Ethical Dilemma: Police Access to Private Internet Data An analysis of the ECPA of 1986, its effects on the St. Louis area, and the proposed solutions to remedy this outdated document.

Amber Essary

Amber Essary

Doctor Scott D. Peterson

HONORS 3100

12/13/20

Paper 7: Ethical Dilemma: Police Access to Private

An analysis of the ECPA of 1986, its effects on the St. Louis area, and the proposed solutions to remedy this outdated document.

Introduction:

When it comes to internet and electronic device privacy, not many people are aware of how much of their information is actually being monitored by multiple parties. Police access to personal internet and media data is one of the most controversial ethical dilemmas in the United States. As long as there are adequate checks and balances in place, police should be able to monitor private internet and media data when solving crimes. Brian A. Jackson points out the ethical dilemma of this topic in his article, "Using Digital Data in Criminal Investigations: Where and How to Draw the Line," when he asks, "Though public safety is an important goal, how much of a modern citizen's 'digital footprint' should be available for criminal or other investigations?" With this in mind, it is shocking to discover that the most recent comprehensive policy on police access to different kinds of internet and media data is the Electronic Communications Act (ECPA) of 1986. As the staff at the American Civil Liberties Union (ACLU) put it in their article, "MODERNIZING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)," "In 1986, there was no World Wide Web, nobody carried a cell phone, and the only 'social networking' two-year-old Mark Zuckerberg was doing was at pre-

school or on play dates.” At this time in the world’s history, the law that would protect the privacy of all the future technologies and social media sites that are used today was passed.

Intro to Maury Travis, St. Louis:

MAURY TROY TRAVIS

OCT 25, 1965- JUNE 10, 2002

According to the St. Louis Post-Dispatch article, "Travis: Mystery of killings unravels slowly," Maury Travis was born and raised in Missouri and attended St. Louis Public Schools from 1971 to 1985. He lived in Ferguson, MO, and was described by neighbors as a "quiet, respectful boy who sometimes mowed her lawn without being asked and showed her how to use an electric hedge trimmer." After graduation, Travis served two years in the Army reserves as a medical and dental assistant. In 1987, twenty-two-year-old Travis attended Atlanta's Morris Brown College. It was during this time that Travis became addicted to cocaine and his seemingly normal life began a downward spiral ("Travis: Mystery...” 10).

Travis's self-described $300-a-day cocaine consumption soon got him into trouble with law enforcement when he robbed five shoes stores in an eight-day period in 1988. Travis was sentenced to fifteen years, released on parole after five years, and imprisoned again for breaking parole by way of illegal drug possession. Soon after his release in January 1999, the body of his first alleged victim, Mary Shields, was found in July of 2000. Travis is imprisoned again in November 2000, for violating parole and released in March of 2001. Once again, another body was discovered shortly after his release. The body of Alysa Greenwade was found in April of 2001. Nine more bodies were located over the next two years, all with similar characteristics to the first two. The only difference in these new bodies is that they were the bodies of local sex

workers, most of whom had an addiction to cocaine. Law enforcement soon realized that they had a serial killer on their hands ("Travis: Mystery...” 10).

Stephanie Simon discusses the ultimate discovery of Maury Travis in her article, "Virtual Trail Led to Serial Killer Suspect." With bodies piling up in the St. Louis area, police had no leads until an anonymous letter with a google map location was sent to a journalist working for the St. Louis Post-Dispatch. It was from this map location that the police derived the site used and subpoenaed from that site the only IP address that zoomed in on that specific area that day. Then the FBI served a subpoena to the internet provider that was over that specific IP address, and the “St. Louis video strangler” was unmasked. According to the article, it was June 7, 2002, that serial killer Maury Travis was arrested by federal officers who followed an intricate trail linking Travis to the murders of multiple women based on his Internet Protocol (IP) address (Simon). On June 10, 2002, Maury Travis committed suicide in his jail cell-- leaving investigators with numerous unanswered questions. This act of selfishness also deprived family members of nearly twenty victims from ever finding out what truly happened to their loved ones ("Travis: Mystery... 10).

