laws

MDPI

Article

Third-Party Doctrine Principles and the Fourth Amendment: Challenges and Opportunities for First Responder Emergency Officials

Klaus Schmidt [1,*], Katrin C. Varner [2] and Agrey D. Chenga [1]

[1] College of Applied Science and Technology, Illinois State University, Normal, IL 61761, USA; adcheng@ilstu.edu
[2] College of Business, Illinois State University; Normal, IL 61761, USA; kcvarne@ilstu.edu
* Correspondence: kschmid@ilstu.edu

Received: 31 December 2019; Accepted: 10 February 2020; Published: 17 February 2020

Abstract: The unresolved issues between the Fourth Amendment and the third-party doctrine provide first responders with challenges in their approach to meet the needs of any emergency they may be called for. A first responder needs to provide help quickly, and often this does not leave much time to think about the legal implications of some of their actions. With the rise of the Internet, the challenges of terrorism, and WikiLeaks, first responders are no longer sheltered from the legal implications that the use of information from online and other secondary sources may have. Specifically, privacy concerns may be raised when first responders use social media either as a tool to gather information about evolving emergencies, or to engage in the process of monitoring those media to detect potential threats to the safety of the country and its citizens. This paper will address some challenges first responders face when considering the third-party doctrine principles and the Fourth Amendment in their rescue efforts. What are some liability and legal concerns in the context of what first responders encounter when responding to potential threats? The paper will also include a discussion of practical experiences with the Fourth Amendment and third-party doctrine principles and explore liability issues related to first responders' use of information.

Keywords: US constitutional law; criminal justice; constitutional law and criminology

1. Introduction

Historically, under U.S. law, any information that has been shared with a third party is considered exempt from any claim of privacy. This is known as the third-party doctrine.[1] There were exceptions made for information shared in the scope of legally recognized confidential relationships, such as doctor-patient, priest-penitent, or spousal communications, but apart from these exceptions, any information shared with a third party, whether a person, organization, or corporation, was per se not private, since there would be no way of guaranteeing that the third party would keep one's confidence. The government would therefore not need to obtain a search warrant before gathering or accessing such material.

The first major component of this paper is the Fourth Amendment of the Constitution. The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. (Bedi 2013).[2] This amendment protects citizens against

[1] Smith v. Maryland, 442 U.S. 735 (1979).
[2] (Bedi 2013).

governmental searches of those items. However, reaction to abuses by potential government agencies often focused on responding to arbitrary searches or seizure procedures, and clearly focused on historical content, rather than taking modern technologies into consideration. Although the revulsion often focused on the techniques used, some of the practices used to obtain data and information were rather abusive and intrusive by the government agencies, they involved things held dear by those subjected to the searches or seizures, such as their persons, homes, and private papers. (Clancy 1998a).[3] The development of the Fourth Amendment intended to prevent from those arbitrary and abusive invasions. The expression of the individual's rights was often phrased by reference to property, and the notion that "a man's house is his castle" became "a part of our constitutional law in the clauses prohibiting unreasonable searches and seizures" (Clancy 1998b).[4]

The second major component of this paper is the concept of third-party doctrine, which started with (*U.S. v. Miller*).[5] Miller claimed that the Fourth Amendment should protect his bank accounts from a warrantless government search. According to the court ruling, Miller did not have Fourth Amendment rights to protect his bank accounts. The bank was considered a third party (*United States v. Miller*).[6] In a later case, *(Smith v. Maryland)*[7], Smith argued that phone numbers he had dialed were subject to Fourth Amendment protection. However, the phone company, a third party, shared that information with the government and the court ruled that the Fourth Amendment did not apply to Smith. Therefore, Smith, or any other individual who provides their information voluntarily to a third party, as in this case with the phone company, has no Fourth Amendment claim to a reasonable expectation of privacy.

Both the unresolved issues between the Fourth Amendment and the third-party doctrine, provide first responders with challenges in their approach to meet the needs from any emergency they may be called for. A First Responder, such as a law enforcement officer, a paramedic, or fire fighter, needs to provide help quickly, and often this does not leave much time to think about the legal implications of some of the actions. With the rise of the Internet, the challenges of terrorism, and WikiLeaks, first responders are no longer sheltered from the legal implications that the use of information from online and other secondary sources may have. Specifically, privacy concerns may be raised when first responders use social media either as a tool to gather information about evolving emergencies or to engage in the process of monitoring those media to detect potential threats to the safety of the country and its citizens.

This paper will address some challenges some of these first responders face when considering the third-party doctrine principles and the Fourth Amendment in their rescue efforts. What are some liability and legal concerns in the context of what first responders encounter when responding to potential threats? The paper will also include a discussion of practical experiences with the Fourth Amendment, third-party doctrine principles, and explore liability issues related to first responders' use of information.

