Police and Privacy: A Comparison of Search and Seizure Protection in the United States and Korea

Chante Westmoreland

Introduction

Across nations, borders, and cultures one statement rings true: the law has a difficult time keeping up with changes in technology. Technology evolves at a faster rate than legislative bodies are able to draft or ratify laws.¹ Accordingly, citizens are often left with a confusing web of outdated laws. “Starting in the 1960s, the topic of privacy received steadily increasing attention.”² The discourse has ranged from popular writers to journalists to experts in law, philosophy, psychology, sociology, literature, economics, and countless other fields.³

With technological innovations comes public fear of a general loss of privacy. Accordingly, people are often required to provide personal information in order to complete even the most mundane tasks.⁴ “The emergence of digital communication networks on a global scale; emerging technologies for protecting communications and personal identity; new digital media that support a wide range of social relationships” are just a few of the ways in which people are asked to forfeit personal information in exchange for access to technology that will keep them “in the loop.”⁵ Even more worrisome, is the fact that nearly 90% of the adult population carries around

---

¹ Adam M. Gershowitz, The Post-Riley Search Warrant: Search Protocols and Particularly in Cell Phone Searches 69 VANDERBILT L. REV. 585, 596 (2016) (“Justice Roberts noted that technology had moved fast and that while smart phones were unheard of ten years ago, today a significant majority of Americans have such phones.”).
³ Id.
⁴ United States v. Jones, 565 U.S. ___ 5 (2012) Sotomayor, J. concurring (“More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expecta-tion of privacy in information voluntarily disclosed to third parties; e.g., Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976) (“This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”)).
mini computers in their pockets; these mini computers—cell phones—store all kinds of personal 
data including recent contacts, financial information, recent locations, etc.⁶

Criminal law has been especially slow in keeping pace with advances in technology. Both 
courts and legislatures have been unable to anticipate how police, suspects, and suspects’ 
technology should interact. How far is law enforcement able to invade an individual's privacy in 
order to stop a crime? What happens if you are accused of a crime while carrying a device that has 
the capacity to hold crucial evidence (or alibis)? This paper will explore whether a nation’s attitude 
toward privacy correlates with law enforcement’s ability to “warrantlessly” search and seize 
suspects’ technology.

First, this paper will explore search and seizure jurisprudence in the United States, and the 
confusing way in which it interacts with technology. Specifically, I will focus on how the law 
treats law enforcement’s ability to perform cell phone searches at the point of arrest. Next, I will 
provide a brief comparison between search and seizure jurisprudence in the U.S. and South Korea. 
It is important to note that the law in this field is generally unsettled. The evolution of technology 
keeps courts several steps behind; for example, police have used cell phone location data for years, 
yet the Supreme Court is only now deciding the scope of the use of these data.⁷ Thus, this paper is 
limited to an overview of existing material. This paper is further limited by my own language 
constraints—while primary sources of Korean laws are translated, translated secondary sources 
are difficult to find. In sum, this paper is will explore how these two nations have attempted to

---

⁶ Adrianna P. Agosta, The Law Catching up with the Evolution of Cell Phones: Warrantless Searches of a Cell 
Phone Are Constitutional under the Fourth Amendment, 92 U. DET. MERCY L. REV. 131 (2015) (citing Mobil 
Technology Fact Sheet, Pew research Center (Jan. 2014). http://www.pewinternet.org/fact-sheets/mobile-
technology-fact-sheet/).

states-2/ (“Issue: Whether the warrantless seizure and search of historical cellphone records revealing the location 
and movements of a cellphone user over the course of 127 days is permitted by the Fourth Amendment.”) (last 
protect the privacy and search and seizure protections at a time when technology is rapidly changing.

**What is Privacy?**

For the purposes of this paper, privacy refers to personal information that individuals are either not willing to share with third parties, or intend to share only for limited purposes; however, scholars admit that the exact definition of privacy is ever changing and often difficult to pinpoint. Alan Westin stated that “no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests, and power.” This lack of clarity makes it difficult for policy makers to legislate around this moving target. Notably, some scholars have interpreted this loose definition as a lack of public concern. Jonathan Franzen notes, “[t]he panic about privacy has all the finger pointing and paranoia of a good old American scare, but it’s missing one vital ingredient: a genuinely alarmed public. Americans care about privacy mainly in the abstract.”

