Privacy Protection Rights: a look into the rights of privacy a user can expect when functioning in the digital world.

Laura Witt

I. Introduction

Technology and digital home assistance devices have increase in prevalence of use in the United States. Some of the more populare devices, such as Google Home or Amazon Alexa, will turn on as the activation word, listen to the request, then complete the task requested. Within the user agreement, the developers have included a blanket waiver to allow them to keep a record of the recording to further "improve the experience"[1] of the user. The developers have the recordings on their servers to better calibrate their listening technology.

Though the developers that maintain the devices only listen for the "wake words"[2], there is an active microphone listening and may be recording what they hear. This would be extremely appealing for the government because the potential criminal would have installed the microphone in their home; they have consented to having this third-party listening for "wake words" but the device is always listening. If the government could get that information from the third-party servers or even listen in live via the active microphone, then they would be able to see the step-by-step planning process of the crime or even include more accessories or co-conspirators to the crime. The question would be what would a government actor need to access these recordings or to be able to permanently turn on the microphone and have a live microphone at all times.

This paper will navigate the historical evolution of the right to privacy in the United States in Part II. In Part III, I will explore the similar surveillance and monitoring requirements from Bosnia and Herzegovina (BiH) Criminal Procedural Code (CPC) and the three canton codes within BiH from the Republic of Srpsha, the District of Brcko, and the Federation of BiH. Part IV will examine the European Convention on Human Rights and the *Klass v. Germany* case that examined the international standard for privacy rights in Europe. Part V will argue that the court should that the approach that information gained from these listening devices should be protected by a search warrant because the sanctity of the home is an important principle to protect.

II. United States of American Right to Privacy, Third Party Doctrine and Technology's Impact on Evidence Gathering

<u>History of the Fourth Amendment</u>

[1] Last updated Sept 24, 2020
https://www.amazon.com/gp/help/customer/display.html?nodeId=202002080
[2] https://www.consumerwatchdog.org/privacy-technology/how-google-and-amazon-are-spying-you

The United States of America and the founding of the nation was heavily influenced by their experience with the British, both positive and negative. The English common law sanctity of one's own home is illustrated in the *Semayne's Case*.[3] This established what is known today as the castle doctrine where an individual may consider "[his] home … as his castle and fortress, as well for his defense against injury and violence as for his repose."[4] Within this decision, however, the King and his agents were granted leave to enter the house after "a knock and request" for entry or if the door was open.[5] By requiring the state actor's to have to "knock" on the door prior to entry and "announcing" their presence, the Court found there was an expectation of "privacy" or a "sanctity" within the home that should be protected from the eyes of the King or the state without just cause.

A second important case for the development of American privacy concept came from *Entick v. Carrington*.[6] This case from 1765 dealt with the general warrant granted to the King's agents. The agents entered Entick's home looking for seditious papers that resulted in hundreds of papers and pamphlets being confiscated and £2000 of damage caused to Entick's home. At trial, Lord Camden found this to be too intrusive and too destructive to the privacy and sanctity of home.[7] The agents took not only the criminal papers but all papers from Entick's home. By the laws of England, every invasion of private property, be it ever so minute, is a trespass."[8] Lord Camden continued his analysis stating that to trespass upon another's property would require justification before a judge who would weigh the argument against the right of man's privacy in his own home.[9]

Back in the colonies, the King's agents were using another legal measure to enforce the will of the King: writ of assistance. The writ of assistance was essentially a carte blanche warrant issued to the King's agents to forcefully search colonists to ensure they were paying the demanded taxes to the Crown; no space or object was safe from an inspection.[10] While this was used as a means to ensure collection of taxes on sugar and molasses, there were no limits on these warrants beyond the lifespan of the issuing King.[11] These writs of assistance enabled "all and singular justices, sheriffs, constables, and all other officers and subjects"[12] to collect the taxes and search the colonists. Upon the death of King George II, there was a six-month term before King George III would be able to renew the writs and general warrants; the

---

[3] *Semayne's Case* 5 Co. Rep. 91 a., 77 Eng. Rep. 194 (1604).
[4] *Id.* at 195.
[5] *Id.*
[6] *Entick v. Carrington*, 19 Howell's State Trials 1029; 95 ER 807 (1765).
[7] *Id.* at 1066.
[8] *Id.*
[9] *Id.* at 1066.
[10] Frederick S. Lane, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 11 (Beacon Press, 2009).
[11] *Id.* at 10.
[12] Excerpt From: John Clark Ridpath. "James Otis the Pre-Revolutionary by John Clark Ridpath and Related Documents." Apple Books. https://books.apple.com/us/book/james-otis-pre-revolutionary-by-john-clark-ridpath/id1459889111

colonists and patriots saw an opportunity to be heard in the court of law.[13] James Otis' oral argument, as preserved by the recollections of John Adams, referenced the new legal texts of English common law in that only "special warrants" meet the modern requirements of probable cause based on an oath or affirmation with particularity of the place to be searched and the things to be seized, and the warrant must be granted by a judge.[14] Otis continued his argument saying the writs were "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that was ever found in an English law book."[15] There does not appear to be a complete record of his concluding statement, one of his last quotes from this five hour, 30,000 word oration describes how "one arbitrary exertion will provoke another, until society be involved in tumult and in blood."[16] This was eluding to the idea that one arbitrary search by the King's agent would frustrate the colonists and provoke a response, which would then lead to a British response until there was war. The Chief Justice found in favor of the King and continued the validity of the writs. Otis' oration had sparked the beginnings of the American Revolution[17] and the authors of the Constitution to protect their citizens from a tyrannical government.

