Are Third Parties Creating a Loophole for Police Investigations?

Alexandria N. Short
Are Third Parties Creating a Loophole for Police Investigations?

ALEXANDRIA N. SHORT*

This article discusses the current case law and statutory law related to the privacy of information collected by third parties. At times, we see the private sector and law enforcement working together to solve crimes. However, that may not always be a good thing. This article offers a solution to these problems of uncertainty by suggesting a uniform code to regulate the private sector, or, in the alternative, a change to the Fourth Amendment that encompasses a more modern interpretation of the information that law enforcement should have access to.

* Alexandria N. Short, J.D. Candidate at Northern Illinois University College of Law, Class of 2022. I would like to thank my Faculty Advisor, Daniel McConkie, for his guidance and support in creating this article. With his expertise I was able to create an article that encompassed two areas of law that I am passionate about. I would also like to thank my husband, Nitin Puri, for his continuous support throughout my law school career.
I. **INTRODUCTION**

Under the current laws, it is unclear whether information, voluntarily given to a third-party, is protected through the Fourth Amendment. As a proposed solution, legislation created a uniform code, or the Fourth Amendment should be refined to accommodate our new society. In Part II of this article, I will first examine current case law, established in *Carpenter v. United States*, and the most current statute, the Electronic Communications Privacy Act of 1986, related to the issue. Then, in Part III, I will discuss the advantages and disadvantages to the current legislation. Furthermore, in Part IV, I will offer a solution that is a compromise, which alleviates some of the issues, while keeping the discussed benefits intact. Then in Part V, I will make concluding remarks regarding the solution and summarize the points made in the article.
II. CURRENT CASE LAW AND STATUTORY LAW

A. CARPENTER V. UNITED STATES

In an era where technology is so vast and has significantly advanced over the years, what does "the right of the people to be secure in their persons, houses, papers, and effects..." in the Fourth Amendment mean? Generally, the Fourth Amendment has been interpreted to protect a person's personal property from unreasonable searches and seizures. However, this protection excludes any searches or seizure of property that does not belong to the individual. Therefore, any other information put out into the world seems to be fair game for the authorities, including information obtained by third parties.

Thinking about the devices we use on a daily basis, it seems reasonable to believe there is an expectation of privacy in that stored information. For example, a cellphone goes everywhere with us, tracking locations, listening to conversations, and storing photos, passwords, and documents. Thinking about anyone—not just the authorities—having access to all of this information, regardless of whether you have anything to hide, sends shivers down the spines of many. This constitutional “expectation of privacy” hinges on a multifaceted analysis that does not seem to resolve the issue at hand.

Recently, in the case U.S. v. Carpenter, four individuals were caught in connection with the crime after a series of armed robberies. After interrogating the individuals, the FBI obtained the phone numbers of the potential robbers. The FBI then sought a court order to search through the personal data that the cell service company had on file in connection with these phone numbers. With the court order, the FBI was held to a much lower standard than probable cause, only having to show “reasonable grounds” that the records were “relevant and material to an ongoing criminal investigation.” This meant that law enforcement only needed to show that the information “might be pertinent to an ongoing investigation—a 'gigantic' departure from

1. U.S. Const. amend. IV.
3. Id.
4. Id.
9. Id.
10. Id.
11. Id. at 2221 (citing 18 U.S.C.S. § 2703).
the probable cause rule.” After receiving the court order, the cell service company was compelled to release the cell service data to the authorities.

The Supreme Court of the United States came to the conclusion that this was an unreasonable search. The court reasoned that the FBI was required to obtain a warrant, not a court order, requiring the police to obtain probable cause prior to the search of these records. The Supreme Court explained that, although the cell phone records are not the property of the Defendant, he still had and expectation of privacy due to the intimate nature of location tracking “revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” This is an abrupt change from the already well established third-party doctrine, an extension of the Fourth Amendment, allowing law enforcement to search any personal information given to third parties. Although the approach is a step in the right direction when protecting our information further, it certainly has its flaws.

As described by the dissenting opinion, this analysis puts the law on a “new and unstable foundation.” This approach is subjective and does not account for further technological developments or personal interpretations of the lower courts. The approach evaluates several variables such as the “intimacy, comprehensiveness, expense, retrospectivity, and voluntariness” to evaluate whether there is a reasonable expectation of privacy. All of these factors are entirely subjective and can be interpreted in many different ways, thus creating different outcomes from court to court.

Carpenter v. United States also fails to overrule other primary cases concerning the same issue including United States v. Miller and Smith v. Maryland. In both cases, there was no expectation of privacy for

---

12. Id.
14. Id.
15. Id.
16. Id.
information given to third parties.\footnote{22} This is confusing, considering the ruling in Carpenter v. United States says the exact opposite.\footnote{23} In United States v. Miller, the information shared with the Defendant’s banking institution was found to be unprotected by Fourth Amendment searches.\footnote{24} The Supreme Court acknowledged that a depositor “reveals many aspects of his personal affairs, opinions, habit and associations” to their bank, providing a “virtual current biography” to a third party.\footnote{25} Additionally, the “bank’s ownership of records permits free access to them by any police officer.”\footnote{26} Similarly, in Smith v. Maryland, the Supreme Court found that the Petitioner voluntarily gave information to his cellular provider when he dialed a phone number.\footnote{27} The Supreme Court reasoned that the Petitioner “assumed the risk that the company would reveal to police the numbers he dialed.”\footnote{28} Yet, the Supreme Court in United States v. Carpenter does not overrule these cases.

