Project 2: Law Enforcement Access to Smart Phone Data

Justin Wasser

University of Maryland Global Campus

INFA 660 9040: The Law, Regulation and Ethics of Information Assurance

Professor Asllani

3/19/2024

Contents

Introduction

This project aims to analyze the cases of United States v. Keck, and Riley v. California, focusing on the application of the Fourth Amendment to the searching of an individual's smartphone or similar device (UMGC, n.d.). Moreover, the question of "Under what conditions or circumstances are law enforcement officers allowed to search an individual's personal devices?" (UMGC, n.d.), and "Under what conditions are law enforcement agencies allowed to remotely access an individual's personal devices?" (UMGC, n.d.) is central to this paper and therefore must be answered (UMGC, n.d.). To that point, answering these questions requires breaking down the concepts they contain which leads to the legal questions, "Does the Fourth Amendment to the U.S. Constitution provide protection against searches of an individual's personal devices, e.g. smart phones or tablets?" (UMGC, n.d.), "Do legal precedents allowing warrantless physical searches of smart phones extend to allowing the use of forensic technologies to obtain local and/or remote access to data stored on the device?" (UMGC, n.d.), and "What technologies are available to law enforcement agencies for use in conducting local and/or remote search and recovery of data from personal devices such as smart phones, tablet computers, etc.?" (UMGC, n.d.).

The crux of the issues brought up by these legal and technical issues is that the Fourth Amendment protects individuals (including their possessions) from "unreasonable searches and seizures" (Constitution Annotated, n.d.). Therefore, the question of note is what the legal definition of unreasonable is in varying situations (Cornell Law School, n.d.; *Riley v. California*, 2014). Put another way, the government needs a legal justification to search people's property (devices) and this can be accomplished in a variety of ways including via obtaining a search warrant, obtaining consent from the individual, as a normal procedure during an arrest i.e.

"incident to arrest" (*Riley v. California*, 2014), if the "automobile exception" (*United States v. Keck*, 2021) applies, or if "Exigent circumstances" (*Exigent Circumstances and Warrants*, n.d.) are present; but different justifications have different scope related limitations that must be examined (Cornell Law School, n.d.; *Exigent Circumstances and Warrants*, n.d.; *Riley v. California*, 2014; *United States v. Keck*, 2021; Wallentine, 2021).

Analysis

The issues brought up in this paper (when are officers allowed to search an individual's device & when are officers allowed to remotely access an individual's device) are important because they illustrate the protections afforded by the 4th amendment concerning personal devices (smartphones, tablets, computers, etc.) in different situations (Constitution Annotated, n.d.; Cornell Law School, n.d.; UMGC, n.d.). This is important because it delineates where 4th Amendment protections end concerning searching a person's device in various situations (Constitution Annotated, n.d.; Cornell Law School, n.d.). Moreover, understanding the individual privacy rights afforded by the 4th amendment of the Constitution helps to ensure that they are not unlawfully infringed upon by the government (Constitution Annotated, n.d.; Cornell Law School, n.d.). For example, the 4th Amendment wouldn't provide nearly as much privacy protections if individuals' devices could be searched any time they were arrested. This is why the "reasonableness" (*Riley v. California*, 2014) of a search is a key consideration when considering whether a search violates an individual's 4th Amendment rights (Cornell Law School, n.d.; *Riley v. California*, 2014; *United States v. Keck*, 2021).

Without these considerations, individuals would not gain nearly as much protection from the 4th Amendment as searches of personal devices would occur regularly, and therefore individuals would not be able to effectively safeguard their privacy (Cornell Law School, n.d.).

Moreover, individual privacy in this context refers to the preservation of the CIA "confidentiality, integrity and availability" (Hashemi-Pour & Chai, 2023) of the information stored on individuals' phones (and similar devices); which would be irreparably harmed as said data could be accessed seemingly at any time (by police) and disclosed, altered or taken without a reasonable legal justification (Cornell Law School, n.d.; Hashemi-Pour & Chai, 2023; *Riley v. California*, 2014).

Furthermore, the research questions posed are important because smartphones (and similar devices) hold so much personal data and are nearly always attached to their users that ensuring said devices receive appropriate 4th Amendment protections, i.e. protection from "unreasonable searches and seizures" (Constitution Annotated, n.d.) is paramount to individuals' maintaining their privacy (preserving the CIA of their personal data) in the twenty-first century (Hashemi-Pour & Chai, 2023; *Riley v. California*, 2014). Moreover, if proper protections were not given to these devices, then warrantless searches (on-premises or remote) of said devices would allow the state to learn almost everything there is to know about an individual (severely undermining personal privacy) anytime an individual was arrested (fairly or otherwise) (Cornell Law School, n.d.; Fakhoury & Kayyali, 2014; *Riley v. California*, 2014; UMGC, n.d.). However, at the same time, law enforcement needs to be able to collect evidence from individuals suspected of committing crimes and there are technologies available to law enforcement to enable such searches (on-premises or remote) when legal authority to do so has been secured (Cellebrite, n.d.-c; Magnet Forensics, n.d.).