After the Revolutionary War, the founding fathers were crafting the legal documents that would govern the future. The Fourth Amendment of the United States Constitution states:

> 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.[18]

This guarantees a person's privacy from searching their person, house, papers, or items from the government agents who were acting without a neutral magistrate saying the government has reached their burden in establishing probable cause and are able to describe with sufficient details what are the items to be found. This does not apply to non-government actors and was limited to physical intrusions upon a person, house, papers, or effects. Traditionally, this was applied under the notion of the property crime of trespass and required a physical intrusion.

Application of the 4th Amendment Before Katz

During the time between the acceptance of the Constitution and the Bill of Rights, the courts interpreted the Fourth Amendment to protect individuals from physical intrusion by government actors and did not grow as technology grew. In

[13] Lane at 11.
[14] Ridpath at 70.
[15] *Id.* at 66.
[16] *Id.* at 74.
[17] *Id.* at 77.
[18] U.S. CONST. amend. IV

Olmstead v. US, a suspected bootlegger had his phone line wiretapped by the police in order for the government to collect evidence about the efforts of the petitioners to import, possess and sell liquor in direct violation to the Volstead Act or the Nineteenth Amendment.[19] The government set up the wiretap on the phone wires leading away from the house to the telephone poles and were able to listen to all the phone conversations Olmstead made and received while in his home.[20] Olmstead alleged this violated his privacy within his home because he was making or receiving the phone calls while in his home.[21] The 5-4 decision determined the wiretapping was not infringing upon the privacy of Olmstead because there was not an "actual physical invasion of his house 'or curtilage' for the purposes of making a seizure."[22] The court found the wires extending from his home would not be considered to be part of the curtilage home to extend to the far reaches of the world because that would be akin to extending the curtilage of the home to all road and highways.[23] While this is not an undesirable analysis, it fails to consider the content of the conversation that was to be protected and not the means of communication itself.

In two cases cited by the court in *Olmstead*, *Weeks v. United States*[24] and *Ex parte Jackson*[25] both agree the Fourth Amendment extends to protect the sealed letters and packages one receives and require a warrant based on an oath or affirmation of probable cause. Magazines and pamphlets were not protected because their unsealed nature lent them to be examined.[26] These documents were not sealed and could be reviewed at any time by the postal worker who was carrying the mail to the intended recipient.[27] Congress recognized the mail also contained papers to be protected from unreasonable searches and using the mail services to send papers would also be protected if they were sealed from privacy. The communication in these papers were entitled to the privacy unless there was a warrant based on oath or affirmation of probable cause and with particularity issued for the examination of that paper. This should have been extended to the telephone wires and communication in Olmstead as phone calls were quickly supplanting the use of letters as the main means of communication. Unfortunately, the Supreme Court was still applying the need for a physical trespass on the person's property before requiring a warrant.

Justice Louis Brandeis' dissent in *Olmstead* was especially revolutionary in that it predicted the time when the Government would be able to access the private papers once kept in a desk without ever trespassing upon one's land.[28] Justice Brandeis thought the Fourth Amendment and the Constitution had to grow with the

---

[19] *Olmstead v. United States*, 277 U.S. 438 (1928).
[20] *Id.* at 487.
[21] *Id.* at 456-57.
[22] *Id.* at 465.
[23] *Id.* at 466.
[24] *Weeks v. United States*, 232 US 383 (1914).
[25] *Ex parte Jackson,* 96 US 727, 733 (1877).
[26] *Id.*
[27] *Id.*
[28] *Olmstead*, 277 U.S. at 474.

technological advances because the Founding Fathers could not have foreseen the advances of telephone and who knew what technology would be. This new technology which can allow for an intrusion without a trespass "places the liberty of every man in the hands of every petty officer."[29] The limited view that an intrusion upon one's privacy could only occur if there was a physical trespass upon a person, their home, their papers, or their effects would be extremely narrow and proceed to expose the most inner workings of a home; "a subversive of all comforts of society."[30]

After *Olmstead*, the courts and government enjoyed almost 40 years of wiretapping and collecting the intimate details of conversations happening between citizens without recourse.