When it comes to privacy in the technology age, it becomes nearly impossible for people to engage in their everyday lives without technology. For example, when using Google Maps to get to and from an unfamiliar location, one must input their starting address (i.e. their home address) and the address for the destination. So, in some ways, Franzen is correct, “people routinely give out their personal information and willingly reveal intimate details about their lives on the

---

8 See Robert Gellman, *Does Privacy Law Work*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193 (MIT Press 1997) (“One of the most quoted formulations comes from Louis Brandeis, who consistently referred to privacy as the right to be let alone.”).
9 Solove, supra note 2, at 1; see also Gellman, *supra* note 8, at 193 (“A logical first step in an evaluation of the law as a mechanism for regulating privacy is to define the universe of privacy law.”).
10 Gellman, *supra* note 8, at 194.
12 Id. at 1.
13 See Jones, 565 U.S. at 5 (Sotomayor concurrence).
Accordingly, it is difficult to assess how individuals truly feel about releasing personal information based solely on their actions.\(^\text{15}\)

There are at least two alternatives to Franzen’s assertion. Perhaps people seem willing to release certain types of information in exchange for convenience, or perhaps they release personal information because they do not fully understand the consequences of doing so.\(^\text{16}\) Rather than trying to gauge people’s feelings on privacy based solely on their actions, we should instead question whether absolute secrecy should be a prerequisite for protecting personal information.\(^\text{17}\)

**United States**

**Attitude towards Privacy**

Citizens of democratic nations would like to believe in the constitutional protections the nation purports to give. The United States is a representative democracy. The Constitution—specifically the Bill of Rights—describes the inalienable rights held by citizens or people otherwise within the country.\(^\text{18}\) In addition to the Constitution, other laws, such as statutes and judge made law, describe the rights that citizens hold.\(^\text{19}\) The democratic nature of the United States means that citizens expect a certain level of privacy.\(^\text{20}\) Generally, the government makes an effort to meet these expectations. Examples of this effort to maintain privacy include statutes such as the Fair

\(^{14}\) Solove, *supra* note 2, at 1.

\(^{15}\) Jones, 565 U.S. at 6 (Sotomayor, J. concurring, “I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”).

\(^{16}\) See Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CENTER INT. & TECH., Jan. 14, 2016 (“Most Americans see privacy issues in commercial settings as contingent and context-dependent.”)

\(^{17}\) Jones, 565 U.S. at 6.


\(^{19}\) See *Your Government and You*, *supra* note 18; Volokh, *supra* note 18.

\(^{20}\) See Jones, 565 U.S. at 7 (discussing how society has a fundamental concept of privacy that might be extra- Constitutional).
Credit Reporting Act, Family Education Rights and Privacy Act of 1974, and the Electronic Communications Privacy Act along with constitutional protections like the Fourth Amendment.\textsuperscript{21} Administrative agencies such as the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) oversee various aspects of consumer protections.

**Search and Seizure Jurisprudence**

Just as U.S. citizens value privacy, citizens also believe in the idea of protections for criminal suspects and defendants. In the U.S. there are constitutional protections for those suspected of committing a crime. Specifically, I will focus on the Fourth Amendment, which protects against unwarranted search and seizure,\textsuperscript{22} and the Fifth Amendment, which protects against self-incrimination.\textsuperscript{23} “Search and seizure” is a term of art, but actually describes two different steps in the treatment of criminal suspects.\textsuperscript{24} This paper will focus predominantly on the “search” portion.

The right of people to be free from warrantless search and seizure lies in the Fourth Amendment. The Fourth Amendment reads:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.\textsuperscript{25}

The Fourth Amendment is based in property law and common-law trespass.\textsuperscript{26} Recently, the Court has expanded the doctrine, noting that “the Fourth Amendment protects people, not


\textsuperscript{22} U.S. CONST. AMEND. IV

\textsuperscript{23} U.S. CONST. AMEND. V

\textsuperscript{24} Search will be defined *infra*; however, there are different types of seizures. Typically, so long as a reasonable person would have felt free to disregard the police and go about his business, there was no seizure. See slide from Weisselberg Crim Pro Fall 2016 titled “Takeaway—What is Seizure,” slide number 86, Sept. 23, 2016.