As a result, United States v. Carpenter does not address the issue of whether stored, third-party information is protected by the Fourth Amendment.\footnote{29} Instead, this case raises several questions, especially considering the technological changes. For instance, if we assume the facts are the same as Carpenter v. United States, what happens if a third-party comes to the police with information?\footnote{30} What if the police purchase the third-party data?\footnote{31} There is also no expansion on the other technologies to which Carpenter’s holding may apply.\footnote{32} In United States v. Carpenter, the court only speaks of a technology that tracks location.\footnote{33} This does not answer whether data from DNA analysis, social media, and voice activated assistants are equally as invasive and give an individual a reasonable expectation of privacy.\footnote{34} Overall, this
case decides merely on the specifics of the case and controversy, but does not make the issues any easier to resolve.\(^{35}\)

With this case, it is apparent that the right to privacy can be vague and uncertain at times. The uncertainty of privacy has only become more confusing as years have passed and technology has evolved.\(^{36}\) Along with the growth in technology, there has been a growth in personal data sharing with major companies.\(^{37}\) Today, consumers share some of their most intimate information with companies.\(^{38}\) For example, companies such as Amazon have entered the homes of so many individuals allowing the third party to know everything from shopping preferences, to in-home conversations, to home security surveillance.\(^{39}\) This technology gives companies enormous databases of personal information that consumers have willingly handed over.\(^{40}\) But it is uncertain whether this information, voluntarily given to a third-party, is protected through the Fourth Amendment. This includes whether the information can reasonably be expected to be private and under what circumstances does the law permit police to use this information as a tool for investigations.

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) OF 1986

The most recent legislation used to address the issues from \emph{Carpenter v. United States} is The Electronic Communications Privacy Act (ECPA) of 1986.\(^{41}\) The act is split into the Wire Tap Act (WTA)\(^ {42}\) and the Stored Communications Act (SCA).\(^ {43}\) The WTA focuses on communications that are

---

35. Tokson, supra note 18.
37. Tokson, supra note 18.
38. \emph{Id.}
39. Amazon.com Privacy Notice, \emph{AMAZON}, https://www.amazon.com/gp/help/customer/display.html/ref=s9_acss_bw_cg_usccpa_4a1_csa_w?nodeId=466496&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=merchanised-search-1&pf_rd_r=F9IY1DKS1NT5D5595CB8&pf_rd_t=101&pf_rd_p=6db4e803-6e6e-461-987d-898640e18e&pf_rd_i=209070110111#GUID=8966E75F-9B92-4A2B-BF5D-967DS513A40 SECTION_87C837F9CCD54769B4AEB14AF4F01 (last updated Jan. 1, 2023) [https://perma.cc/TP6E-H8C6].
40. Alton, supra note 30.
42. 18 U.S.C. § 2510.
43. 18 U.S.C. § 2701.
happening in real-time.\textsuperscript{44} Whereas, the SCA focuses on communications that have already occurred and can be reviewed later.\textsuperscript{45}

Regardless of which act is violated, it is essential to note that not all technology fits into these two categories.\textsuperscript{46} Especially since the "key technologies" that have been identified include only e-mail, website access, voicemails, voice activated assistants, keyboard or other computer input, and previously recorded information.\textsuperscript{47} This is not an exhaustive list, but it certainly "dates" the statute. This list of "key technologies" does not account for communication passed through video calls or encryption.\textsuperscript{48} Also, there is no clear definition of what constitutes a communication.\textsuperscript{49} Therefore, the best law available does little to protect some of our most intimate information. The DNA sent in to 23andMe, or the facial and fingerprint scan on an iPhone, likely cannot be protected by the ECPA.\textsuperscript{50}

With the uncertainty caused by the ECPA, courts have ruled differently on similar cases due to the complications of applying an act from 1986 to the technology of today.\textsuperscript{51} For example, in Hately v. Watts, the court, to understand the plain meaning of the statute, went through several definitions of terms such as, "protect", "backup", and "copy."\textsuperscript{52} Ultimately, the court decided that emails, opened and delivered, are electronic storage within the meaning of the Act.\textsuperscript{53} Whereas, in United States v. Weaver, it was decided that opened and delivered emails did not fit into the meaning of electronic storage.\textsuperscript{54}

In addition, the court in Carpenter v. United States mentioned the inapplicability of this law to new technology. After the FBI obtained the phone numbers of the suspects, they sought a court order to search through the

\textsuperscript{44} Michael E. Lackey, Jr. et al., \textit{Electronic Communications Privacy Act (ECPA): Key Issues}, MAYER BROWN LLP, https://plus.lexis.com/api/permalink/dadf0ec9-5aab-4b8c-a143-c20a2884ae61/?context=1530671 (last updated May 6, 2022) [https://perma.cc/828J-56EE].

\textsuperscript{45} Id.

\textsuperscript{46} Id.

\textsuperscript{47} Id.

\textsuperscript{48} Id.

\textsuperscript{49} Lackey, Jr. et al., \textit{supra} note 44.


\textsuperscript{51} Hately v. Watts, 917 F.3d 770, 790–98 (4th Cir. 2019) (finding that previously opened and delivered messages stored in an email to client were in electronic storage for purposes of the SCA); United States v. Weaver, 636 F. Supp. 2d 769, 771–73 (C.D. Ill. 2009) (holding previously opened messages not in electronic storage for purposes of the SCA).

\textsuperscript{52} Hately, at 790–98.

\textsuperscript{53} Id. at 770.