Katz v. United States and "The Fourth Amendment protects people, not places."[31]

Charles Katz was a man who lived in Los Angeles, California with a weakness for college basketball and gambling.[32] He went to the payphone on the 8200 Sunset Boulevard block between February 19th thru February 25th, 1965 and made a series of phone calls to bookies on the east coast discussing what the point spreads should be.[33] The federal agents, who were aware of Katz's betting scheme, set up microphones on the phone booths on this block to record the phone conversations between Katz the handicapper and his bookies.[34] They taped the microphones on the outside of the phone booths, not inside the booth, and had federal agents follow Katz from his apartment to the phone booths to then signal to their partner Katz was making a phone call and to begin to record the conversations.[35] The FBI agents were able to get the information they needed to arrest and search Katz's apartment with a warrant.

Harvey Schneider, defense counsel for Katz, argued in his post-cert grant brief that once Katz closed the door to the phone booth, there was a "reasonable expectation of privacy" that society would deem as reasonable.[36] The "reasonable person" standard was drawn from the concept of tort law, which took root in the majority opinion authored by Justice Stewart, and the concurrence by Justice Harlan. This "reasonable person" standard created a new test and privacy analysis for the Court to grow with the technological advances.

Justice Harlan's concurrence expanded the idea of an intrusion to include the electronic intrusion that had previously been disregarded in *Olmstead*.[37] He continued to outline what has become known as the *Katz* test for a person's privacy

---

[29] *Id.* (quoting James Otis).
[30] *Id.* (quoting Lord Camden from *Entick v. Carrington*).
[31] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[32] CSPAN LANDMARK CASES, https://www.c-span.org/video/?440873-1/supreme-court-landmark-case-katz-v-united-states (Last visited Apr. 21, 2021); Harvey Schneider, "*Katz v. U.S.:* The Untold Story," 40 MCGEORGE L. REV. 13 (2016).
[33] *Katz v. US*, 369 F.2d 130, 131-132 (9th Cir. 1966).
[34] *Id.* at 132.
[35] CSPAN, *supra*.
[36] Schneider, *supra*, 17
[37] *Katz*, 389 U.S. at 360-361.

protection under the Fourth Amendment. The first step was to establish the person has displayed an actual expectation of privacy. In applying this to the facts of the case, Katz showed he had an actual expectation of privacy because he closed himself in the phone booth.[38] While the public could see him through the glass panes of the booth, Katz was trying to exclude the "uninvited ear" to his conversation, not the "intruding eye."[39]

The second part of the *Katz* test was whether or not society accepts the expectation to be "reasonable."[40] The Supreme Court had already held that intercepting communication via electronic penetration would be a "search and seizure."[41] The Federal Communications Act of 1934 protected the content of aural communications from distribution to those not intended for the conversation.[42] By having Congress pass this federal statute, society has deemed it reasonable for conversations being held over the phone lines and in a "private" place to be a reasonable expectation of privacy.

Most interestingly, from Justice Harlan's concurrence was perhaps the foundation for what later becomes known as the third party doctrine: what a person has in their home has an expectation of privacy but what the person has "exposed to the 'plain view' of outsiders [is] not protected because there is no intention to keep them to himself…"[43]

Third Party Doctrine and *Miller* and *Smith*

When discussing the third party doctrine, the two seminal cases that establish the government's ability to access data from a party not the plaintiff without a warrant were *United States v. Miller*[44] and *Smith v. Maryland*.[45]

In *Miller*, the federal government had passed the Bank Secrecy Act of 1970[46] which required banks to keep copies of financial data of their customers in an effort to combat money laundering and counterfeiting of US currency. Miller was an undocumented whiskey distiller in Georgia who was brought to trial by the Alcohol, Tobacco, and Firearms Bureau for conspiracy to distill spirits and possession of an unregistered still.[47] Part of the ATF's evidence was bank records they had obtained via a subpoena, not a warrant.[48] This was an important distinction because the bar for acquiring a subpoena would be lower than that for a warrant and would not be considered a "seizure" under the Fourth Amendment.[49] The government's argument

[38] *Katz*, 369 F.2d at 132.
[39] *Katz*, 389 U.S. at 352
[40] *Id.* at 361.
[41] *Silverman v. U.S.*, 365 US 305 (1961)(concluding that the physical penetration into the petitioner's apartment to intercept communication violated the Fourth Amendment).
[42] 47 U.S.C. § 605
[43] *Katz*, 389 U.S. at 362.
[44] *United States v. Miller*, 425 U.S. 435 (1976).
[45] *Smith v. Maryland*, 442 U.S. 735 (1979).
[46] 12 U.S.C. § 1829b (2020).
[47] *Miller*, 425 U.S. at 435-36.
[48] *Id.* at 437.
[49] *United States v. Dionisio*, 410 U.S. 1, 8-9, (1973).

was this information was knowingly disclosed to the bank and therefore Miller did not have an expectation of privacy because checks are not a private exchange of information but negotiating tools used in commercial transactions.[50] In addition to this reduced expectation, the records were kept in accordance with the Bank Secrecy Act of 1970 and thus "business records" of the bank and not the private papers of Miller.[51]

This was an interesting perspective that the Court and Congress have taken because at least one Founding Father felt the protection of his own financial data was something that is protected.[52] John Adams once wrote in his diary "I have no moral or other [o]bligation to publish to the [w]orld how much my [e]xpenses or my [i]ncomes amount to yearly."[53] Yet, Congress and what laws they have passed have usually been a good barometer for what society has deemed to be reasonable because they have to be elected by the people and have to answer to the people.[54] Based off of Congress' passage of this bill, society has decided financial institutions should allow access to their private information, with a subpoena, on the mere suspicion of wrong-doing. Society has decided that this expectation of privacy of personal financial data is not reasonable.