\textsuperscript{25} U.S. CONST. AMEND. IV

\textsuperscript{26} Jones, 565 U.S. at 4 (“our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.”).
places.”\textsuperscript{27} The analysis has broadened from a simple trespass determination to an analysis of whether a “government officer [has] violate[d] a person’s ‘reasonable expectation of privacy.’”\textsuperscript{28} Reasonable expectation of privacy was first discussed in \textit{Katz v. United States}.\textsuperscript{29} “Under \textit{Katz v. United States}, police activity constitutes a search only if it implicates reasonable expectations of privacy. This is a two-prong test, requiring first that the person manifest a subjective expectation of privacy, and second, that the expectation of privacy “be one that society is prepared to recognize as ‘reasonable.’”\textsuperscript{30} As it stands, courts use both the trespass and reasonable expectation of privacy test to determine whether a Fourth Amendment violation has occurred.\textsuperscript{31}

There are several exceptions to the right to be free of unwarranted search and seizure. The first exception is clear on the face of the amendment: if law enforcement attains a warrant they can search things that are otherwise protected.\textsuperscript{32} The warrant must be supported by probable cause and must be authorized by a judge.\textsuperscript{33} The other exceptions to the warrant requirement include: “search of the person incident to arrest; search of the area incident to arrest; stop-and-frisks; searches conducted during hot pursuit of a fleeing suspect; searches prompted by fear for the health or safety of one or more individuals; searches conducted to prevent the impending destruction of evidence; searches of vehicles; searches of containers in vehicles; consent searches; and an impressive

\begin{itemize}
\item \textsuperscript{27} Jones, 565 U.S. at 5.
\item \textsuperscript{28} Id.
\item \textsuperscript{29} Katz v. United States, 389 U.S. 347 (1967); see also Jones, 565 U.S. at 7 (quoting Minnesota v. Carter, 525 U. S. 83, 88 (1998), “[The] very definition of ‘reasonable expectation of privacy’ which we have said to be an expectation ‘that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.’”).
\item \textsuperscript{30} Burke, Consent Searches and Fourth Amendment Reasonableness, at 517-18 (In applying the Katz standard, the Court has held that when people make otherwise private information available publicly, governmental inspection of that information does not implicate reasonable expectations of privacy and therefore does not constitute a search.”).
\item \textsuperscript{31} Jones, 565 U.S. at 8. (“[T]he Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”).
\item \textsuperscript{32} See e.g. Payton v. New York, 445 U.S. 573 (1980).
\item \textsuperscript{33} See e.g. Katz, 389 U.S. 347 (1967).
\end{itemize}
variety of inspection, regulatory, and other “special needs” searches.” I will focus on exigent circumstances, search incident to arrest, and the third-party and consent exceptions as they are the most pertinent to this privacy analysis.

Turning first to the exigent circumstances exception, this exception allows officers to conduct a warrantless, consentless search “when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.” This allows law enforcement, for example, to enter homes to render emergency services, or to conduct a search without a warrant to avoid “imminent destruction of evidence.” In order for the search to be valid, the officer must have probable cause in addition to exigency.

In his pre-Riley piece, Searching Cell Phones After Arrest: Exceptions to the Warrant Requirement, Clifford Fishman explores the application of the exigent circumstances doctrine to cell phones. Fishman lists several circumstances where law enforcement could have access to a suspect’s cell phone such as when the suspect is using the phone in the officer’s presence or where officers have probable cause to believe that the suspect used the phone in the commission of the arrest offense. Fishman states:

Courts generally agree that when police are executing a search warrant in a home or office and a landline phone on that premises rings, the officers may answer the phone even if the warrant does not explicitly authorize them to do so. Answering an arrestee’s cell phone in the immediate aftermath of the arrest where probable cause exists that the defendant

35 There could of course be extensive discussion concerning all of these exceptions; however, I am focusing specifically on the invasion of privacy suspects experience at the moment of arrest or detention.
36 Fishman, supra note 34, at 1002 (quoting Missouri v. McNeely, 133 S. Ct. 1552, 1558 (2013)) (note that Fishman’s piece was written prior to the Court’s decision in Riley v. California; however, as Erica Danielson points out, searches of cell phones in exigent circumstances are still likely allowed even after Riley).
37 Fishman, supra note 34, at 1003.
38 Id.
39 Id. at 1004-05.
used his phone in committing the crime, establishes an even stronger justification for answering it or for reading or responding to incoming text messages.\textsuperscript{40}

Thus, when it comes to answering phones, courts tend to allow the exigent circumstances themselves justify the officers’ behavior.\textsuperscript{41} Relatedly, Fishman states that certain circumstances justify “an officer [answering] a suspect’s cell phone, even if there is no apparent connection between the call and the arrest crime.”\textsuperscript{42}

Fishman discusses the district court case, \textit{United States v. Davis},\textsuperscript{43} in which an officer answered a suspects’ phone, and the court held “that both answering the phone and the subsequent search of it to discover the origin of the call were unlawful because there was no reason to believe the call or the phone would produce evidence of the reckless driving charge.”\textsuperscript{44} Fishman purports that while this is sufficient rationale for a simple traffic violation, “it is questionable whether it applies when a motorist attempts to outrun police pursuit [which likely indicates that] something more serious than a mere traffic violation is afoot.”\textsuperscript{45} However, Fishman’s suggestion seemingly opens the flood gates in a time where cell phones are not simply phones, but mini computers. Does Fishman’s suggestion extend to suspects’ internet search history, text messages, and emails under similar circumstances?