\textsuperscript{54} United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009).
personal data that the cell service company had on file. This court order was obtained through the Stored Communications Act, which states:

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

The FBI was told that they must show “reasonable grounds” before obtaining the court order that falsely implicated Carpenter. But, as stated by the court, “reasonable grounds” is not sufficient when it comes to a search classified as a Fourth Amendment search. The court explains that a Fourth Amendment search requires the FBI to show probable cause, a much higher standard to obtain a warrant, not a court order. The court states that when there is a search into data as sensitive as geographical location, there must be probable cause to support the search of information that an individual can expect to be private, and that the public would deem to be a reasonable expectation of privacy. The SCA became the main cause for this case and controversy, demonstrating how confusing the statute can be and the issues it creates.

These flaws with the current form of the ECPA demonstrate a real need for updated legislation. The courts do not have a certain path to follow with the current statute, and law enforcement is forced to apply the statute to new cases. Additionally, it does not resolve the issue whether information voluntarily given to a third-party is protected through the Fourth Amendment.

III. OUTSOURCING ASSISTANCE VIA PRIVATE ORGANIZATIONS

Outsourcing to third-party organizations is when law enforcement solicits information from a company because they believe there is information in the possession of the third party that may lead to an arrest. Third-parties

56. 18 U.S.C.S. § 2703(d).
58. Id.
59. Id. (quoting Smith v. Maryland, 442 U.S. 735 (1979)).
60. MALCOLM K. SPARROW, U.S. DEP’T OF JUST., NAT’L INST. OF JUST., NEW PERSPECTIVES IN POLICING: MANAGING THE BOUNDARY BETWEEN PUBLIC AND PRIVATE
do not have to be private organizations, but this is where the article will primarily focus. The private sector encompasses large corporations such as Apple, Google, Facebook, and Microsoft. The private sector also consists of private individuals or non-profit organizations and volunteers. When law enforcement works with the private sector, it can be due to a lack of resources, whether that is money, information, skills, or expertise. Law enforcement could use the private sector as a mechanism to bypass judicial processes and oversight that come with trying to obtain a warrant. When law enforcement has insufficient information to make a search or an arrest, it is much easier to consult the private sector and obtain the information required to meet the standard of probable cause. Although it is currently unclear whether information voluntarily given to a third-party is protected through the Fourth Amendment, there are many advantages and disadvantages that arise from current legislation, which is important to understand when proposing a possible solution to this issue.

A. ADVANTAGES

The outsourcing of information to third parties by law enforcement, has proven itself to be useful for many reasons. Allowing law enforcement access to the information of private organizations has led to many societal benefits in terms of crime solving. It has also, at times, resulted in a better public image for the private companies willing to be open with the police.

i. Expedited/Efficient Crime Solving

One of the benefits of allowing the private sector to assist in investigations is a more efficient crime-solving technique. When a crime has occurred, it is essential that the police gather as much information because they are then responsible for identifying and apprehending the criminal before another

61. Id.
62. Id.
64. Id.
65. SPARROW, supra note 60.
66. Id.
crime occurs.68 However, there are limited resources, preventing law enforcement from effectively protecting the community. With limitations in the public sector, it is understandable that the number of unsolved crimes has continued to grow at an “alarmingly rapid pace.”69 With assistance from the private sector, however, law enforcement is able to mitigate these limitations.

A current limitation exists with the law enforcement’s use of a program named CODIS (Combined DNA Index System). This program was developed by the FBI to identify DNA profiles across the nation.70 But a major limitation of this program is that it only works to identify a suspect if they are already in the DNA Index.71 The DNA Index consists of DNA submitted from either a previous arrest or incarceration. This means that law enforcement is limited to a database of individuals who have prior criminal records. Therefore, if the suspect is a first-time offender, or a serial offender who has never been caught, law enforcement is at a dead-end.72

Due to this limitation, several police departments began to use private companies and their databases. Companies such as GEDmatch, 23andMe, and Ancestry have allowed the police to use the DNA of their consumers to do genetic searches based on all the consumers who have paid to have their DNA evaluated.73 As a result, law enforcement’s access to DNA profiles has increased, broadening the search to those who may not have been incarcerated or arrested in the past. When law enforcement submits a suspect’s DNA into a private database, law enforcement can find the suspect based on close matches, such as a partial match to a parent, sibling, or cousin.74 This has allowed law enforcement to solve crimes through familial connections, crimes that may have otherwise gone unsolved.75 It has also created a more efficient crime solving technique.


71.  Id.


73.  Id.

74.  Id.

For example, in a case where DNA was found at the scene, police were limited in their ability to analyze the DNA evidence through CODIS.\textsuperscript{76} After multiple searches, law enforcement could not find a match to the perpetrator who had not been caught for nearly 30 years despite a multitude of heinous crimes.\textsuperscript{77} Once more information became available about DNA and services such as GEDmatch became available, however, the perpetrator was finally caught in 2018.\textsuperscript{78} GEDmatch, by 2010, had created and built up its DNA database via its consumers, which led law enforcement to a more efficient crime solving technique.\textsuperscript{79} Not only has this type of information sharing helped solve crime, but it has also prevented future crimes as well.

\textit{ii. Preventing Future Crimes}

Since law enforcement started to work with the private sector, there has been a significant deterrence effect, making offenders aware that the chances of getting caught are much higher.\textsuperscript{80} Not only is the private sector offering information, it is also offering products specifically designed to cater to police departments. For instance, companies such as Media Sonar Technologies, Inc. have offered police a way to analyze different social media platforms and focus their surveillance on specific individuals.\textsuperscript{81} The program called Media Sonar also identifies certain trends of violent language and inappropriate images that are alarming when brought together.\textsuperscript{82} This allows law enforcement to identify potential issues before they arise, with the help of algorithms and analysts.

As an example, in Iowa, Jasper County was utilizing a program, similar to Media Sonar Technologies, called Zencity.\textsuperscript{83} In Jasper County, there was

\begin{flushleft}

\textsuperscript{77} Id.