Another case that cemented the third party doctrine was *Smith v. Maryland*.[55] Patricia McDonough had been robbed by an individual later identified as Michael Lee Smith.[56] He was identified because he made numerous phone calls to McDonough's residence claiming to be the robber and once asked her to step out onto her porch as Smith drove by in his Monte Carlo.[57] The police installed a pen register on Smith's phoneline to see if he was the individual who was calling McDonough.[58] Once the pen register confirmed Smith was indeed the caller, the police obtained a warrant to arrest Smith.[59] Smith alleged his Fourth Amendment right to privacy was violated when the police installed the pen register on his phoneline without a warrant.[60]

The pen register has been used by phone companies since the beginning of the use of phones as a means of knowing how to charge their customers. The pen register does not record the content of the phone call made but merely the phone numbers dialed from that line.[61] In a 5-3 decision, the Court found there was no "legitimate" expectation of privacy[62] because this information is voluntarily given to a third party and this information is routinely used by the third party for business purposes.[63]

---

[50] *Miller*, 425 U.S. at 442.
[51] *Id.* at 442-443.
[52] Lane, *supra*, 2.
[53] *Id.*
[54] *Baker v. Carr*, 369 U.S. 186, (1962).
[55] *Smith v. Maryland*, 442 U.S. 735 (1979).
[56] *Id.* at 737.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *See generally, Smith v. Maryland*
[62] *Smith*, 442 U.S. at 745.
[63] *Id.* at 744.

The pen register has been a mere tool for the phone company for billing purposes for many years. Historically, there was a phone operator who would physically connect the two phone lines in order for the phone call to take place. There was no intrusion upon the customers' conversation or communication which can relate back to the historical Fourth Amendment protection. The Founders were searched by the British for any communication about seditious acts or the start of the Revolution based on mere suspicion.[64] *Silverman* and *Katz* emphasized the content of the communication was equivalent to the exchange of letters the earlier Courts held to be protected in *Weeks* and *Ex parte Jackson*. The pen register and the information obtained from the phone numbers would be equivalent to the address on the outside of a sealed envelope or the weight of the letter. The postal service would need to know where to send the letter and how much postage to charge the sender as part of their carrying services. The phone company knowing which number to dial and possibly the duration of the phone call for the purposes of billing would not be considered to be too invasive information to collect and store.

Both of these cases cemented the idea of disclosing certain information to third parties was not subject to the stringent standard of the Fourth Amendment scrutiny. The third party doctrine has to balance the expectation of privacy of the individual and the needs of the government to gather information to protect the public.[65]

Interim with *US v. Warshak* and *US v. Microsoft*, and the Stored Communications Act of 1980

Technology moves by leaps and bounds whereas the law moves like molasses in January in the Rockies. From the days of having a home phone like in *Smith*, most communication is done via the invisible waves of the internet. Cellphones have quickly replaced the need for a landline and the traditional postal services used for mailing letters have been replaced by the instantaneous delivery of electronic mail, also known as email.

The Stored Communications Act of 1980 has greatly eroded the protection once afforded by the Fourth Amendment.[66] The government may compel an ISP or other electronic database to turn over information, including communications, that have been stored on their servers over 180 days with either a subpoena or a court order.[67] Though this section states the government is required to notify the private individual of the request for information, a later section in the Act allows the government to delay that notice for up to ninety (90) days if there is reason to believe notice would hinder the government's interest.[68] However, there has not been a Supreme Court case to challenge the Stored Communications Act and whether their guidelines are

[64] *See generally*, Lane *supra*.
[65] Mihailis E. Diamantis *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485, 504 (2018).
[66] 18 U.S.C. § 2703 (2021).
[67] 18 U.S.C. § 2703(b).
[68] 18 U.S.C. § 2705.

constitutional. There was one case that came close to discussion and that was *United State v. Microsoft*.