Maury Travis is an excellent example of how allowing the police to properly access internet data resulted in the ending of an almost two-year-long killing spree. If it had not been for the FBI and police being permitted to access that specific data, it is unknown how many more helpless women Maury Travis would have brutally tortured and killed. Juan I. Blanco discusses the legal side of the Maury Travis discovery in his article, "Maury Troy Travis: Murderpedia, the Encyclopedia of Murderers." He writes how, luckily, when it came to obtaining IP addresses in 2002, the USA Patriot Act of 2001 had recently clarified the requirement that a subpoena is necessary to access this form of data. Before this, the ECPA of 1986 had painted a vague shadow

over this specific area, causing investigators to have to look to previous court rulings to decide how to proceed. This minor update greatly aided investigators by saving time and providing clarity to what was expected to access the information they required.

Background of ECPA of 1986:

History and Contents of the Electronic Communications Privacy Act and its Family

The article, "Privacy & Civil Liberties," by the DHS/ Office for Civil Rights and Civil Liberties and the DHS/ Privacy Office helps explain the origin of the Electronic Communications Privacy Act (ECPA). The ECPA was adapted in 1986 and contains the Stored Wire Electronics Communications Act. This act came as an update to the Federal Wiretap Act of 1968 and helped further define the requirements regarding law enforcement access to personal data. At this time in America's history the internet was a brand-new concept, and there was no way that the writers of this document could comprehend how far this area would advance in the next few years. The lack of applicability in this document has led to outdated stipulations being applied to concepts that were never even understood at the time of this document's inception. With no specific policy on the newly developed means of communications and data storage since 1986, law enforcement has been left to refer to past court decisions and personal judgement to make calls regarding accessing private internet data. While the ECPA has not been updated itself since it was created, there are certain amendments that have been made to help further define different problem areas.

The ECPA is made up of three titles which are as follows: Title I- the Wiretap Act, Title 2- the Stored Communications Act, and Title III- the Pen/Trap Statute. Title I: The Wiretap Act gives regulations regarding the allowances for intercepting communications as well as restricts the use of this evidence if it is obtained illegally. Title II: The Stored Communications Act

defines privacy protection for stored files and records that are held by service providers. (It is this section that vaguely covers access to IP addresses and has since been further clarified by the USA PATRIOT Act of 2001.) Title III: The Pen/Trap Statute covers trap and trace devices by mandating that a court order be obtained before using a "pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated)" ("Privacy & Civil…"). The most notable amendments to the ECPA are as follows: Communications Assistance to Law Enforcement Act (1994), the USA Patriot Act (2001), the USA Patriot Reauthorization Acts (2006), the FISA Amendments Act (2008), and others all branch off of the ECPA ("Privacy & Civil Liberties"). Each of these did a part in attempting to further define a specific area where the ECPA was excessively lacking; however, there are still numerous pieces that need updates and better unification.

Argument for Police Right to Access Private Data

Emphasizing the Need for Effective Policy

Police right to monitor private internet data is ethically justified due to their power, process, and product. It is clear to see that there is work that needs to be done in the area of policy-making; however, with technology advancing as rapidly as it has been, law enforcement is already struggling to stay ahead of the curve. This kind of access to personal data both prevents and resolves crimes.

Police possess the power necessary to fulfil the duties of the job of serving and protecting the people. They are expected to investigate claims of crimes and do what they can to prevent crimes from happening in the future. When it comes to the power to access specific versions of

media or internet data, police practices are generally led by previous court rulings (Jackson). Theodoric Meyer discusses in his article, “No Warrant, No Problem: How the Government Can Get Your Digital Data,” the current practices in place that allow police to gain access to personal data. With the fourth amendment in the forefront of their minds, it is up to the courts to review cases regarding the legality of different police data invasion instances (Meyer).

Although not perfectly lined out, the police process helps provide a guideline on how to proceed when seeking access to a person’s private data. According to Meyer, “The electronic Communications Privacy Act (ECPA) – a 1986 law that underpins much of how the government can get digital data — requires providers to allow access to real-time data with a court order and historical data with a subpoena.” According to “Subpoenas, Court Orders and Search Warrants,” a court order is a judge issued command, a subpoena is a court issued request usually filled out by an attorney, and a search warrant is a variation of a court order that instructs law enforcement where and what to search for. While search warrants require probable cause, both subpoenas and court orders do not. They simply require a relevance to the investigation (Meyer).