Fishman’s views show how some individuals seem to value crime-control over privacy. The \textit{Riley} decision (discussed further below) seems to address the counter-argument. The case

\begin{thebibliography}{99}
\bibitem{40} Fishman, \textit{supra} note 34, at 1004 n.38.
\bibitem{42} Fishman, \textit{supra} note 34, at 1006.
\bibitem{43} \textit{United States v. Davis}, 787 F. Supp. 2d 1165 (D. Or. 2011) (The officer watched the driver of a vehicle commit several traffic offenses (i.e. speeding and running lights). He pursued the driver; the driver attempted to flee, but crashed his vehicle and fled on foot. The officer found a cell phone in the abandoned vehicle. The phone rang repeatedly as the officer transported it to the police station, and eventually the officer answered the phone); see also \textit{State v. Carroll}, 778 N.W.2d 1, 9 (Wis. 2010) (holding that a search was justified under the exigent circumstances exception where the suspect dropped his cell phone as he was fleeing police, police looked at the screensaver, which was a picture of the suspect smoking marijuana, and then answered an incoming call believing that it was likely evidence of a drug-related crime).
\bibitem{44} Fishman, \textit{supra} note 34, at 1006 (citing 787 F. Supp. 2d at 1171, 1174).
\bibitem{45} \textit{Id.} (Fishman suggests that under the circumstances, answering the phone or checking the call log is reasonable).
\end{thebibliography}
“provides specific examples of exigent circumstances which may apply to a cell phone search, such as “a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child’s location on his cell phone.” Because these are quite clearly extreme examples, Erica Danielson suggests that we can read Riley as stating that only in rare cases will exigent circumstances justify a warrantless search of a cell phone. Therefore, Riley seems to indicate that courts must balance crime-control and privacy.

Searches Incident to Arrest

Search incident to arrest is a second exception to the warrant requirement. The Court created the search incident to arrest exception in Chimel v. California. In Chimel three officers went to the petitioner’s home with an arrest warrant; immediately after arresting the petitioner, the officers thoroughly searched the arrestee’s house. The Court found that it was reasonable for officers to search the individual being arrested and the area around the individual to ensure the officer’s safety.

The search incident to arrest exception is particularly tricky to apply in the age of technology because it is difficult to define the scope of a search where electronics may contain massive amounts of data. The Supreme Court in Riley v. California held that “the search incident to arrest exception does not apply to cell phone searches.” In Riley, the Court distinguished smartphone searches from searches of other containers at issue in previous search incident to arrest

---

47 Id. at 986.
49 Id.
50 Id.
51 See Gershowitz Post Riley, supra note 1, at 596 (discussed supra (“Justice Roberts noted that technology had moved fast and that while smart phones were unheard of ten years ago, today a significant majority of Americans have such phones.”)).
52 Danielson, supra note 46, at 986.
cases. As previously mentioned, cell phones can hold “millions of pages of text, provide a history of internet usage, and access even more data in the cloud.” Further, unlike other containers, cell phones would not “contain” a weapon and therefore do not pose the same type of threat to officers. Thus, given the potential for such a massive privacy invasion, and the lack of immediate harm to officers, the Court limited searches incident to arrest in regard to cell phones.

Public and media reaction to the Riley decision was “nearly universally positive.” However, some critics have argued that Riley does not go far enough—the language in Riley does not properly ensure that judges would require narrowly-tailored cell phone search warrants. So while Riley requires officers to have a warrant prior to searching a cell phone, once they have a warrant, they could seemingly search as thoroughly as they want. However, arguably, the Court rightfully left this decision to legislators.