In 2017-18, the Supreme Court was holding arguments and accepting briefs for the case between the United States Department of Justice and Microsoft Corporation.[69] The DOJ had provided warrants supported by probable cause to Microsoft Corp. for the contents of emails they (Microsoft) had stored on servers in Ireland.[70] However, this case was never fully decided and analyzed by the Supreme Court because Congress and the President passed and signed into law the CLOUD Act to amend the Stored Communications Act.[71] This CLOUD Act ordered any service provider in the United States to comply with a warrant for information whether that information is stored in the United States or abroad.[72] Because this law was passed while the Supreme Court was accepting briefs and debating the outcome, the case had to be vacated and remanded to follow the newly signed CLOUD Act.[73]

In the Sixth Circuit, there was a case that questioned the constitutionality of the SCA to allow the contents of emails to be obtained without a warrant supported by probable cause and with particularity.[74] This Court compared the internet service provider (ISP) to that of the postal service or telephone company; both of which the Supreme Court said would trigger a Fourth Amendment violation if they attempted to access the content of the communication they are transporting on behalf of their customer.[75] They acknowledge this opinion is contra to *Miller* decision but the analogy with the postal carrier is not apt than that of a bank collecting pertinent information during the "ordinary course of business."[76] Mere access to information does not correlate the right to access such information.[77]

In *Riley v. California*,[78] Riley was arrested for driving on a suspended license. During the search incident to a lawful arrest, the police found a smartphone on Riley's person. On the phone, the arresting officers found evidence Riley was part of a gang and other evidence that he may have been a part of a gang shooting the police were investigating. The Supreme Court held the information recovered from the phone would require a search warrant because of the vast amounts of information that can be stored on these small devices. They also concluded that since the phone was already in police custody, there was little chance of the individual gaining access to the phone to destroy any evidence before a warrant was issued by a judge. While there

---

[69] Supreme Court docket, https://www.supremecourt.gov/DocketPDF/17/17-2/39928/20180323205735087_17-2%20USA%20V.%20Microsoft%20Corp..pdf (Last visited Apr. 2, 2021).

[70] https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/

[71] https://www.supremecourt.gov/DocketPDF/17/17-2/39928/20180323205735087_17-2%20USA%20V.%20Microsoft%20Corp..pdf

[72] https://www.supremecourt.gov/DocketPDF/17/17-2/39928/20180323205735087_17-2%20USA%20V.%20Microsoft%20Corp..pdf

[73] https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/

[74] *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

[75] Warshak at 286.

[76] Warshak at 288 (quoting and analyzing Miller).

[77] Warshak.

[78] *Riley v. California*, 573 U.S. 373 (2014).

may be a valid concern for a remote wiping of the information on the phone, the police would be able to prevent that by disconnecting the phone from the internet or cell service by simply turning off the phone.

Another interesting case that discussed what society knowingly exposes to the public is from the concurrences of *United States v. Jones*.[79] Justice Sotomayor discussed the relative ease of using GPS location, the inexpensive nature of the equipment or even the ability for the government to "store and mine" the information collected for years after the initial contact. Justice Alito also agreed that short-term monitoring had been previously discussed in *United States v. Knotts* as allowed. In *Jones*, the better question to answer where once long-term monitoring was cost prohibitive, now cheaply and accurately done should be addressed under the 4th Amendment's purview. Both pointed to the inefficiency of Congress and state governments to act and their inaction has led to this being decided by the Supreme Court and decided, perhaps, incompletely.

Carpenter and CSLI

In 2018, the Supreme Court heard a case that carved out an extremely narrow exception with respect to cell site location and the government's ability to access that information.

There were a series of armed robberies occurring in the Detroit, Michigan metro area.[80] A member of the robbers was apprehended and turned his phone over to the police who later used a court order to compel the cell companies for the cell-site location data from sixteen numbers in the phone who were identified as taking part in the robberies.[81] Per the Stored Communications Act, the government may compel telecommunication companies to disclose certain "records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'"[82] Carpenter's CSLI (cell site location information) court order produced 127 days of information, 12,898 data points for the government to analyze.[83] Through this information, the police were able to confirm Carpenter was in the area of four confirmed robberies at the time of the robberies.[84] Carpenter alleges this was an invasion of his privacy and Fourth Amendment expectation of privacy.[85]

The Court entertained an analysis about how the cellphone has the capacity to store "massive amounts of data" that generally require a warrant before searching.[86] But CSLI, compiled by the phone companies for business purposes, also falls into the realm of third party doctrine because there is a third party who is compiling

---

[79] *United States v. Jones*, 565 US 400 (2012).
[80] *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018).
[81] *Id.*
[82] *Id.* (quoting 18 U.S.C. § 2703(d)).
[83] *Id.* at 2212.
[84] *Id.* at 2213.
[85] *Id.* at 2212.
[86] *Id.* at 2214 (quoting *Riley v. California*, 573 U.S. at 34 (2014)).

information, not content, about their user.[87] Cell companies were required by the Wireless Communication and Public Privacy Act to be able to pinpoint the location of a cell phone in the case an emergency call was made.[88] This requirement is similar to *Miller* in that a non-government agent is required to maintain business records in accordance with a federal statute and thus, the individual who is using the service should not have an expectation to privacy. However, the Court had previously found that long-term GPS (global positioning system) without a warrant would "impinge[] on the expectation of privacy" because they can monitor "every movement."[89] Having the location of an individual constantly monitored or available for recall months after the fact is invasive.