As stated in the previous paragraph, much of police protocol is based on previous court rulings on similar instances of internet and media data monitoring; therefore, each ruling is determined by each situation that is encountered. While listening in on phone calls without a warrant is illegal, monitoring incoming calls, outgoing calls, and call duration does not require a warrant due to 1979 Supreme Court case Smith v. Maryland. When it comes to cellphone location data, the courts are divided as to whether a warrant is needed to access this information or not. Although some states require warrants for cellphone location data, others do not. Under the ECPA, requirements for accessing IP (Internet Protocol) addresses were vague and often contested by different political interpretations. However, the general principle was to require a

court order for real time data and a subpoena for historical records. Regarding emails, the age of the email and whether or not it has been opened determines if a court order, subpoena, or warrant is needed. The older the email, the more easily accessible it becomes. Even draft emails can be accessed with only the need of a court order or subpoena because they are seen as "stored electronic data" (Meyer). Cell phone text messages follow the same rules as emails when it comes to age determining how accessible they are. The only difference is that the phones of arrested people require a warrant to access them. Cloud data is focused on whether it is considered stored data or communication. If it is considered a communication, a warrant is usually required; however, if it is considered stored, then it is treated like draft emails and requires only a subpoena or court order. Regarding social media, the courts are still deciding whether or not to require warrants (Meyer).

The product of police access to internet data is clearly portrayed by the positive results that have emerged. August 8, 2011, marked a day that Missouri granted over $390,000 to law enforcement to aid in the fight against internet crimes in the St. Louis area per the "Department of Public Safety News Release." This clearly shows a need for police on the internet to prevent and solve crimes. Serial killer Maury Travis was arrested by federal officers who followed an intricate trail linking Travis to the murders of multiple women based on his Internet Protocol (IP) address (Simon). While both examples show the necessity of police access to private data in the St. Louis area, they also show the importance of relevant policy to help save valuable time and resources.

With adequate policies and procedures in place, police investigation of internet and media data can become as commonplace as in-person investigating. Considering the rapid advancement in technology over the past few years, there is no surprise that crime solving is

shifting online. From illegal websites of child pornography and violence, to online threats, to solving crimes – the monitoring of internet data is inevitable in preventing and solving crimes. Without law enforcement being allowed to monitor data, there would be many more serial killers and criminals continuing their crime sprees unchecked.

Although personal privacy is a hot topic right now, not everyone completely understands the importance of police having access to personal internet and media data. It is evident that police deserve the right to access this data because of their power, policy, and product in prior situations. There are many instances of crimes being both prevented and solved due to police following procedure to access a person's data. When it comes down to the countless parties that have access to personal data, police access should be the least concerning.

Ethical Dilemma Solutions:

A Moral Analysis of Revising V. Replacing the ECPA

When it comes to policy reform, there are two prominent routes that can be taken—one is to update the ECPA and the other is to repeal the ECPA and replace it with a new privacy policy. Without this policy reform, how can one be convinced that their rights are being adequately protected regarding police access to private data? To fully analyze these two possible solutions, both the teleological and deontological theories will be used to from Ronald F. White's book on ethical frameworks, Moral Inquiry.

The staff at the ACLU believe strongly that the ECPA is grossly outdated and are strong supporters of a much-needed revision to the current policy. They narrowed their list of necessary updates to the ECPA down to five essential points. With the first point being a closure of loopholes that allow electronic information to be accessed due to the age or nature of the information. The second point of change would be to require a warrant from law enforcement to

access location information. The third revision is to update all law enforcement surveillance requirements to equal that of current wiretapping policy. The fourth correction proposed is to treat electronic evidence the same as non-electronic when it comes to illegally obtained evidence being inadmissible in court. The fifth and final proposition by the ACLU staff is to mandate that the viewing of records only be allowed in emergency situations and with adequate consent and notice of involved parties (staff ACLU). It is from these five updates to the ECPA that the staff of the ACLU is hoping to narrate policies specific to law enforcement access to internet data.

In favor of repealing ECPA and enacting a new privacy act is Orin S. Kerr. He writes in his article, "The Next Generation Communications Privacy Act," how the current ECPA is so outdated that, if all necessary updates were completed, this policy would hardly even be recognizable. Kerr's four ideas for the new privacy act are as follows:

> To impose the same requirement on access to all contents, to impose particularity requirements on the scope of disclosed metadata, to impose minimization rules on all accessed content, and to impose a two-part territoriality regime with a mandatory rule structure for U.S.-based users and a permissive regime for users located abroad.