\textsuperscript{78} Id.

\textsuperscript{79} About GEDmatch, GEDMATCH, https://www.gedmatch.com/about-us [https://perma.cc/838Q-YRCT].


\textsuperscript{81} Johana Bhuiyan & Sam Levin, \textit{Revealed: the software that studies your Facebook friends to predict who may commit a crime}, THE GUARDIAN (Nov. 17, 2021, 6:00 PM), https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager [https://perma.cc/FBD9-DQVV].

\textsuperscript{82} See MEDIA SONAR, https://mediasonar.com [https://perma.cc/KFA2-53NR].

\textsuperscript{83} Sidney Fussel, \textit{This AI Helps Police Monitor Social Media. Does It Go Too Far?}, \textsc{Wired} (July 6, 2021, 8:00 AM), https://www.wired.com/story/ai-helps-police-monitor-social-media-go-too-far/ [https://perma.cc/Y2A3-SR46].
\end{flushleft}
a recent killing of a 44-year-old African American man in Grinnell, Iowa.\textsuperscript{84} This man lived in a predominantly white neighborhood, causing residents to believe the attack was racially motivated.\textsuperscript{85} This rumor started to spread rapidly on social media. This rumor caused great concern among law enforcement. Especially since the police department knew that the town did not have the resources to handle a potential attack or large protest.\textsuperscript{86} Luckily, through the data collected from Zencity, county officials were alerted to this rumor and were able to hold a press conference with the true details of the case.\textsuperscript{87} The societal upset was a trend identified by Zencity, which allowed county officials to act quickly and de-escalate any potential threats.

There are also products, designed for the public, that also assist police through the connection with the private sector. For instance, a business that has been successful in utilizing the public to collect information and channel it to the police is the Citizen Application, created by sp0n, Inc.\textsuperscript{88} This application allows users to report an incident and upload information about a potentially dangerous situation.\textsuperscript{89} This information can be submitted in the form of photographs, videos, or even live feeds, allowing others to tune in and steer clear of the area, preventing any further harm.\textsuperscript{90} This coalition of forces between the private companies, private individuals, and law enforcement is something new that has revolutionized the efficiency of crime solving and prevention.

B. DISADVANTAGES

Although there are plenty of benefits to the cooperation of the private sector and law enforcement, it does not come without criticism and genuine concerns. Under the current laws, it is unclear whether information voluntarily given to a third-party is protected through the Fourth Amendment, making the application of such laws confusing and relatively far-fetched when applied to current day situations. This cooperation then leads to consequences in the form of additional costs, societal upset, and distrust of law enforcement.

i. Consent and Privacy Concerns

With the cooperation of law enforcement and third parties comes a variety of consent and privacy concerns. Consumers are beginning to realize

\begin{itemize}
  \item \textsuperscript{84} Id.
  \item \textsuperscript{85} Id.
  \item \textsuperscript{86} Id.
  \item \textsuperscript{87} Id.
  \item \textsuperscript{88} Citizen, https://citizen.com [https://perma.cc/8MQE-SGW9].
  \item \textsuperscript{89} Id.
  \item \textsuperscript{90} Id.
\end{itemize}
how much information private organizations have about them.\textsuperscript{91} These private companies, like Facebook or Apple, have the most ubiquitous forms of technology. They have quickly made their products essential to daily life, leaving consumers without true consent or privacy.\textsuperscript{92} Although the goods and services of the private sector have become societal needs, the law has yet to catch up completely with how these companies can elicit consent and distribute data.\textsuperscript{93}

One of the most common forms of “consent” that the private sector uses is the acceptance of terms and conditions and a privacy policy.\textsuperscript{94} This acceptance is meant to satisfy consent under the Fourth Amendment, granting law enforcement access.\textsuperscript{95} Arguably, an individual gives consent by agreeing to the terms and conditions, which may include the distribution of private information.\textsuperscript{96} However, it is difficult to argue that a consumer has truly consented, especially when we know that the terms and conditions often go unread.\textsuperscript{97} The lengthy terms are a tool made by the private sector to gain consent on behalf of the consumer.\textsuperscript{98}

Additionally, it is well known that an individual’s needs factor into their decision to “consent.”\textsuperscript{99} Societal needs have changed greatly since the 80’s, which is not reflected in current legislation.\textsuperscript{100} As stated prior, the private sector has created necessities, through their goods and services, and it is

\begin{flushleft}


95. United States v. Matlock, 415 U.S. 164, 177 (1974) (the court found that voluntary consent is not limited to proof that consent was given by the defendant, but may show that permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or items to be inspected).


98. Sobh, supra note 96, at 630 (discussing the circumvention of privacy interests in genetic data by claims that a person who exposes their DNA to a company or website that collects and analyzes DNA has undermined their privacy interest).

99. Cakebread, supra note 97.

\end{flushleft}
unlikely someone can obtain them without agreeing to the terms.\textsuperscript{101} For example, before creating a Facebook profile to communicate and share updates with friends, the user must accept the terms.\textsuperscript{102} Similarly, with an iPhone, the consumer is continually put in a situation where the terms are changing with each update, forcing the consumer to decide whether to throw out their expensive phone, or consent to the terms.\textsuperscript{103} When the only other option is to go without a computer or cellphone service, a few basic needs, people will gladly accept the terms.\textsuperscript{104} Consumers are not given the option to opt-out when it comes to the majority of these businesses, and it is unfair to assume there is true consent, when the only other option is to live off-the-grid.\textsuperscript{105} Therefore, when consumers agree to the terms and conditions, it is certainly not “consent” under the Fourth Amendment. A better term for this type of consent would be “coerced consent,” from a business that knows you need them more than they need you.