Third-Party Doctrine

The third-party doctrine is another exception to the warrant requirement. Under certain circumstances, courts have considered whether an individual actually has an expectation of privacy in a device or certain information to which a third party has access. For example, the court in United States v. Warshak, held that law enforcement violated the defendant’s Fourth Amendment rights by compelling the Internet Service Provider to turn over his emails without a warrant. The

---

53 Gershowitz Post Riley, supra note 1, at 596.
54 Id.
55 Gershowitz Post Riley, supra note 1, at 596.
56 Gershowitz Post Riley, supra note 1, at 596; see also Agosta, supra note 6, at 133 (stating that, “56% of American adults have a smart phone, 31% have private medical information on their cell phones, and 29% use online banking on their cell phones.”).
57 Gershowitz Post Riley, supra note 1, at 588.
58 Gershowitz Post Riley, supra note 1, at 588.
59 See generally Gershowitz Post Riley, supra note 1; but see Law Enforcement Cyber Center: Digital Search Warrants, Digital Search Warrants (Last visited Dec. 12, 2017) http://www.iacpcybercenter.org/prosecutors/digital-search-warrants/ (explaining how the Fourth Amendment particularity requirement should act as parameters for prosecutors seeking a warrant to search electronic evidence).
60 See generally, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
court reasoned that like a letter through a post office, “[e]mails must pass through an ISP’s servers to reach their intended recipient”; accordingly, where police are not allowed to storm a post office, they must also acquire a warrant before obtaining emails from an ISP.61 “As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.”62

Scholars wonder whether society is becoming numb to the idea of privacy because of the amount of information they share.63 As it stands, society recognizes the idea that police should not have access to one’s cell phone without a warrant or consent from the owner.64 This assumption forms the basis of the previously discussed reasonable expectation of privacy test. However, considering the amount of information consumers voluntarily provide third-parties through apps and other web based services, scholars question whether this societal expectation is eroding.65

---

61 Warshak, 631 F.3d at 286 (emphasis added).
62 Warshak, 631 F.3d at 286; see also Arkansas v. Bates, CASE NO. CR-2016-370-2, (Ark. Cir.) (in which Arkansas prosecutors subpoenaed Amazon seeking to obtain recordings that occurred on the Amazon Echo belonging to a murder suspect).
65 See Smith v. Maryland, 442 U.S. 735, 737 (1979) (discussing third party doctrine and pen register); United States v. Miller, 425 U.S. 435 (1976) (holding that bank records are not protected by the Fourth Amendment warrant requirements); see also Coldewy, supra note 60 (excerpting the Amicus Brief filed by the Center for Democracy and Technology in Carpenter v. United States “The changes resulting from digital technology — with Americans storing vast quantities of personal information with third parties, and third parties creating databases of personal information not previously available — make it eminently reasonable to conclude that Americans have a legitimate expectation of privacy with respect to much of this information. The Court also should recognize that whether the individual provided personal information “voluntarily” should not be accorded any weight in the reasonable-expectation-of-privacy inquiry, because there is no correlation between the voluntary provision of information to a third party and legitimate expectations of privacy. For example, individuals voluntarily transfer the contents of emails, photographs, and sensitive personal documents to third-party service providers who store this information. Yet individuals believe, correctly, that absent very unusual circumstances, this information will be private: it will not be viewed by anyone other than themselves or persons who they authorize.”).
I would argue that consumers retain an expectation of privacy even where they share certain personal information with third parties—it is simply a narrower expectation.\textsuperscript{66} Consumers voluntarily provide third-parties access to their phones in exchange for convenience and functionality. Exposure to a third-party company does not necessarily mean a complete diminution of the desire for privacy. There is a recognizable difference in the way a company and law enforcement use the information. In the exchange between consumers and companies, individuals share information with the expectation that it will be used for a limited, mutually helpful purpose.\textsuperscript{67} Meanwhile, in the exchange between suspects and police, individuals share information for different reasons such as to appear cooperative or out of fear.\textsuperscript{68} Thus, to assume that police should have access to the same information as companies simply because a consumer shared the information goes against the spirit of Fourth Amendment protections.

\textit{Consent Searches}

The power dynamic between police and suspects also causes courts to scrutinize searches performed based on consent.\textsuperscript{69} While law enforcement may perform a warrantless search with a suspects’ consent, critics of this exception question the circumstances under which an individual would feel free to deny an officer’s search request.\textsuperscript{70} Courts have held searches invalid where consent was not freely given, but was given as a result of coercion.\textsuperscript{71}