It is these four concepts that Kerr believes are necessary and sufficient to effectively govern police investigation into current levels of internet and media data (374).

The two frameworks that will aid in the ethical analysis of these solutions are the teleological and the deontological theories. White, a philosophy professor at the College of St. Joseph in Cincinnati, OH, describes the teleological theory as a moral theory focused on consequences. He writes, "…from a teleological perspective, motives really have nothing to do with the rightness or wrongness of the act" (Behrens et al. 252). By using the teleological approach, human behavior cannot be decided as right or wrong until there are consequences to

analyze. An example would be the decision to run or not to run from police when a traffic violation has been identified. Someone using this approach would weigh the extreme possible consequences on each side to determine what choice is best for them to make. The other framework discussed by White, the deontological theory, focuses primarily on duties or obligations. This approach is enveloped in the idea of specific roles that require exact responses, and distances itself from the teleological approach by looking primarily at motivations behind actions. If a person was doing their duty and acting out of good will, then those following the deontological approach would see no issue with their actions. While both frameworks have specific strengths and weaknesses and would be best utilized in accordance with one another, they are still great standards to hold ideas to in order to determine what path is best to take (Behrens et al. 253).

When looking through the lens of the teleological approach at the first solution of revising ECPA, both advantages and disadvantages come into focus. With consequences being the primary motivator of this approach, one must consider the consequences of revising a general policy that applies to all facets of internet or media data. Two positive consequences of this action would be that it is less challenging and faster to fix what is already there than it is to remove a mother policy and replace it with a new policy. As Kerr writes, “Congress rarely enacts sweeping reforms. Slow evolutionary change ruffles fewer feathers than does wholesale revision” (418). Regarding disadvantages of the revision of a comprehensive policy, the dangers of the updates still being too general and not specific enough must be acknowledged. With internet and media data advancing at such a rapid pace and being comprised of so many variations, there is no question that some things will be forgotten. This is where more revisions and additional policy will need to be made to cover specific instances. Another issue with this

solution of a generalized policy is the timeframe of the correction. If it were to be revised piece by piece, this would help with quicker results for specific categories; however, if it were to be corrected as a whole, the amount of changes required are so catastrophic that it would take a long time to get it fully approved and instated (Kerr 418). Ultimately, it appears that any solution will become quite time consuming.

When it comes to the deontological approach regarding the solution of revision or replacement of a generalized act, duty is the primary influence. It is the duty of law enforcement to carry out the laws passed down to them by the legislature, and it is the duty of the legislature to make laws that effectively protect the rights of the people. Since police are fulfilling their duties by following the policies currently laid out for them, it is the duty of the lawmakers to revise this extremely outdated law. There is no question that the protection of privacy rights by way of policy making is the responsibility of the law makers. As Kerr wrote in his article, "The vital importance of computers and the Internet tasks Congress with keeping the privacy laws up to date" (419).

Both the teleological and deontological approaches help frame the decision making in relation to this solution of revising the ECPA. When dealing with policy that is so blatantly outdated, it can be hard to know which path forward is best. While the teleological approach showed that there are both good and bad consequences that can come from this solution, it is obvious from the deontological approach that this or a similar solution is overdue and expected from lawmakers.

By using the teleological approach to look at the solution of replacing the ECPA with an entirely new policy on internet and media data privacy, we can identify some of the consequences of choosing this path as well. A great advantage to the replacement of the ECPA

would be that it would provide a clean slate on which to create policy regarding such a controversial area; thus, doing away with the outdated and, arguably, unjust allowances provided for by said document. Kerr writes, “If Congress could start fresh and enact a new statute, those changes would lead to a law very different from ECPA statute on the books today” (373). One of the big issues of the ECPA that was pointed out by both Kerr and the staff of the ACLU is the variation among the accessibility of different forms of data. Kerr discusses the solution to these discrepancies by writing how a revised statute “… would abolish ECPA's antiquated distinctions, such as the difference between real-time access and stored access…” which would require the police to “…treat all access to contents under the same warranted standard” (377). Negative consequences related to the replacement of the ECPA are the amount of time and effort it would take to repeal and reenact a new policy, as well as the margin of error that could occur due to the constant update of technology. It is by weighing these positive and negative consequences that the best decision can be made through the teleological approach.