These issues seem to arise on a regular basis now. For example, Apple has found itself, for many years, sharing private consumer information with the authorities.\textsuperscript{106} More recently, Apple was discovered to have shared private information of government officials, and their family members, at the Trump Administration’s request.\textsuperscript{107} However, this information was not necessarily shared willingly.\textsuperscript{108} Through a variety of vague subpoenas, companies have been forced to hand over data, even if it means losing the trust of their customers.

Apple has received criticism from consumers, questioning whether the information on their device is actually private.\textsuperscript{109} Apple claims that they do not give up information willingly and that they have a difficult time being put in between the law and their consumers.\textsuperscript{110} These requests to view user records are ultimately justified by, what the attorney general calls, policies that have “existed for decades.”\textsuperscript{111} However, companies like Apple have started to resist such warrants due to the increase in vague and broad warrant

\begin{flushright}
\textsuperscript{101} \textit{Id.}
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{103} Cakebread, supra note 97.
\end{flushright}

\begin{flushright}
\textsuperscript{104} Editorial Board, supra note 102.
\end{flushright}

\begin{flushright}
\textsuperscript{105} Id.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{107} Id.
\end{flushright}

\begin{flushright}
\textsuperscript{108} Id.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{110} Nicas et al., supra note 106.
\end{flushright}

\begin{flushright}
\textsuperscript{111} Id.
\end{flushright}
submissions that are in violation of the Fourth Amendment, but are still enforced by the courts.\textsuperscript{112} Apple has a reputation of being the best advocate for consumer protection, but they have also gained a reputation for being hypocrites in this regard.\textsuperscript{113} There have been concerns about Apple’s true intentions behind fighting warrants with each request.\textsuperscript{114} For example, Apple may choose to avoid a police investigation, but inquire when the police are inevitably able to get the information on their own. This brings into question Apple’s true ability to maintain consumer privacy, if it can be easily worked around by the police.

Not only Apple’s abilities, but also Apple’s intentions come into question. Especially, in light of recent news of an iPhone update that “tears at the heart of privacy of individual citizens.”\textsuperscript{115} With this new update, Apple has created a unique tool in reporting criminal activity by scanning information on iPhones. However, this new technology seems to contradict the message they portray in the media, vowing to protect consumer data at all costs, regardless of whether it will help investigations.\textsuperscript{116} The new technology that Apple will deliver within the next year, via an iPhone update, will essentially scan photos uploaded to the Cloud and identify any traces of Child Sexual Abuse Material (CSAM).\textsuperscript{117} This update will come with the regular terms and conditions, requiring every iPhone user to accept, or risk an inferior operation of the phone.\textsuperscript{118} Although there is a great advantage to collecting this information and putting away criminals, it demonstrates how easily the private sector can force users to consent and collect data, to be handed over to law enforcement, or anyone else for that matter. It also exploits how companies such as Apple may seem like the gold standard for consumer privacy but are actually trying to keep the public happy and distracted from their true intentions. Although, good intentions do exist, this is a slippery slope. If Apple

\begin{itemize}
  \item[\textsuperscript{112}] GeoFence Warrants and the Fourth Amendment, 134 HARV. L. REV. 2508, 2513-14 (2021).
  \item[\textsuperscript{113}] Bogost, supra note 109.
  \item[\textsuperscript{117}] Siddique, supra note 115.
  \item[\textsuperscript{118}] Id.
can be so coercive as to scan personal devices and turn individuals into law enforcement, there is no stopping other companies from doing this too. This shift may ultimately lead to the private sector doing the majority of policing.

There has also been concern with data sharing that may involve more sensitive information such as DNA.\(^{119}\) Companies such as GEDmatch have agreed to fight the vague warrants and subpoenas as well.\(^{120}\) Primarily in order to maintain trust between them and their customers.\(^{121}\) Although, there is nothing stopping GEDmatch from changing the terms and conditions in the future.\(^{122}\) After all, they are a private profit-based company that makes money through their distribution of information to crime labs.\(^{123}\) Also, GEDmatch only recently made the change in their policy, adding an “opt-in” option for the sharing of DNA to law enforcement.\(^{124}\) This occurred after nine years of GEDmatch sharing data with law enforcement without the true consent of consumers.\(^{125}\)

Overall, consumer privacy laws have contributed to a loophole in the justice system. Allowing law enforcement to circumvent the consent requirements of the Fourth Amendment. In the absence of any legislation relevant to a modern society, consumers will be shown again and again how their data is used against them. This will result in consumers becoming less likely to comply or associate with the private sector and this type of data collection. This would be truly unfortunate, losing the data that has been so valuable.\(^{126}\) The Supreme Court of the United States has blatantly recognized a high standard related to the invasion of one’s privacy.\(^{127}\) Yet, consumers are still losing their constitutional rights for merely making an account or buying a product.

---

119. Rosen, supra note 72, at 208.
120. Id.
121. Id.
122. Id.
123. Id.
124. Nila Bala, We’re Entering a New Phase in Law Enforcement’s Use of Consumer Genetic Data, SLATE (Dec. 19, 2019, 7:30 AM), https://slate.com/technology/2019/12/gedmatch-verogen-genetic-genealogy-law-enforcement.html [https://perma.cc/9DDT-F2GR] (“With no legal regulations providing clarity on how and when genetic genealogy should be used to fight crime, we have left private entities in charge of the decision-making.”).
125. Id.
ii. Associated Cost

Another area of concern is the cost associated with some of these databases.128 Today, law enforcement typically does not have extra money to spend on external resources.129 This is even more true in an era where police reform and defunding the police have become real topics of discussion, placing more strain on already strained budgets.130 Yet, law enforcement still chooses to invest in programs offered by the private sector due to its value.

