disclose to the public.[110] The Court likened these types of devices to computers and cellphones due to the type of data they store and their capacity.[111] As a result, the Court held that the warrantless search of the GPS device was inappropriate.[112]

Other states such as Florida and North Carolina have also extended *Riley* to allow for increased protections that are not afforded under the U.S. Constitution.[113] The courts in each respective state gave similar reasoning.[114] Each individual court took caution from the analysis in *Riley* and held that all electronic devices are subject to the warrant requirement.[115] Above all, these state court decisions regarding searching high tech storage devices focus on the storage capacity of these devices and the information they contain, not merely the physical device itself.[116]

Some states, however, have not heeded the warnings embedded in the analysis in *Riley* and have interpreted the case narrowly.[117] They have taken the high Court's

---

[106] *Id.*

[107] Wertz v. State, 41 N.E.3d 276, 287 (Ind. Ct. App. 2015).

[108] *Id.*

[109] *Id.* at 279.

[110] *Id.* at 283–84.

[111] *Id.* at 280.

[112] *Id.* at 281.

[113] *See, e.g.*, Willis v. State, 148 So. 3d 480 (Fla. Dist. Ct. App. 2014) (declining to allow a good-faith exception for the warrantless search of a cellphone); State v. Clyburn, 770 S.E.2d 689 (N.C. Ct. App. 2015) (holding that the protections in *Riley* applied to GPS devices).

[114] *Willis*, 148 So. 3d at 482; *Clyburn*, 770 S.E.2d at 694.

[115] *Willis*, 148 So. 3d at 482; *Clyburn*, 770 S.E.2d at 694.

[116] *Willis*, 148 So. 3d at 482; *Clyburn*, 770 S.E.2d at 694.

[117] *See, e.g.*, State v. Carle, 337 P.3d 904 (Or. Ct. App. 2014) (declining to extend *Riley* protections to information sent out of an electronic device); Sinclair v. State, 118 A.3d 872 (Md. 2015) (declining to

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

holding to mean that only cellphones should be subject to the warrant requirement and in doing so, have not addressed whether many high tech devices that currently exist would also be subject to the warrant requirement.[118] For example, the California Court of Appeals declined to extend *Riley* to digital cameras.[119] In *People v. Raoult*, the California court had the chance to examine the warrantless search of a digital camera found in the defendant's car.[120] The Court decided in this case that *Riley* could not be stretched to encompass cameras under the warrant requirement.[121] The Court's reasoning was that digital cameras do not share many of the capabilities of smartphones, except for their ability to take and store photos.[122] Police therefore have a limited ability to reconstruct a person's life by searching their digital cameras.[123] The court seems to disregard key aspects of the *Riley* decision, such as capacity.[124] Many other jurisdictions, despite limiting constitutional protection to cellphones, still acknowledge the critical privacy interests associated with devices that store electronic information.[125] However, this narrow interpretation of *Riley* cannot possibly continue, as it would result in a chaotic outcome, leaving courts in the fog about how to treat these massive sources of information.

All opinions duly noted under this factor, the Pennsylvania judiciary should give deference to the many states which have adopted a broad interpretation of *Riley*, and protect electronic devices in general. Wearable technology shares many key characteristics with cellphones and store much of the same types of personal information.[126] Extending constitutional protection to all wearable technology means safeguarding vital information such as health statistics, photographs, geolocation,[127] etc. Indeed the list of information that wearable technology may become capable of

extend *Riley* to the plain view of information on a cellphone); People v. Raoult, 2d Crim. No. B256148, 2015 WL 3874302, at 3 (Cal. Ct. App. June 23, 2015) (declining to extend the holding in *Riley* to cover digital cameras).

[118] *Raoult*, 2d Crim. No. B256148, 2015 WL 3874302, at 3.

[119] *Id.*

[120] *Id.* at 1.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] Saphner, *supra* note 1, at 1703–04.

[125] *See* State v. Andrews, 134 A.3d 324 (Md. 2016); State v. Lowell, 364 P.3d 34 (Or. Ct. App. 2015); *In re* J.E., 205 Cal. Rptr. 3d 28 (Cal. Ct. App. 2016).

[126] Saphner, *supra* note 1, at 1706–07.

[127] Peyton, *supra* note 15 (discussing capabilities of everything from connected pacemakers to apple watches).

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

storing in the future is infinite.[128] Failing to establish broad protection for all wearable technology leaves a great deal of unanswered questions about how the courts should treat the wide variety of electronic storage devices.[129] Accordingly, interpreting *Riley* narrowly would be at odds with Pennsylvania's history of affording its citizens more protections against intrusion.[130]

The fourth and final *Edmunds* factor involves an in-depth analysis of the policy considerations associated with searches of high tech wearable electronic devices.[131] In *Commonwealth v. Stem*, the Pennsylvania Superior court echoed the policy concerns advanced in *Riley* in protecting the high tech data stored on cellphones.[132] These policy concerns include the intimacy of information which is stored on cellphones.[133] This includes health information, location data, and information about other aspects of life that Americans do not typically share with the public.[134] The critical concern in *Riley*, which is echoed in *Stem*, involves balancing individual privacy interests with the needs of law enforcement, which include officer safety and preventing the destruction of evidence.[135] In balancing the privacy interests of the cellphone owner and the needs of law enforcement, our nation's Supreme Court and the Pennsylvania Superior Court both explain that the vast capacity of cellphones enables the user to carry around massive amounts of information which they could not possibly carry in their traditional paper format.[136] Further, they explained that much of this information is traditionally kept private.[137]

---

[128] Anjanette H. Raymond & Scott J. Shackleford, *Jury Glasses: Wearable Technology and Its Role in Crowdsourcing Justice*, 17 CARDOZO J. CONFLICT. RESOL. 115, 117 (2015) (suggesting that advances in wearable technology can lead to infinite possibilities in every field from healthcare to Justice).