By using the deontological approach to look at this solution one can observe the duty-based side of deciding what is the better option. When it comes to distinguishing between the lawmaker’s duty to either reform or replace policies, there is not a major difference between the two options. It is the legislative branch’s responsibility to make the laws while interpreting the rights of the people. As Alan Wheler states in his article, “The feds need to stop using a 30-year-old law to access user data online,” “Only Congress can address the shortcomings of ECPA. Only Congress can address the conflicts of law facing providers, safeguard the rights of our citizens, and ensure lawful access to suspects’ data for law enforcement.” The need for improvement simply emphasizes the importance of action on the part of the lawmakers in the United States. With little to no reform since 1986, those using the deontological approach would

begin to question the moral judgement of those who have yet to push for a change in this sensitive area.

When using both the teleological approach and the deontological approach, the solution of replacing the ECPA with a new policy can be analyzed effectively. While the teleological approach revealed both positive and negative consequences that varied from the solution of revising the ECPA, the deontological approach results fell closely in line with that of the revision solution. There is no doubt that some form of correction is needed to give the American people peace that their rights are being protected, even if the resolution involves adding more restrictions to law enforcement.

While there are groups like the American Bar Association that provide standards for police practices regarding issues like private data access, this is only a temporary fix for what is truly needed-- policy reform. When looking in the direction of ECPA reform, there are two main options—the revision of the current ECPA or the replacement of it. Both proposed solutions were analyzed using White's ethical frameworks of the teleological and the deontological theories to aid in determining the individual effectiveness levels. It is through this ethical analysis of solutions that one can effectively decide which choice would be the most beneficial to society.

Argument for the Best Solution

Improving the Future of America

With the two main solutions that have been proposed to solve this decades-old dilemma being to revise the ECPA or to repeal and replace it with another comprehensive internet privacy policy, this work will discuss which choice is the most beneficial overall. Upon using the teleological (consequences based) approach from White's book, Moral Inquiry, it becomes clear

that the optimal outcome solution concerning both police and public interests is one which strengthens the policy that currently dictates what is expected from police regarding private data. When it comes to organization, practicality, and overall timesaving, the amendment process proves to be superior to that of the replacement process. While many do argue that the replacing of this act with a new one is superior because it would provide a clean slate to work with for those in legislature, this argument falls short because of the complexity and interdependence that laws have with other laws as well as the amount of resources that would be required. It is the solution of repealing the ECPA that is more favorable than replacing the ECPA because repealing it is more organized, practical, and time conscious.

The first reason that a revision of the ECPA is better than the replacement is that a revision will aid in the overall organization of the justice system. With there already being multiple amendments and laws linked to the ECPA, this route of correction is a more ideal solution. Amending one document is much easier than having to amend and/or replace many, because they are all interconnected. As previously mentioned, the ECPA contains the Stored Wire Electronics Communications Act and is made up of three titles: Title I- the Wiretap Act, Title 2- the Stored Communications Act, and Title III- the Pen/Trap Statute. Also connected to this act are the Communications Assistance to Law Enforcement Act (1994), the USA Patriot Act (2001), the USA Patriot Reauthorization Acts (2006), the FISA Amendments Act (2008), and others all branch off of the ECPA (“Privacy & Civil Liberties”). If a repeal of the ECPA were to occur, then all these related law documents would have to be reviewed and possibly changed to reflect the new policies that would be to come. This could cause major issues for both national and local law enforcement that will be discussed further on in this paper.

The second reason that revision is a better route to take with the ECPA than replacement is due to the practicality. Massive policy reform would be detrimental in the areas of cost, training, and an overall learning curve for those affected. The amount of work that would be required to repeal, rewrite, and approve a new law as compared to simply revising one would be significantly more. Also, if a law that has been in place since 1986 was repealed and replaced with a new law, police would need to be retrained on new policy. In addition to everything already stated, there would have to be a learning curve in place for law enforcement and officials to be at a place to adequately understand and perform the new processes in place. All of these changes add up to significant amounts of time and money that would be spent to replace this act. Tom Gantert writes in, "Enacting A New State Law Costs $272,500, On Average," that "State Rep. Matt Maddock, R-Milford, had requested the analysis" that showed how "The average cost of passing a new state law in Michigan is $272,500, according to an analysis by the Legislative Service Bureau." This gives a small glimpse into the amount of effort it would take to enact a federal-level law. With just an update to one blanket document, St. Louis police will be able to save money and time by just focusing on learning specific updates instead of completely new policy.