For example, the Los Angeles Police Department spent $73,000 for a database created by Media Sonar Technologies, Inc.131 The hefty price tag shows how much value law enforcement places on this software, which assists in the prevention of future threats or incidents.132 In addition to monetary costs there is a societal cost as well. The software is used primarily for surveillance purposes.133 Watching people online to prevent crime is controversial and may lead to unnecessary societal upset, especially since research has demonstrated that this type of surveillance does not necessarily amount to any true threats to the public.134 Therefore, it would be risky to implement this type of technology across the nation.

Societal and monetary costs also stem from companies who outsource their data from the public.135 This includes applications such as Citizen,
formerly known as Vigilante in 2016.136 As the previous name suggests, there is a huge cost when police departments support these sources of information.137 The potential danger to citizens attempting to intervene or capture evidence in the moment is a real danger that has a huge liability, which is probably why Apple had to remove it from their app store when it was named Vigilante.138 On the app, individuals are encouraged, and some are even paid, to gather information and upload it to the application.139 The company prides itself on the protection of others; however, encouraging this type of data collection leads to a variety of vigilante efforts that could end up being more costly.

For example, there is a risk of people being hurt by each other or the possible criminal.140 There are risks of people accusing the wrong person of a crime, thus, ruining a person’s reputation.141 There are also risks that criminals, after not being handled properly, go free only to commit more crimes.142 These dangers, that Citizen seems to indirectly advocate for, are costly in terms of delivering public safety and proper justice.

iii. Shared Information May be Inaccurate or Biased

In addition, accuracy of certain information, and the potential biases involved, is another area of concern. For example, in 2014, a man named Michael Usry was connected, through the popular database Ancestry.com, to a homicide.143 However, after multiple hours of interrogation and being forced

137. Kimmel, supra note 135.
to provide his DNA, the results were not a match to the DNA found.\textsuperscript{144} Unfortunate situations such as these have made individuals more wary of the potential outcomes of this technology for fear that they may be accused of a crime they did not commit.\textsuperscript{145} There have also been a series of evidence mishandlings where the bias of police or third parties have influenced or changed evidence based on their desired outcome.\textsuperscript{146} This fear has only grown and become more evident through movements, such as Black Lives Matter, making it clear how widespread the mistrust of the police has grown.\textsuperscript{147}

This is a very big and unfortunate hurdle that police need to overcome in order to have better access to valuable information. However, there is a valid fear that the police are working against innocent citizens, especially against citizens of color who are punished more severely and more often.\textsuperscript{148} For example, certain developments in technology, like Zencity, have been used to target people of certain races.\textsuperscript{149} This has led to law enforcement surveying individuals based on race without probable cause before any crimes are ever committed.\textsuperscript{150} This is, again, another essential component of the Fourth Amendment, which requires the police to have a reason before searching through private information. This constitutional disregard causes the consumer to have valid concerns about their privacy. It alludes to how other countries, such as China, survey their citizens, so much to the point that freedom of speech and expression is chilled, out of fear for the potential consequences.

\section*{IV. Alleviating the Issues and Maintaining the Benefits}

Under the current laws, it is unclear whether information voluntarily given to a third-party is protected through the Fourth Amendment. Although a solution is required, it would be unfortunate to lose the benefits that can come from the use of third-party information. Therefore, as a solution, legislation must be reevaluated to create a uniform code to be adopted across the nation, or the Fourth Amendment should be refined to accommodate our new society.

\begin{itemize}
\item[]{144. \textit{Id.}}
\item[]{145. \textit{Id.}}
\item[]{146. \textit{Id.}}
\item[]{147. \textit{BLACK LIVES MATTER}, https://blacklivesmatter.com (last visited Jan 15, 2022) [https://perma.cc/59C2-DH4N].}
\item[]{149. Fussell, supra note 83.}
\item[]{150. \textit{Id.}}
\end{itemize}
A. UNIFORM CODE

There must be an updated and uniform system for addressing the concerns that individuals have regarding the protection of their data. The type of collection and distribution of information is variable from state to state and company to company, such that a more uniform system is essential. The European Union, for example, has been able to implement a more modern statute related to consumer data privacy that is uniform across the entire continent. This is an opportunity for the United States to implement the same program and potentially evolve it into something new. There can no longer be a reliance on laws that have “existed for decades” to justify taking away fourth amendment rights.

Under the Fourth Amendment, there is a requirement for police to have probable cause before they can obtain a warrant to search and seize potential evidence. As stated, there still exists a major loophole within the private sector that allows the private sector to present any information in their legal possession to law enforcement. A contributory factor to this unregulated spread of information comes from the absence of appropriate legislation. It may or may not be surprising to know that there is no uniform federal law that regulates the storage and sharing of consumer data. There are a mix of laws from state to state, but nothing that meets the needs of the entire nation. Nationwide legislation is one of the only solutions that will control the companies that exist in many different states but reach and impact a huge population across the entire country.

The European Union, a huge international community across the world concerned about their rights, recognized a need for such laws by implementing the General Data Protection Regulation (GDPR), which requires "companies to ask for some permissions to share data and gives individuals rights to access, delete, or control the use of that data." Enacted in 2016, and enforced in 2018, the GDPR was established in response to an ever-growing need to update the laws related to consumer data.

---

151. Fritsvold, supra note 67.
153. Fritsvold, supra note 67.
154. Nicas et al., supra note 106.
155. SPARROW, supra note 60.
156. Klosowski, supra note 152.
157. Id.
privacy.159 The European Union found that the legislation from 1998 was an outdated law that no longer met the needs of individuals, regularly interacting with nationwide and worldwide companies.