\textsuperscript{66} Jones, 565 U.S. at 5 (“Perhaps, as JUSTICE ALITO notes, some people may find the “tradeoff” of privacy for convenience “worthwhile,” or come to accept this “diminution of privacy” as “inevitable,” post, at 10, and perhaps not.”).
\textsuperscript{67} Id.
\textsuperscript{69} See generally Schneckloth v. Bustamonte, 412 U.S. 218 (1973) (discussing the totality of the circumstances test for determining whether voluntary consent was actually given).
\textsuperscript{70} Florida v. Jimeno, 500 U.S. 248 (1991) (discussing the scope of consent and using an objective standard to evaluate the reasonableness of officers believing that the person consenting actually had the authority to consent).
\textsuperscript{71} See Bustamonte, 412 U.S. at 220 (explaining that if consent is obtained through coercion—an express promise or an express threat—it does not constitute voluntary consent).
In the case of developing cell phone technology, questions of consent become even more complicated. Most smart phones today allow users to lock the phone when it is not in use. Unlocking the phone may require a passcode, a fingerprint scan, or even facial recognition. Technologists argue over the level of protection provided by each option—especially when it comes to keeping law enforcement out. For example, if a police officer seizes a suspect’s phone and asks for permission to look through their phone, in which case has the suspect given adequate consent: If the suspect answers, “yes”?: if the suspect gives the officer the passcode?: if the suspect enters the passcode?: if the suspect scans their fingerprint?: if the suspect faces the camera for a facial scan?

Passcodes appear to be the safest way to go. Individuals are likely protected from giving law enforcement their passcodes under the Fifth Amendment right against self-incrimination. The Fifth Amendment states, “No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury.” In other words, the Fifth Amendment protects an individual from self-incrimination. Law enforcement may not compel testimony from a suspect that is self-incriminating. “Evidence is testimonial (and thus protected by the Fifth Amendment) if it causes an individual ‘to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts

75 See generally Adam M. Gershowitz, Password Protected - Can a Password Save Your Cell Phone from a Search Incident to Arrest, 96 IOWA L. REV. 1125 (2011).
76 U.S. CONST. AMEND. IV
77 Gershowitz Password Protected, supra note 75, at 1170.
and beliefs with the Government.” The Supreme Court has stated that most statements “convey information or assert facts”; therefore, “[t]he vast majority of verbal statements thus will be testimonial.” The Fifth Amendment would likely protect one from being coerced into providing a cell phone password to a police officer because it would require an individual to share the contents of their mind.

While verbal testimony is protected by the Fifth Amendment, physical traits—such as the sound of your voice, your appearance, or your fingerprints—remain outside the scope of the amendment’s protection. The court in Commonwealth of Virginia v. Baust held that there was no violation of a suspect’s Fifth Amendment rights where police officers forced a suspect to provide fingerprints. Similarly, the Court in Schmerber v. California held that there was no Fifth Amendment violation where a suspect was required to provide a blood sample to police. Accordingly, law enforcement might be able to use biometric scanning technology like fingerprint scanners or facial recognition software to gain access the suspects’ cell phone.

---

78 Id.
79 Id.
81 Gershowitz Password Protected, supra note 75, at 1170 (“Asking a suspected drunk driver if he has been drinking calls for a testimonial response, whereas taking a sample of his blood only represents a physical trait that is nontestimonial.”).
83 Schmerber v. California, 384 U.S. 757 (1966) (The suspect was accused of driving under the influence and while he was protected from verbally admitting guilt, he was required to provide police with an incriminating blood sample).
84 Gershowitz Password Protected, supra note 75, at 1170; see also Pennsylvania v. Muniz, 496 U.S. 582, 594-95 (1990); Schmerber v. California, 384 U.S. 757, 761 (1966); but see Brian Fung, What Happens if a Cop Forces You to Unlock Your iPhone X With Your Face?, THE WASHINGTON POST, Sept. 13, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/09/13/what-happens-if-a-cop-forces-you-to-unlock-your-iphone-x-with-your-face/?utm_term=.e1f983e1fe64 (“Americans enjoy one additional layer of legal protection. Even if a police officer uses your biometric information to unlock a phone, he or she must still obtain a search warrant to search the phone. The warrantless searching of cellphones was ruled unconstitutional by the Supreme Court in Riley v. California in 2014.”); see also Jerry Hildenbrand, Your Privacy, Fingerprints and the Fifth Amendment, ANDROIDCENTRAL, Feb. 1, 2017, https://www.androidcentral.com/your-privacy-your-fingerprints-and-fifth-amendment.
Korea

According to a study by DLA Piper, the United States and South Korea tend to have “heavy” (i.e. more protective) privacy laws.\(^8^5\) Interestingly, “[b]eyond the United States, the vast majority of nations protect privacy in their constitutions. For example. . .South Korea announces that ‘the privacy of no citizen shall be infringed.’”\(^8^6\) Moreover, “[w]hen privacy is not directly mentioned in constitutions, the courts of many countries have recognized implicit constitutional rights to privacy, such as Canada, France, Germany, Japan, and India.”\(^8^7\) Because South Korea and the U.S. have strong privacy protections and are advanced in their developments of new technologies, but have different origins, I thought it would be interesting to compare the two.