The third reason the solution of amending the ECPA is better than that of replacing it is the overall time that would be spent on the process. The main difficulty behind instating new laws is the process of gaining support from lawmakers. The critical step of deriving a policy that obtains backing from all necessary parties can be a frustrating and extensive one. According to the article, "How long does it take to pass and enact Bills?" the average day count for each step are as follows: "153 days from introduction to adoption, 96 days from adoption to assent by President, 161 days from assent to commencement, and 410 days from introduction to

commencement." This brings us to the accumulative average of 820 days (26.96 months/ 2.25 years) to have a bill go through the full legislative process. That does not even factor in the amount of time that is now needed to train all affected personnel or repeal the ECPA. It is very evident that the solution of repealing and replacing the ECPA would prove to be a very tedious alternative. When it comes to the privacy of billions of people being protected, police and other law enforcement officials need to receive up-to-date policy as soon as possible.

Maury Travis, the "St. Louis Video Strangler," was caught primarily due to law enforcement officials obtaining a subpoena to investigate into his IP address. The 2001 USA PATRIOT ACT further defined the requirements necessary for obtaining the information required. This specific revision helped save investigators time and resources by providing them exactly what they needed to find the perpetrator (Blanco). It is updates like these that are needed more than ever regarding similar areas covered by the ECPA. It is a sobering thought to consider what may have happened if their actions were deemed unconstitutional by the court due to a lack of policy regarding this instance and instances like these. Maury Travis, and many others, may have never been caught. In another light, there is no way to know how many others have gotten away with their crimes due to a lack of policy on accessing private data. Without a revision to the ECPA, police in St. Louis and all over the nation are left to make the best decision they can without knowing if the courts will support their decisions or not.

One of the strongest arguments for the replacement of the ECPA is that it will provide a "clean slate for lawmakers to enact a very different statute" as mentioned by Orin S. Kerr in his article, "The Next Generation Communications Privacy Act" (390). He continues by saying, "As a practical matter, lawmakers rarely start from scratch when passing legislation. Amending prior laws is the norm for a variety of reasons" (Kerr 377). While there are numerous necessary

revisions to the current ECPA, removing a policy and replacing with another just for the purpose of a clean slate is not entirely justifiable. As mentioned before, the complexity of the laws that are tied to the ECPA as well as the waste of resources it would be to rework something that is already there prove how uncalled for a clean slate truly is. Although it does sound appealing to be able to start from scratch on laws that apply to the ever-growing realm of technology, lawmakers would be remiss to believe that this would be better than building on a foundation that has already been set, no matter how faulty that foundation may be. When it comes to law, revision is generally better than replacement. There are reasons the United States has never replaced the Constitution even though it is over 230 years old. It is instances like the Maury Travis case in St. Louis that help emphasize how essential it is to have a law in place regarding these situations. If the ECPA were repealed while the new law awaited approval, this case would have faced a lot of unnecessary and time-consuming problems. The takeaway from this argument of a clean slate allowing more legislative freedom is to inspire both lawmakers and citizens to ensure that they do not get cheated on the level of revising that is necessary for this document. The solution of revising the ECPA is completely ineffective if the revisions do not match the key elements that need to be addressed in the realm of internet privacy.

According to the Electronic Privacy Information Center in their article, “EPIC—Electronic Communications Privacy Act,” the “ECPA has been amended several times, but has not been significantly modified since becoming law.” The solution of revising the ECPA is the most favorable choice as it will be the most organized, practical, and time conscious. While some states such as California have already enacted their own privacy laws, the revision of this act will greatly impact both the St. Louis area as well as many others like it. When one focuses on a consequences-based (teleological) ethical approach, it becomes more apparent that the revision

of the ECPA solution has fewer negative and more positive consequences than that of the repeal and replace the ECPA solution. The argument that a clean slate or brand-new policy would be better than revising an age-old policy is tempting; nonetheless, this kind of dream does not take into full consideration the complexity and resource consumption that a solution like that would require.