Ultimately, the Court held the information stored via CSLI was too invasive to allow the government access without a warrant.[90] "[N]ear perfect surveillance"[91] was too much for the Court to rationalize as reasonable. Chief Justice Roberts returned to Justice Brandeis' dissent from *Olmstead* to ensure the progress of science and technology does not erode the Fourth Amendment as intended by the Founding Fathers by allowing the government an effortless tool to carry out their duties.[92]

The Court did create a bit of life for the government actor who wanted CSLI without a warrant. They declined to establish a minimum number of days the government may request the cell companies to turn over but they did state that seven (7) days of consecutive information was too much and constitutes a "search" under the Fourth Amendment.[93] Because there has not been any new case law to debunk this minimum, the government can access the CSLI for a number for up to six (6) consecutive days without needing a warrant, which is the ultimate end goal. Requiring a warrant for access to private data would create more barriers between the government and citizens' privacy.

III. Bosnia and Herzegovina Criminal Procedure Code

Bosnia and Herzegovina (BiH) is a nation located in the Balkan region of Europe. Their legal system was established in the civil law tradition meaning they rely heavily on their civil code.[94] After a devastating civil war in the 1990s, the governing powers of BiH have four separate codes by which they operate. The US federal equivalent would be the BiH CPC. The other three represent the three entities that compose BiH. The Federation of Bosnia and Herzegovina (the Federation) and the Republic of Srpska (Srpska) are the two largest entities. The District of Brcko (Brcko) is a smaller city-state like entity that had to be collectively negotiated for

---

[87] *Id.* at 2209-10.
[88] Jen Manso, CELL-SITE LOCATION DATA AND THE RIGHT TO PRIVACY, 27 Syr. J. of Science and Tech. L. 1, Fall 2012.
[89] *Id. Carpenter,* 138 S. Ct. at 2215 (quoting *United States v. Jones*, 565 U.S. 400 (2012)).
[90] *Id.* at 2217.
[91] *Id.* Carpenter at 2217.
[92] *Id.* Carpenter at 2224.
[93] *Id.* Carpenter at 2217, footnote 3.
[94] https://www.cia.gov/the-world-factbook/field/legal-system/ (last accessed Apr. 6, 2021).

independence from both Srpska and the Federation at the conclusion of the war. All three entities have their own CPC but there had to be strong similarities between the three for their citizens to enjoy relative uniformity and peace. Plus, in order to be accepted to the Council of Europe, certain rights and guaranties had to be included in their new codes.

Generally speaking, all four CPC codes have the same laws but under different code numbers. For example, the requirements for searching a dwelling, or other premises and persons would all contain something similar to the following:

> (1) A search of dwellings and other premises of the suspect accused or other persons as well as their personal property outside the dwelling may be conducted only when there are sufficient grounds for suspicion that the perpetrator, the accomplice, traces of a criminal offense or objects relevant to the criminal proceedings might be found there.
> (2) Search of personal property pursuant to Paragraph (1) of this Article shall include a search of the computer systems, devices for automated and electronic data processing and mobile phone devices. Persons using such devices shall be obligated to allow access to them, to hand over the media with saved data, as well as to provide necessary information concerning the use of the devices. A person, who refuses to do so, may be punished under the provision of Article [] Paragraph (5) of this Code.
> (3) Search of computers and similar devices described in Paragraph (2) of this Article, may be conducted with the assistance of a competent professional.[95]

Searching of a computer and other similar devices would require a search warrant and an expert to access the information.[96] This would not be unreasonable because of the sensitive nature of the technology. One wrong keystroke or accidental brush of the chip could lead to destruction of evidence or even property if it was later discovered the potential suspect was unassuming.

Surveilling or means of gathering evidence from suspects were termed as "special investigative actions" in the BiH codes. All four codes[97] [98] [99] [100] have essentially the same list that require approval from the judge before the police would be able to carry them out. Monitoring telecommunications, surveilling individuals, and access to computer data all would require the court approval for collection or

[95] Chapter 8 Article 51 Crim P. Code Brcko District.
[96] *Id.*
[97] Chapter 9 Article 116 Crim. P. Code Bosnia and Herzegovina.
[98] Chapter 9 Article 130 Crim P. Code Federation of Bosnia and Herzegovina.
[99] Chapter 9 Article 116 Crim. P. Code Brcko District.
[100] Chapter 8 Article 116 Crim. P. Code Republic of Srpska

monitoring. Personal data that has been willingly disclosed to businesses or internet service was not addressed in the BiH codes but it has been addressed by European entities.

IV. Comparison with European Council for Human Rights and the Council of Europe

The Council of Europe is the leading organization on the Continent in protecting the human rights their society has deemed to be appropriate and acceptable. There are many benefits to being a member of the Council that lead to the independent nations to adopting the ideals to their own laws. In fact, there is only one nation in Europe that is not accepted to the Council and that is Belarus.[101] This is not to be confused with the European Union. The Council of Europe's purpose is to protect human rights and the rule of law in Europe with promoting democracy;[102] the European Union is a smaller subset of the Council of Europe that has an economic focus in addition to the Council of Europe goals of protecting human rights.[103]

Of the many Articles of Human Rights, Article 8 protects the right of privacy of an individual. "Everyone has the right to respect for his private and family life, his home and his correspondence."[104] This evolved from the Germanic idea that an individual has an expectation of privacy about the intimate details of his life that he has chosen to not make public.[105] The idea of protecting family life and private life was to allow "the development, without outside interference, of the personality of each individual in his relations with other human beings."[106] This broad term would allow the law to grow with the change society would make as technology and intellect change.