Kipyo Kim stated, “[t]o understand Korean law, it is essential to have knowledge about Korean legal history.”\(^8^8\) Kim stressed that foreigners may generally find the Korean legal system difficult to understand because “it has its own unique and traditional legal history and system different from those of Western and other countries.”\(^8^9\) In 1945, Korea gained its independence from Japan.\(^9^0\) Despite its independence, the country’s traditional authoritarian regime continued until 1987.\(^9^1\) In 1987, the authoritarian regime in Korea fell and “opened a road toward democracy.”\(^9^2\) The 1987 Constitution significantly changed the way the country viewed criminal

\(^8^6\) Solove, supra note 2, at 3.
\(^8^7\) Solove, supra note 2, at 3.
\(^8^8\) Kipyo Kim, Overview, in INTRODUCTION TO KOREAN LAW 1 (Korean Legislation Research Institute 2013).
\(^8^9\) Id. at 2.
\(^9^0\) Id. at 2; see also Andrea M. Savada, et. al., SOUTH KOREA, A COUNTRY STUDY 200 (Library of Congress, Federal Research Division 1992) https://lccn.loc.gov/91039109.
procedure and included explicit references to the administration of due process.\textsuperscript{93} “Separation of powers came from the political process as well as from the formal structure of government embodied in the Constitution.”\textsuperscript{94}

In addition to constitutionalizing criminal procedure, Korea established a Constitutional Court “as a watchtower to monitor unconstitutional laws and police practices” and to protect fundamental rights.\textsuperscript{95} According to John Leitner, “‘fundamental rights’ refers to the constitutional rights that are possessed by Korean citizens under the text and provisions of the Constitution and can be enforced through constitutional adjudication.”\textsuperscript{96} Notably, the Constitutional Court “is consistently rated one of the most effective institutions in Korea by the public . . . it [has] received the highest ratings of any government body . . . in terms of public influence and trust.”\textsuperscript{97}

\textbf{Attitude towards Privacy}

Korea’s authoritarian history—complete with the tight restrictions on expression and heavy government surveillance—makes citizens especially sensitive to government-privacy encroachments.\textsuperscript{98} Korean teachers are expected to teach junior and high school students from an “IT Ethics” textbook “whose chapters include ‘Healthy Mobile Phone Culture,’ and ‘Protecting

\begin{itemize}
\item \textsuperscript{93} \textit{Id.} at 377-78.
\item \textsuperscript{94} \textit{Id.} at 378.
\item \textsuperscript{95} \textit{Id.} at 379; see also Tom Ginsburg, \textit{The Constitutional Court and the Judicialization of Korean Politics}, in \textit{NEW COURTS IN ASIA} 145, 146 (Andrew Harding & Penelope Nicholson ed. 2010) (“The Court consists of nine justices who serve six-year renewable terms, now staggered so that justices are appointed in sets. Six votes are required to declare a law unconstitutional, to dissolve a political party, to accept a constitutional complaint or to overrule a previous precedent of the Constitutional Court. Three justices each are appointed by the Supreme Court, the National Assembly and the President.”).
\end{itemize}
As previously mentioned, the Korean Constitution includes explicit protection for liberty and secrecy with respect to one's private life, freedom of residence, freedom of expression, secrecy of communications, authority regarding an individual's personal information. Other statutes that indicate Korea’s strong privacy protection include: The Communication Secrecy Protection Act of 1993, the Personal Information Protection Act (PIPA), the Criminal Code, the Act on the Promotion of IT Network Use and Information Protection (Network Act), and the Use and Protection of Location Information Act. Similar to the U.S., Korean has certain administrative agencies that help oversee consumer protection and privacy rights, including the Korea Communications Commission.

Last year, South Korea was ranked “the world’s most innovative economy . . . based on indicators such as research and development capability, tech density and patent activity.” The “quarter-century old” democracy has proven itself a “leader in data privacy innovation” by coming up with a set of laws to fairly quickly address arising privacy issues. Perhaps the country’s newer governmental structure allows it to operate more efficiently and address consumer privacy concerns at a more rapid pace?