The United States is in a similar situation that the European Union was in as well. The United States has seemingly ancient laws that are in fact much older than 1998. It has been stated repeatedly that the United States can no longer rely on consumer protection laws that have not been updated since the 1980s.160 The United States must take into consideration a law similar to GDPR. However, it may be difficult to reverse the way companies currently store and exchange data. For instance, it took the European Union two years to make the adjustment before the law could be enforced.161

On the other hand, it is not impossible since most of the big corporations in the United States do business internationally. Companies that do business internationally have already been required to adopt the GDPR.162 Therefore, it would not mean starting from scratch completely like the European Union. The transition could have a foreseeable shorter timeline than when the GDPR was first created. Most of the major corporations have already implemented these regulations across the world and could facilitate a smoother transition. Although this type of legislation will resolve some of the issues, it will not resolve everything.

A part of the GDPR that is concerning is the level of discipline applied to companies who do not comply. For example, Google was fined for various instances of non-compliance.163 However, they were only fined a mere €50 million, which in the United States is about $57 million.164 This is a hefty price to pay for a violation, but it does not seem like much when billed to a trillion-dollar company.165 A more meaningful punishment for this behavior would consist of a heavier fine166 or a sort of injunction167 to prevent

160. Nicas et al., supra note 106.
161. Burgess, supra note 159.
162. Klosowski, supra note 152.
163. Burgess, supra note 159.
164. Id.
companies like Google from profiting through these practices that are not in line with legislation.

There is no reason for the United States to avoid the adoption of this type of legislation. The more conservative side of the United States may not be very enthused to adopt this type of legislation.\textsuperscript{168} It may be viewed as an anti-capitalist approach and create an economic downturn initially. However, when the legislation protects everyone’s information from being shared, these results will plateau and prove that there are protections with both conservative and democratic ideals in mind. Topics such as consumer privacy quickly become bipartisan issues, depending on where the conversation leads. However, this type of legislation, over time, could foreseeably garner bipartisan support. Considering conservative values related to the collection of consumer data, such as China’s collection of information through social media, it could reasonably become a stance that both parties can align with long term.

In addition, for any issues that may arise, companies that do business internationally already know how the GDPR is implemented and are likely aware of any flaws.\textsuperscript{169} These companies can be of great assistance in terms of how the United States implements any new legislation, giving their input on areas of improvement. With this new legislation, features such as the opt-in or opt-out option will be available, in addition to a notification system to alert individuals of investigations, and give individuals the ability to see what information exists between these companies, allowing them to choose whether to keep it or have it erased. This puts the individual in control of their information that is shared from company to company. Although it may still be unclear whether information voluntarily given to a third-party is protected through the Fourth Amendment, at least individuals will have more control over their personal data and the private sector will be held accountable for any violations.

B. REFINING THE FOURTH AMENDMENT

i. Consent

In the alternative, a second solution could be achieved by amending and refining the Fourth Amendment. In order to alleviate some of the concerns that individuals have, it would be best to refine the meaning of consent. Although consent is not explicitly stated in the Fourth Amendment, it states that


\textsuperscript{169} Lackey, Jr. et al., supra note 44.
there is a “right of the people to be secure in their persons.” 170 This can reasonably interpreted as allowing individuals to have a choice in the matter of whether their information is searched by law enforcement. If the idea of consent is changed to fit into our modern society, it would take into account the “coerced consent” by the private sector, not only by law enforcement.

The issue of consent can be resolved in many ways. For example, areas of the private sector have used an opt-in option that does not automatically consent until the consumer reads the information and chooses to share their information with law enforcement. This option also does not punish the consumer in any way for choosing to opt-out.

This is a feature that should be implemented with all private organizations, instead of collecting and distributing the information then having the consumer find out about it later, which only contributes to further mistrust of law enforcement and the private sector. Giving individuals a more active form of consent can help both the individual giving them the option to be “secure in their persons” or be open with law enforcement. 171

This may not be a popular option, considering companies are able to do a lot more with information if all consumers are opted-in to begin with or given no choice. 172 However, there is still a more ethical view of companies that allow this option. 173 Also, the number of individuals who choose to opt-in, according to research, is still significant and has less of an effect on profits. 174 Lastly, if all companies can comply on a uniform level, this could become the norm and lead to better legislation in the future.

In addition, it will create, most importantly, an opportunity for real consent from individuals. We cannot continue with the current version of the Fourth Amendment. Consent is a key element of the Fourth Amendment. Therefore, it must be refined to consider the way consent and information given to third-parties has evolved. If the Fourth Amendment is changed, it could also lead to a change in the third-party doctrine, which is outdated in terms of consent as well.

**ii. Ownership of persons, houses, papers and effects**

Under the Fourth Amendment, individuals are only protected from an unreasonable search and seizure if a reasonable expectation of privacy exists.
with the property in their possession.\textsuperscript{175} With the private sector collecting personal data at such a large scale\textsuperscript{176} via the goods and services essential to modern society,\textsuperscript{177} it is important to know whether these companies are keeping this information private since they are the technical owners of this property.\textsuperscript{178} Private actors are not bound to the same constitutional restrictions as law enforcement,\textsuperscript{179} giving them the freedom to expose any data they have on an individual.\textsuperscript{180} Left exposed is a major loophole, giving law enforcement everything they need to assert probable cause and make the arrest, skipping over various procedural steps.\textsuperscript{181}

Since the private sector is not required by the Constitution to keep all the collected information private,\textsuperscript{182} there is no consideration of whether the information could reasonably be expected to be private,\textsuperscript{183} depriving the individual of their rights. The reasonable expectation of privacy only comes into play when the government, either state or federal, conducts a search.\textsuperscript{184} This allows any private entity to assist and participate in any investigation without knowledge of the consumer, as long as it is not initiated or instructed by the police.\textsuperscript{185}

In this case, it is only fair that the Fourth Amendment change the idea of ownership. Today, the private sector has found a way to take our personal information and monetize it. However, is it really their property now? The information that the private sector has created from our DNA, shopping preferences, and relationships, is all unique to each individual. Therefore, it is difficult to understand how a private company can be the owner of this information when it is unique to a specific person and would not exist without that person.