The primary purpose of Article 8 is "to protect against arbitrary interferences with private and family life, home and correspondence by a public authority."[107] This right is weighed against the state's interest in promoting and "necessary to maintaining a democratic society."[108] The nature of the invasion and the type of information being sought would have to be considered.[109] Typically, prolonged and

---

[101] 47 member states, https://www.coe.int/en/web/portal/47-members-states (last accessed Apr. 13, 2021).
[102] The Council of Europe in brief, https://www.coe.int/en/web/about-us/do-not-get-confused (last accessed Apr. 17, 2021).
[103] About European Union, https://europa.eu/european-union/about-eu/eu-in-brief_en (last accessed Apr. 17, 2021).
[104] Article 8 section 1 of the European Convention on Human Rights – Right to respect for private and family life.
[105] Gloria Gonzalez Fuster THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 25-27, (Springer Int'l Publ'g Switz, 2014).
[106] *Guide to Article 8 of the European Convention on Human Rights – Right to respect for private and family life*, 31 Aug 2020, available at https://www.echr.coe.int/documents/guide_art_8_eng.pdf; at 38 (last accessed Apr 20, 2021); *see also* Gonzales Fuster at 23-24
[107] *Guide to Article 8*, p7
[108] Article 8 § 2 ECHR
[109] *Id.* at 38-39

persistence surveillance would trigger an Article 8 evaluation and require justification from the state for why they felt the need to violate the rights of an individual. They also would consider whether or not that information would be readily accessible to the public at large. If a person was walking down a public street, access to a security camera pointed to the sidewalk to see that individual would not be considered an invasion of privacy under Article 8.[110] The rationale for the public sidewalk monitoring not being too systematic, one of the hallmarks for an invasion of privacy, was the acts were being exposed to the public already; technology merely allowed for there to be a record of the acts.[111]

In Klass and others v. Germany,[112] the German government had authorized the surveillance of communication between attorneys and their clients for the purposes of gathering evidence. The petitioners in this case alleged the long-term nature of the surveillance required the state to notify them of the surveillance being conducted. The State maintained the surveillance had to be conducted in secret to preserve the integrity of the information collected from the monitoring. Article 8 specifically created an out for the government to intrude upon the privacy of the citizens if it was necessary for the maintenance of the democratic state. In this case, the German law allowed for any communication to be monitored if there was sufficient cause and the applicable warrants were issued. The Court held there was no violation of Article 8 because the state showed sufficient reasons for maintaining the secrecy.

Article 8 also considered what was knowingly disclosed to the public sphere to be collectable by the state.[113] This would lead to accessing information from various third-parties to whom the individual had disclosed information. A third-party application on a cell phone or even the cellphone itself would have massive amounts of information that could be accessed easily if there was a need. Instagram and Facebook have routinely requested the ability to track the user's current location. The social media company's rationale for gathering the user's location is to better provide information and a more curated experience for the users. Many think it may also have to do with this is marketable data social media developers can use as leverage for businesses who hope to use their platform for promotion purposes. If Facebook know a great majority of their users are posting about a new musical festival happening in the Caribbean, then there is a high probability they would try to either set up direct competition with that music festival or they would attempt to broker some deal to become a part of the financial venture. The Council has considered this and their recent resolutions would require an analysis on the intentions of the information gathering.

In 2016 and in 2018, the European Union, a niche of the Council of Europe, implemented new resolutions that would further protect the data of the users in technology. Regulation 2016/679 was concerned about the movement of information

---

[110] *Id.* at 39
[111] *Id.* at 120
[112] Klass and others v. Germany, A Eur. Ct. H.R. 28 (1978).
[113] Article 8 guide at 38

within the market.[114] Regulation 2018/1725 further required clear and affirmative consent to allow the entities who are requesting the data to have the data.[115] The individual nations have to implement something similar to their codes.[116] Both resolutions required an independent council to monitor the entities who are conducting business on the Continent and within the EU to comply with their guidelines.[117]

For the governments to have access to the data the European users have knowingly granted valid consent to be used, the state actors have to show there is a compelling interest in having access to that information.[118] The Council of Europe's dual goals are to promote democracy and protect human rights. The human right to privacy has to be balanced against the state's interest to protect the rule of law. Generally, if there is a valid government interest in the information, and they are able to show access to the data is "necessary and proportionate in a democratic society to safeguard public security and for the prevention, investigation and prosecution of criminal offenses or the execution of criminal penalties,"[119] the court will allow them access to the data. This is similar to what the United States have.