It is evident that there must be a change to this outdated document, and it needs to be soon. Congresswoman Tulsi Gabbard really put the need for an ECPA revision into focus when she said,

> We live in a world where technology has changed every aspect of our lives since 1986. The Electronic Communications Privacy Act (ECPA) of 1986 needs to be updated as it reflects a world of the past that does not resemble our current online landscape. Americans ought to have a reasonable expectation of privacy for their personal and professional content stored online, and laws protecting our Fourth Amendment and digital privacy rights must be updated to reflect advances in technology that have progressed rapidly in the last three decades. (Press Release)

With updates to the ECPA, St. Louis police officers can have a well-defined policy to follow that will protect them from the dangers of vaguely outline procedures. This will also protect those that law enforcement serves from having their privacy invaded. A revised ECPA would provide courts with policy to look to instead of previous court rulings. Having an up-to-date law in place will ensure each and every citizen of St. Louis possesses the capability of knowing what their rights are concerning internet and media privacy. With the future of society and technology rapidly shifting online, it is imperative that clear and current legislation be in place to protect the civil liberties of those who call this nation “home.”

Works Cited

Alan Wehler, opinion contributor. “The Feds Need to Stop Using a 30-Year-Old Law to Access User Data Online.” 23 Oct. 2017, thehill.com/opinion/technology/356668-the-feds-need-to-stop-using-a-30-year-old-law-to-spy-on-users-online.

Blanco, Juan Ignacio. “Maury Troy Travis: Murderpedia, the Encyclopedia of Murderers.” murderpedia.org/male.T/t/travis-maury.htm

Department of Public Safety News Release. 2011, dps.mo.gov/news/newsitem/uuid/6697f760-cb94-4587-ba70-20d3ee4964bf.

Electronic Privacy Information Center. EPIC – “Electronic Communications Privacy Act (ECPA).” 2016, epic.org/privacy/ecpa/.

“How Long Does It Take To Pass And Enact Bills?: PMG.” Parliamentary Monitoring Group, 2015, pmg.org.za/page/How long.

Jackson, Brian A. Using Digital Data in Criminal Investigations. 15 May 2017, www.rand.org/blog/2017/05/using-digital-data-in-criminal-investigations-where.html.

"June 23, 2002 (Page 10 of 472)." St. Louis Post-Dispatch (1923-2003), Jun 23, 2002, pp. 10. ProQuest, http://ezproxy.umsl.edu/login?url=https://www-proquest-com.ezproxy.umsl.edu/docview/1905311156?accountid=14595.

Kerr, Orin S. “The Next Generation Communications Privacy Act.” University of Pennsylvania Law Review, vol. 162, no. 2, 2014, pp. 373-419. JSTOR, www.jstore.org/stable/24247892. Accessed 27 Oct. 2020.

“Law Enforcement Access to Third Party Records Standards.” 2013. www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/.

Meyer, Theodoric. “No Warrant, No Problem: How the Government Can Get Your Digital Data.” 27 June 2014, www.propublica.org/article/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data.

“Privacy & Civil Liberties.” Electronic Communications Privacy Act of 1986, DHS/ Office for Civil Rights and Civil Liberties and the DHS/ Privacy Office, 23 Apr. 2019, it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

Rep. Tulsi Gabbard Co-Sponsors Legislation Protecting Electronic Privacy Rights, Congresswoman Tulsi Gabbard Hawaii's 2nd District, 5 Feb. 2015, gabbard.house.gov/news/press-releases/rep-tulsi-gabbard-co-sponsors-legislation-protecting-electronic-privacy-rights.

Simon, Stephanie. “Virtual Trail Led to Serial Killer Suspect.” Las Angeles Times, 17 June 2002, www.latimes.com/archives/la-xpm-2002-jun-17-na-serial17-story.html.

“Subpoenas, Court Orders and Search Warrants.” generalcounsel.ncsu.edu/legal-topics/lawsuits-and-litigation/subpoenas-court-orders-and-search-warrants/.

Staff, ACLU. “Modernizing the Electronic Communications Privacy Act (ECPA).” 2020. www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa.

Tom Gantert | September 9, 2019. “Enacting A New State Law Costs $272,500, On Average.” Michigan Capitol Confidential, 9 Sept. 2019, www.michigancapitolconfidential.com/enacting-a-new-state-law-costs-272500-on-average.

White F. Ronald. “Moral Inquiry.” A Sequence for Academic Writing, by Laurence Behrens and Leonard J. Rosen, Pearson, NY, NY, CA, 2018, pp. 251-254.

Link to Website: https://ethicaldilemmapoliceaccesstoprivatedatast.weebly.com/intro-to-maury-travis.html