As a result, the Fourth Amendment must reevaluate ownership. Ownership of property must encompass information that is personal and unique to that specific individual. Especially in cases where the information: (1) would not exist without the individual, and (2) could severely impact the individual if it is mishandled. The Fourth Amendment can no longer recognize sensitive

\textsuperscript{176} Aten, \textit{supra} note 30.
\textsuperscript{179} United States v. Crowley, 285 F.3d 553, 558-59 (7th Cir. 2002).
\textsuperscript{180} \textit{SPARROW}, \textit{supra} note 60.
\textsuperscript{181} \textit{Id}.
\textsuperscript{182} United States v. Crowley, 285 F.3d 553, 553 (7th Cir. 2002).
\textsuperscript{184} \textit{Id} at 547.
information as property of a third-party because the consequences that are dealt apply primarily to the individual.

iii. Unreasonable Searches and Probable Cause

Another essential element of the Fourth Amendment is probable cause. The issue with probable cause and searching is that it does not require advanced notice to an individual, prior to the search. Every individual has the right to know whether they are being investigated after law enforcement has received probable cause. This right is essential, giving each person a chance to obtain representation and create a strategic plan for when, or if, the issue goes to court. When the police are surveying individuals, it is only right to have the individual notified and allow a check on law enforcement’s use of probable cause.

Companies such as Apple, Google, and Facebook have complained about the subpoenas for information on their consumers. The private sector has argued that the subpoenas are usually overly vague and do not allow the company to notify the consumer that their information is being shared with the authorities. Even though some efforts to inform consumers have been successful, law enforcement has still found ways to work around this and get the information they want without notifying the consumer. This, again, creates a general mistrust of the private sector that is collecting this sensitive information, and also law enforcement. With a notification system in place, there is more trust and gives individuals the right to take action to defend themselves early on. A notification system would only allow for a check on whether the information is sufficient probable cause, or law enforcement trying to take a shortcut.

There are, of course, pitfalls to consider, such as notifying a true criminal before officials are granted access to search the information. This may give the perpetrator the chance to delete information or escape justice. However, criminals are still citizens too and require a fair chance to defend themselves as well. There are also ways to prevent these fears of escape. If the

186. U.S. Const. amend. IV.
189. Id.
190. Id.
police know the individual will be notified, they can take action to prevent any chance of escape. Once the police have collected enough information to satisfy probable cause, nearby law enforcement can handle the rest. Lastly, even if the criminal does escape, it is better that they escape instead of having an innocent person suffer. This reasoning goes back to the historical language of Justice William Blackstone stating that a fundamental value of our justice system is that it is better for ten guilty men to go free than to have one innocent person convicted.\footnote{William Blackstone, Commentaries \textsc{*352}.}

Also, looking at the broader scope of society as a whole, violations of individual privacy can have a wide and long-lasting impact on the nation.\footnote{Swish Goswami, \textit{The Rising Concern Around Consumer Data And Privacy}, \textit{Forbes} (Dec. 14, 2020, 7:40 AM), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=741eef01487e [https://perma.cc/PQS4-QF8K].} As we have seen, society is already suffering from the harsh aftermath of these types of privacy violations.\footnote{Matt Burgess, \textit{supra} note 159.} The policies that tend to put individual privacy to the side have created an overall distrust of the police and other public entities as a whole, making compliance and cooperation from the public difficult. It is certain that recent events stem from this loss of trust.\footnote{Id.} Thus, leaving an impression that says the government can override individual rights regardless of any law or regulation in place. Although a notification system for individual consumers may alert a potential wrong doer, the overall impact of violating a person’s privacy has proven to have a ripple effect, impacting the rest of society and causing much greater consequences.\footnote{U.S. Dept' of Just., Comty. Rel. Servs., \textit{Importance of Police-Community Relationships and Resources for Further Reading}, https://www.justice.gov/file/1437336/download [https://perma.cc/R8GN-YFMV].}

Therefore, it is essential that the Fourth Amendment change and require that individuals are notified when law enforcement is looking into their personal information, after obtaining probable cause. Not only to provide a check on law enforcement, but to give individuals a chance to protect themselves in the process. This would also remedy a great amount of mistrust that has built up towards law enforcement over the years, allowing them to complete their work more effectively.

\textbf{V. Conclusion}

If law enforcement can steer the public into trusting them again, then the information that has been proven to solve many crimes and prevent future crimes will still be available for law enforcement to use, which will in turn save the police the time and cost of a legal battle to obtain the necessary
permissions to use this valuable information. The ultimate goal is to prevent crime, but not at the expense of individual rights. Whether they are innocent or not, it should still be a priority. Under the current laws, it is unclear whether information voluntarily given to a third-party is protected through the fourth amendment privacy protections. As a proposed solution, legislation must be a uniform code, or the Fourth Amendment should be refined to accommodate our new society. Otherwise, as the distrust among the public grows, collecting the information and having access to databases will be much more difficult. If this issue is not resolved soon, the community itself will suffer, pushing us back into an era where criminals were much harder to catch.