V. Where the United States should go from here

Privacy, in a very real legal sense, has to do with the right to disseminate information to whomever, however, whenever (or never), an individual may chose. This also includes the very personal development of a personality and how that individual evolves as a person or how they will interact with human beings and society at large. This very broad yet fragile concept is not something that can be easily separated from the idea of a "public" life because they are intertwined and intersect at times the individual may wish they would not. An English word that is not included in the modern law that I think would apply well is intimacy. The intimate life an individual has within a home has some sort of legal protection from unnecessary and capricious intrusions of the government, but we do not always call it intimacy. The United States has evolved the right to privacy to protect many things from choice of sexual and intimate partner,[120] to the right to rear a child to be multilingual in direct defiance of a state mandate that said otherwise,[121] to the right to protect the goodwill of a person's reputation from harm. This concept is ever expanding yet can be

---

[114] Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 Apr. 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (last accessed Apr. 19, 2021).
[115] Regulation (EU) 2018/1725 of the European Parliament and of the Council, 21 Nov. 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN (last accessed Apr. 19, 2021).
[116] *Id.*
[117] European Data Protection Board, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (last accessed Apr. 21, 2021).
[118] Regulation 2018/1725, *supra*.
[119] *Id.* at § 44.
[120] *Lawrence v. Texas*, 539 U.S. 558 (2008).
[121] Meyer v. Nebraska, 262 U.S. 390 (1923).

extremely narrowed in on the individual's freedom to make choices about their personal lives that are not a detriment to society as a whole. This is extremely similar to the Article 8 of the Council of Europe because they feel the right of an individual to develop their own personality, outside the direction of others, is paramount to the human life experience.[122]

With respect to the civil law tradition, the Bosnian codes have specifically laid out what may and what may not be allowed when investigating a person. The specificity of this code allows the police to look and see if the surveillance technique they are using will require additional clearance before proceeding. In the US, the police act but do not know whether that act is considered unconstitutional until many years later as the case works its way through the court system. Having the specific list is beneficial because it clearly outlines what is and is not appropriate behavior.

The Bosnian code and the Council of Europe resolutions outline the fundamental right to privacy as an essential human right. However, they have conceded the governmental interest in preserving democracy can impinge this right. This is similar to the United States in the governmental interests to promote the rule of law outweigh the individual privacy rights. The balancing test is conducted by a learned judge who evaluates if the government has shown valid reasons. Both entities agree if someone is willingly disclosed to the public or another party, the expectation of privacy is significantly reduced.

A compelling suggestion from the literature is to expand the idea of "privilege" discourse and information.[123] There is only one codified privilege in the federal code and that is the attorney-client privilege. This is an interesting argument because there is already a precedential example of how a client knowingly, intelligently, and voluntarily discloses information to another individual (the attorney) yet that individual has the duty to keep that information confidential is a powerful argument. To treat every relationship or exchange of information like that of the attorney-client privilege would be too harsh of a rule to put into place. Physicians and those with access to medical information are required to keep that information confidential unless there is some compelling interest such as a global pandemic or subpoena to a court of law. The doctor-patient privilege is only recognized as the state level in case law and some state statutes; US federal law does not have such recognition. A state actor can access that information if they are able to show a compelling interest to need access. Impeding the police would reduce their ability to promote the rule of law.

Perhaps a better argument would be to evaluate what is deemed as public knowledge and what is not. If a social media user has most of their setting on "private" and reduces who may or may not view their profile, they would have a higher expectation of privacy than say a celebrity who has their profile public for all the world to see, even non-platform users. What is a reasonable expectation of privacy and how can we, as a society, be sensitive to the needs of different sects of our society? A person who posts their entire life on a social media platform may knowingly expose

---

[122] *Guide to Article 8, supra.*

[123] Mihailis E. Diamantis *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. Pa. J. Const. L. 485 (2018).

certain aspects of their life but they should also be able to control what is easily accessible by someone who does not have their explicit permission.

My suggestions for adaptation by both the US and Bosnia and Herzegovina is to consider what is necessary for the third parties to conduct business and would requiring a warrant for access to that information change the content of the information or the volume of information collected. *Riley* noted the cellphone we carry everywhere, everyday has mass amount of information stored in a neat, compact format that would provide the police with information they did not know they would need. Requiring a warrant for something already in their custody and without the ability to tamper is not too much of an imposition upon the government. *Jones* concurrence by Sotomayor and Alito both mention the technology in use then was too precise, to easy to access by police that there has to be more steps to complete before they would have a near accurate depiction of the whereabouts and happenings in an individuals life. The requirements for a warrant are higher than a court order or a subpoena but there are some areas of life that are too precious to not protect.

The former CEO of Google once said "…when you post something, the computers remember forever,"[124] Because the internet and computers have vast memory capabilities and there is usually some way to retrieve that information, the threat of loss of evidence loses the weight of the argument against needing a warrant for access. A warrant requirement does not forever forbid access to the information like the attorney-client privilege can do; it merely adds an additional step to try and prevent egregious police misconduct and protect the privacy of individuals.

[124] THE COLBERT REPORT: ERIC SCHMIDT; (Comedy Central Broadcast Apr. 23, 2013).