---

100 Jin Hwan Kim, et. al., Privacy in South Korea: Overview, THOMSON REUTERS: PRACTICAL LAW, Jul. 1, 2015 https://content.next.westlaw.com/Document/1569c17ae4f5211e498db8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default (explaining that the latter refers to the right to decide the timing, scope, and identity of recipients with respect to the sharing and use of personal information).
of their privacy laws. Nevertheless, South Korea has seemingly found a way to be interconnected while still acknowledging their citizens need for privacy.\footnote{Greenleaf, \textit{supra} note 103, at 157.}

**Attitude towards Search and Seizure**

Korea’s Criminal Procedure Act provides protections for defendants and suspects. Article 201 of the CPC requires a judicial warrant for search, seizure, or inspection.\footnote{Cho \textit{Unfinished, supra} note 92, at 385 (citing CPC Art. 201).} A criminal investigation can be triggered by: “arrest of a flagrant offender, inquest of a person who died unnaturally, complaint by a victim of crime, accusation by any person who believes that an offense has been committed, and surrender of a suspect to the police.”\footnote{Kwoncheol Lee, \textit{Criminal Law and Procedure, in INTRODUCTION TO KOREAN LAW} 155, 171 (Korean Legislation Research Institute 2013) (citing the Criminal Procedure Act, Art. 212, 222, 223, 234, and 240).} Accordingly, the Code of Criminal Procedure delineates two types of investigations: those based on voluntariness and those based on “compulsory measures.”\footnote{Lee, \textit{supra} note 107, at 171.} The code presumes that most investigations will be carried out with a willing suspect (i.e. voluntary investigation); therefore, the code presumes that the suspect will not be placed immediately under arrest.\footnote{Id. at 172.}

Exceptions to the warrant requirement include search incident to arrest with a warrant; emergency arrest; arrest of flagrant offenders; detention on warrant; emergency search and seizure; and inspection on the spot of committed crimes.\footnote{Cho \textit{Unfinished, supra} note 92, at 385 (quoting articles 215; 216 (1)-(3)).} However, because most investigations would likely require some compulsory measures, the code mandates that any detention, search, or seizure be used sparingly and only to the least extent necessary.\footnote{Lee, \textit{supra} note 107, at 172.} And while law enforcement is typically required to obtain a warrant before any of these things, interestingly, “in an emergency, the
authorities may carry out the measures first and request the issuance of the warrant ex post facto.”

Public pressure led the Korean legislature to adopt an exclusionary rule in 2007. In the U.S., physical evidence that was obtained in violation of a suspects’ constitutional rights may be excluded from trial. For many years, this was not the case in Korea; Korean courts categorically refused to exclude wrongfully obtained physical evidence stating, “[e]ven though the procedure of seizure was illegal, the value as evidence does not change because the procedure did not affect the quality and shape of the substance itself.” Finally, in November 2007 (just before the eventual revision of the CPC), the Korean Supreme Court decided to exclude illegally obtained physical evidence. While the Korean Supreme Court adopted the rationale of the U.S Supreme Court’s decision in Mapp, the exclusionary rule in Korea remains merely discretionary.

Conclusion

While Korea seems better at keeping consumer privacy laws in step with technological advances, limits on law enforcement seem to still be developing. Practically speaking, part of the problem is getting policy to translate into practice where “law enforcement [continues to] emphasize the superiority of crime control over due process” and privacy. On the outside the nation appears to be making strides, but internally citizens are still questioning how to balance

---

112 Id.
113 Kuk Cho, The Exclusion of Illegally Obtained Confessions, Electronic Communications, 13 J. KOR. L. 175, 185 (2014) (“In 1993 the CPPA was legislated to exclude communications obtained by illegal wiretapping. . . In 2007, the CPC was revised to stipulate a general provision of the exclusion of illegally obtained evidence.”).
115 Cho Unfinished, supra note 92, at 393 (“Unless the illegally-obtained evidence is excluded, the constitutional requirement for the search-and-seizure warrant is left without strong teeth. There are no other effective remedies for illegal police misconduct in Korea. Criminal or civil liability and internal discipline have not shown promise to deter the police misconduct in Korea, like in the United States.”).
117 Id. at 213 (Notably, in 2010, the Korean Supreme Court held that the “secret recording of mobile phone communication by police informant, who was imprisoned at that time and given the phone by the police, is illegal.”).
118 Cho Exclusion, supra note 113, at 217.
these concerns. Similarly, American law surrounding law enforcement’s ability to warrantlessly search technology is still evolving. While both nations have a strong history of preserving citizens’ privacy, the question remains how far each government will be willing to go to protect something with such a fluid definition in the face of rapid technological changes. Hopefully, tradition and societal pressures will help keep the balance between the need to administer justice and the need to retain society’s rights to privacy.

---

119 Jung-a, supra note 102 (“[T]here is growing fear that the country is falling behind. . . because of red tape and a risk-averse culture.”).