Does the Fourth Amendment to the U.S. Constitution provide protection against searches of an individual's personal devices, e.g. smartphones or tablets?

So long as the search/seizure is "unreasonable" (Constitution Annotated, n.d.) the Fourth Amendment grants individuals protection from "government searches and seizures, and this protection extends to your computer and portable devices" (Fakhoury & Kayyali, 2014). Moreover, smartphones were given heightened protection from warrantless searches because of the unprecedented amount of personal data they stored about their owner (*Riley v. California*, 2014). However, searches of devices may be deemed reasonable if any of the following situations apply: if a search warrant is obtained, consent is given by the individual, or if "Exigent circumstances" (*Exigent Circumstances and Warrants*, n.d.) are present (Cornell Law School, n.d.; *Exigent Circumstances and Warrants*, n.d.; *Riley v. California*, 2014; Wallentine, 2021).

However, the condition of note for the cases of United States v. Keck and Riley v. California is "warrantless searches" (*Riley v. California*, 2014) performed during an arrest (*Riley v. California*, 2014; *United States v. Keck*, 2021). Moreover, the main considerations regarding the constitutionality of this type of search are whether an officer may be harmed or evidence may be destroyed if a search was not conducted immediately (*Riley v. California*, 2014). To that point, neither of these considerations was judged to be generally applicable concerning digital information on a personal device, and therefore warrantless searches of said devices were deemed to violate the Fourth Amendment (Fakhoury & Kayyali, 2014; *Riley v. California*, 2014). However, warrantless searches of personal devices are permissible when the scope is limited to the physical aspects of a given device as those attributes may reasonably constitute a threat to an officer (*Riley v. California*, 2014).

If the Fourth Amendment did not afford protection to personal devices then the individuals' ability to preserve the privacy of their information would be greatly diminished (*Riley v. California*, 2014). The reason is, that the security of the data stored on a device i.e.

"confidentiality, integrity and availability" (Hashemi-Pour & Chai, 2023) could not be assured, as even minor law infraction may lead to one's entire private data being reviewed/copied, accidentally altered, or accidentally deleted by police (Hashemi-Pour & Chai, 2023; *Riley v. California*, 2014).

Do legal precedents allowing warrantless physical searches of smartphones extend to allowing the use of forensic technologies to obtain local and/or remote access to data stored on the device?

Legal precedents allowing warrantless physical searches of smartphones do not extend to allowing the use of forensic technologies to obtain local and/or remote access to data stored on the device (Fakhoury & Kayyali, 2014; *Riley v. California*, 2014). While searches "incident to arrest" (*Riley v. California*, 2014) may deem it appropriate to seize an individual's device, "the Supreme Court held that a warrant is required to search a cellphone incident to an arrest" (Landau, 2020). While some exigent circumstances may call for the immediate search of a person's device, those circumstances are the exception, not the rule (*Riley v. California*, 2014). A more standard situation is found in the case of United States v. Keck, where officers arrested the suspect (Keck) and instructed Keck to hand over any electronics without coercing him to do so (*United States v. Keck*, 2021). The officers merely secured the suspect's electronic devices but did not search them until they secured a search warrant to do so (*United States v. Keck*, 2021).

This case illustrates that the use of forensic technologies to obtain local/remote access to data stored on a device is not generally allowed as part of warrantless searches (UMGC, n.d.; *United States v. Keck*, 2021). Moreover, accessing data from personal devices as part of a warrantless search implies that there will be some reviewing of the data once it is accessed, which is deemed to violate the Fourth Amendment and is therefore unconstitutional (Fakhoury &

Kayyali, 2014; *Riley v. California*, 2014). Lastly, law enforcement can get around this limitation if an individual consents (sometimes occurring under questionable circumstances) to having their device searched, in which case "mobile device forensic tools (MDFTs)" (Koepke et al., 2020) are used (Koepke et al., 2020; Landau, 2020).