[129] *See generally* Saphner, *supra* note 1 (discussing the issues that a narrow interpretation poses towards activity trackers).

[130] *See* Thomas M. Hardiman, *New Judicial Federalism and The Pennsylvania Experience: Reflections of the Edmunds Decision*, 47 DUQ. L. REV. 503, 513 (citing the fact that the Pennsylvania constitution was adopted ten years before the ratification of the United States Constitution and that this historical context supports a stronger notion of privacy).

[131] Commonwealth v. Gary, 91 A.3d 102, 127 (Pa. 2014).

[132] Commonwealth v. Stem, 96 A.3d 407, 413 (Pa. Super. 2014).

[133] *Id.*

[134] *Id.*

[135] Riley v. California, 134 S. Ct. 2473, 2477–78 (2014).

[136] *Id.*; *Stem*, 96 A.3d at 413.

[137] *Riley*, 134 S. Ct. at 2847.

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

There are two main justifications in asserting a need to dispense with the warrant requirement.[138] The first justification advanced in *Riley* is the need to prevent the destruction of evidence.[139] The *Riley* court accepted the preservation of evidence as a compelling issue, but held that it does not justify disregarding Fourth Amendment protections.[140] While the government contended that there was a possibility of destroying data stored on cellphones from a remote location, the Court rejected this argument based on the ability of law enforcement to prevent remote wiping easily and effectively by placing the device in faraday bags.[141]

The concerns in the area of search and seizure law are almost identical for wearable technology.[142] Many wearable devices such as smart watches or Fitbits have the same features and abilities as cellphones, albeit in a more limited fashion.[143] Such devices function in almost the same ways as a mass storage device as they are carried on the consumer's person and amass a great deal of private information.[144] Due to their near identical features, wearable devices exhibit the same possibility of remote wiping as with cellphones.[145] But as the Supreme Court explained in *Riley*, these situations are easily dealt with, and the possibility of destruction of evidence is so minimal it does not justify diminishing privacy interests.[146]

The second justification for dispensing with the warrant requirement is the compelling need to protect officers engaging in law enforcement activities.[147] Similar to the first justification, the *Riley* Court held that officer safety is not a compelling enough reason to limit the privacy interests of cellphone users.[148] The Court's reasoning is simple; it is highly unlikely that a cellphone would be used to conceal a

[138] *Id.* at 2483.

[139] *Id.*

[140] *Id.*

[141] *Id.* at 2486 (dismissing concerns of remote data wiping, indicating the possibility that officers could either turn the phone off or place them in "Faraday bags," disabling their abilities).

[142] Saphner, *supra* note 1, at 1710–11.

[143] *Id.* at 1711–16.

[144] *Id.* at 1691–92.

[145] *Id.* (explaining that Smart phones and wearable activity trackers have similar properties and thus present similar concerns).

[146] Riley v. California, 134 S. Ct. 2473, 2486 (2014).

[147] *Id.* at 2478.

[148] *Id.* at 2483.

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu

weapon.[149] Absent some extraordinary circumstance whereby the user is demonstrating a danger to officers or others, the cellphone cannot cause harm.[150] In these rare situations, warrantless searches can be addressed on a case-by-case basis by reviewing the exigency of the situation.[151]

As previously stated, wearable technology exhibits many of the same properties as cellphones and do not readily present danger to officers.[152] Because they have the same properties, the same issues are present for wearable technology.[153] As the Court explained in *Riley*, the concern for officer safety may be satisfied by allowing police to examine the physical exterior of the phone to ensure that it presents no danger to officers as a weapon.[154] In the event a wearable device presents the immediate possibility of harm, the officer may seize and search the device, but absent this, a warrant must be obtained.[155] As a result of the identical concerns, and the identical solutions to these concerns, wearable technology should receive the same treatment as cellphones.

III. CONCLUSION

The incredible rate at which the wearable technology market has grown suggests that it has become a large part of daily life.[156] Similar to cellphone usage, Americans are now wearing cutting edge devices on them everywhere they go, collecting data which assists them in their daily lives.[157] But the average American using wearable technology is unlikely to think about how stored data can be used by law enforcement to incriminate them. Additionally, users of wearable technology probably do not want their personal information disclosed to the public. As a result, the Pennsylvania judiciary must require law enforcement to obtain a warrant before searching wearable technology. The Pennsylvania judiciary has a history of extending Fourth Amendment protections and should continue to do so.

---

[149] *Id.* at 2485 ("Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case.").

[150] *Id.*

[151] *Id.* at 2494.

[152] Saphner, *supra* note 1, at 1710–11.

[153] Riley v. California, 134 S. Ct. 2473, 2485 (2014).

[154] *Id.*

[155] *Riley*, 134 S. Ct. at 2494.

[156] Lamkin, *supra* note 8.

[157] Kosir, *supra* note 2.

Volume XVII – Spring 2017 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2017.197 ● http://tlp.law.pitt.edu