If the Fourth Amendment did not afford protection to personal devices from warrantless searches using various forensic technologies, then the individuals' ability to preserve the privacy of their information would be greatly diminished (*Riley v. California*, 2014). The reason is, that there are often no restrictions placed on the scope of the data extracted by MDFTs, and therefore all an individual's data is laid bare (Koepke et al., 2020). Therefore, the security of the data stored on a device i.e. "confidentiality, integrity and availability" (Hashemi-Pour & Chai, 2023) could not be reasonably assured if warrantless searches using various forensic technologies were permissible, as nearly any law infraction may lead to one's complete private data being disclosed, accidentally altered, and/or accidentally deleted by police (Hashemi-Pour & Chai, 2023; *Riley v. California*, 2014).

What technologies are available to law enforcement agencies for use in conducting local and/or remote search and recovery of data from personal devices such as smartphones, tablet computers, etc.?

Technologies such as "mobile device forensic tools (MDFTs)" (Koepke et al., 2020) are available and widely used by law enforcement agencies in the U.S. use in conducting local/remote (remote searches seem to be less prevalent) searches and recovery of data from personal devices (Koepke et al., 2020; Landau, 2020; UMGC, n.d.). Moreover, many of these technologies can bypass encryption methods used by the most popular device makers such as Apple, and Google (Koepke et al., 2020; Landau, 2020; Newman, 2021).

One example of MDFT technologies is Cellebrite's "UFED" (Cellebrite, n.d.-b) which stands for "Universal Forensic Extraction Device" (*Common Digital Forensics Terms, Acronyms, and Certifications*, n.d.). This software technology can "extract data from a wide variety of mobile devices" (*Common Digital Forensics Terms, Acronyms, and Certifications*, n.d.) via a physical connection to said device (Cellebrite, n.d.-b). Another example of MDFT technologies is Cellebrite's "Endpoint Inspector" (Cellebrite, n.d.-c) which allows for remote acquisitions of mobile devices, although marketed to businesses, it does not say that it is prohibited for use by law enforcement (Cellebrite, n.d.-c). Moreover, Cellebrite's products are restricted for use by entities/nations for ethical/lawful purposes (Cellebrite, n.d.-a). Another example of MDFT technologies is Grayshift's/Magnet's "GrayKey" (*Common Digital Forensics Terms, Acronyms, and Certifications*, n.d.) which can bypass security mechanisms of Apple (iOS) and Google (Android) mobile devices and recover data from said devices via physical connection to said devices (Magnet Forensics, n.d.). Moreover, GrayKey is only available to law enforcement agencies (*Common Digital Forensics Terms, Acronyms, and Certifications*, n.d.). Additionally, Belkasoft's "X Forensic" (Belkasoft, n.d.-a) is a forensics tool that can acquire evidence from Apple and Google mobile devices in numerous ways (Belkasoft, n.d.-b). For example, X Forensic can acquire data from iOS mobile devices via "checkm8-based" (Belkasoft, n.d.-b), "passcode brute-force" (Belkasoft, n.d.-b) and "Agent-based" (Belkasoft, n.d.-b) methods while Android data can be acquired via "passcode brute-force" (Belkasoft, n.d.-b), "ADB backup" (Belkasoft, n.d.-b), and "Agent-based" (Belkasoft, n.d.-b) methods (Belkasoft, n.d.-b). Furthermore, this product is only available to law enforcement agencies (Belkasoft, n.d.-a). Lastly, "Pegasus" (PBS, 2023) is a spyware tool created by the "NSO Group" (PBS, 2023) that can collect data from a range of mobile devices remotely once it has infected its target,

although “Officials would not say if U.S. law enforcement and intelligence agencies currently use any commercial spyware” (PBS, 2023).

Based on the prevalence of mobile forensic products available to law enforcement it is crucial to limit the occurrences of uses of these technologies as they harm the confidentiality (and possibly harm the integrity and availability as well) of the data stored on a device which they used (Hashemi-Pour & Chai, 2023).

Summary

In conclusion, the cases of United States v. Keck, and Riley v. California both deal with under what circumstances and with what if any limitations, the police/government can search an individual’s electronic devices (UMGC, n.d.). More specifically, these cases deal with the legality of warrantless searches in the context of the Fourth Amendment (*Riley v. California*, 2014; *United States v. Keck*, 2021). To that point, the rulings in these cases concluded that the Fourth Amendment applied to today’s technological environment means prohibiting searches of an individual’s electronic device’s contents (but not its physical components) without a warrant, without the owner’s consent, or absent “Exigent circumstances” (*Exigent Circumstances and Warrants*, n.d.), because searching so much private data absent a warrant is not reasonable (Fakhoury & Kayyali, 2014; *Riley v. California*, 2014; *United States v. Keck*, 2021). Moreover, this necessarily includes the use of forensic tools (local or remote-based) to access the data of said devices (Fakhoury & Kayyali, 2014; *Riley v. California*, 2014; UMGC, n.d.). Lastly, as illustrated by the vast array of forensic tools available to law enforcement for acquiring data from an individual's electronic devices, protecting said devices from seemingly arbitrary warrantless searches allows individuals to protect their privacy (data’s CIA) as is their

constitutional right (Constitution Annotated, n.d.; Hashemi-Pour & Chai, 2023; Koepke et al., 2020; *Riley v. California*, 2014).

References

Belkasoft. (n.d.-a). *Belkasoft for Law Enforcement*. Belkasoft.com. Retrieved March 6, 2024, from https://belkasoft.com/law-enforcement

Belkasoft. (n.d.-b). *Mobile acquisition with Belkasoft X*. Belkasoft.com. Retrieved March 6, 2024, from https://belkasoft.com/mobile_acquisition

Cellebrite. (n.d.-a). *Cellebrite Provides Facts About its Business and Solutions - Cellebrite*. Cellebrite.com. Retrieved March 5, 2024, from https://cellebrite.com/en/cellebrite-facts/

Cellebrite. (n.d.-b). *Cellebrite UFED | Access and Collect Mobile Device Data*. Cellebrite.com. Retrieved March 5, 2024, from https://cellebrite.com/en/ufed/

Cellebrite. (n.d.-c). *Remote Mobile Collection Capabilities*. Enterprise Solutions. Retrieved March 5, 2024, from https://enterprise.cellebrite.com/remote-mobile-collection-capabilities/

Common Digital Forensics Terms, Acronyms, and Certifications. (n.d.). Retrieved March 5, 2024, from https://www.nacdl.org/getattachment/e30285fa-61eb-4b71-9bdb-6458b7140dc9/common-digital-forensics-terms-acronyms-and-certifications-1-.pdf

Constitution Annotated. (n.d.). *U.S. Constitution - Fourth Amendment*. Constitution.congress.gov. Retrieved March 3, 2024, from https://constitution.congress.gov/constitution/amendment-4/

Cornell Law School. (n.d.). *Fourth Amendment*. LII / Legal Information Institute. Retrieved March 3, 2024, from https://www.law.cornell.edu/wex/fourth_amendment#:~:text=Electronic%20Surveillance

Exigent Circumstances and Warrants. (n.d.). LII / Legal Information Institute. Retrieved March 4, 2024, from https://www.law.cornell.edu/constitution-conan/amendment-4/exigent-circumstances-and-warrants

Fakhoury, H., & Kayyali, D. (2014, October). *Know Your Rights*. Electronic Frontier Foundation. https://www.eff.org/issues/know-your-rights

Hashemi-Pour, C., & Chai, W. (2023, December). *What is the CIA Triad? Definition, Explanation and Examples*. TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Koepke, L., Weil, E., Janardan, U., Dada, T., & Yu, H. (2020, October 20). *Mass Extraction*. Upturn. https://www.upturn.org/work/mass-extraction/

Landau, S. (2020, December 7). *Law Enforcement Is Accessing Locked Devices Quite Well, Thank You*. Default. https://www.lawfaremedia.org/article/law-enforcement-accessing-locked-devices-quite-well-thank-you

Magnet Forensics. (n.d.). *Magnet GRAYKEY*. Magnet Forensics. Retrieved March 6, 2024, from https://www.magnetforensics.com/products/magnet-graykey/#:~:text=85%25%20of%20surveyed%20GRAYKEY%20users

Newman, L. H. (2021, January 13). *How Law Enforcement Gets Around Your Smartphone's Encryption*. Wired. https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/?redirectURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fsmartphone-encryption-law-enforcement-tools%2F

PBS. (2023, March 27). *U.S. to adopt new restrictions on the use of commercial spyware*. PBS NewsHour. https://www.pbs.org/newshour/politics/u-s-to-adopt-new-restrictions-on-the-use-of-commercial-spyware

Riley v. California. (2014, June 25). Casetext.com. https://casetext.com/case/riley-v-cal-united-states-1

UMGC. (n.d.). *Project 2: Law Enforcement Access to Smart Phone Data*.

United States v. Keck. (2021, June 29). Casetext.com. https://casetext.com/case/united-states-v-keck-2

Wallentine, K. (2021, December 21). *Exigent Circumstances in Warrantless Search & Seizure*. Lexipol. https://www.lexipol.com/resources/blog/exigent-circumstances-saves-evidence-of-child-sexual-exploitation/