2. Background

Peter Swire (2014), an internationally recognized expert in privacy law and Professor of Law and Ethics at the Georgia Institute of Technology, said that it is the government's responsibility to protect both the nation as a whole and personal privacy.[8] Governments often regard security as either national or homeland security or as the Fourth Amendment right of the people to be 'secure in their

---

3 (Clancy 1998a).
4 (Clancy 1998b).
5 United States v. Miller, 307 U.S. 174 (1939).
6 United States v. Miller, 307 U.S. 174 (1939).
7 Smith v. Maryland, 442 U.S. 735 (1979).
8 Swire (2014). Testimony before the House Committee on the Judiciary. Hearing on: Examining Recommendations to Reform FISA Authorities, 4 February 2014.

persons, houses, papers, and effects against unreasonable searches and seizures'. Two perspectives exist when discussing a government's right to observe private citizens. First, the government should feel comfortable using information to gain situational awareness and therefore allow first responders to quickly access and respond to the occurring emergency or crisis, and second, private citizens should not feel insecure or stressed about the possibility of the government using their information without consent.

Some recent cases, such as *Riley v. California*,[9] have started to chip away at this long-held standard. Here, the police stopped the petitioner David Leon Riley for a traffic violation that led to his arrest on weapons charges. Riley moved to suppress all evidence that the police had obtained from his cellular phone, claiming that those searches violated the Fourth Amendment. The trial court, however, rejected his argument and the California Court of Appeals affirmed that decision. An officer had seized Riley's phone without a warrant, but since he had gathered pertinent information on communications with a street gang and a murderer a few weeks prior, videos and images captured from Riley's phone were admitted into evidence.

In 2012, *United States v. Jones*,[10] provided some parameters for the concept of government monitoring. The defendant, Antoine Jones, was suspected of drug-trafficking. In order to build a case against him, the police attached a Global Positioning System (GPS) tracker to his car and monitored Jones's movements for four weeks. Even though a person's movements in public are generally not considered to be private, the Supreme Court found that using a GPS tracker changed the legal framework in this case (Bedi 2014).[11] Simply following a person on foot or in a car is permissible, but attaching a GPS tracker requires the kind of occupation of private property that necessitates a warrant.

In the 2018 case of *Carpenter v. United States*[12], the U.S. Supreme Court found that the police also needed a search warrant, in this case before obtaining information collected from cell towers by wireless carriers. The defendant in the case, Timothy Ivory Carpenter, was suspected of planning and participating in a series of armed robberies in Detroit, acting as a lookout and getaway driver. Prosecutors in the case made liberal use of cellphone records to establish Carpenter's location throughout several months *(Carpenter v. United States*).[13]

Even though the information was obtained from third parties, various cellphone companies, the Court found that the information was nevertheless private and subject to Fourth Amendment protections. Technological advances have created circumstances where people, in order to participate in everyday life, have no reasonable choice but to share such data with these third parties, even though this data can be rather intimate. To conclude that this therefore creates a kind of loophole around the warrant requirement is incorrect; technological advances require adjustments to our interpretation of legal protections. According to Chief Justice Roberts in his majority opinion:

> "Cellphones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern life while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. After all, [in 1979,] few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements . . . When the government tracks the location of a cellphone, it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user (*Carpenter v. United States*)."[14]

---

[9] Riley v. California, 573 U.S. 373 (2014).
[10] United States v Jones 132 S.Ct. 945 (2012).
[11] (Bedi 2014).
[12] Carpenter v. United States 585 U.S.__ (2018).
[13] Carpenter v. United States, 585 U.S. __ (2018).
[14] Carpenter v. United States, 585 U.S. __ (2018).

Therefore, the collection of cell tower data by the government now requires a search warrant. Justice Sonia Sotomayor anticipated this decision in her concurring opinion in the Jones case in 2012 when she wrote, "It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (Call 2018).[15] Whether this protection would extend to other third-party communications, such as social media posts, emails, internet searches, or credit card records, remains to be seen. The Carpenter case was decided on narrow grounds and the Court specifically made its traditional exceptions for emergency situations, such as abductions or terrorist threats, but as modern society increasingly requires us to share private information with third party service providers, it is likely that the courts will be addressing variations on these questions for years to come (*Carpenter v. United States*).[16]

However, in the case of *Hoffa v. United States*,[17] union boss Jimmy Hoffa invited someone he believed to be a fellow union member into his hotel room and shared confidences with him. His confidant, Edward Partin, turned out to be a government informant, who regularly shared details of their conversations with a federal agent and whose testimony at trial was a substantial factor in Hoffa's conviction for attempted bribery. Hoffa argued that because Partin failed to disclose his identity, Hoffa had not truly consented to having him in the hotel suite and that by listening to Hoffa, Partin conducted, supposedly, an illegal search, violating the Fourth Amendment. The Court however rejected this view, reasoning that Partin did not forcefully enter the suite. Partin was invited by Hoffa to come to the suite. The conversations that took place in that suite took place in his presence. Rather than relying on the security of the hotel room, Hoffa relied on his misplaced confidence that Partin would not reveal details of their conversations *(Hoffa v. United States*).[18] The Court concluded: "Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it" *(Hoffa v. United States*).[19]

Hoffa paved the way for the 1976 case of *United States v. Miller*[20] which would help crystallize the modern-day third-party doctrine. In 1976, Miller involved the federal government's use of defective subpoenas to obtain copies of the bank records of Mitch Miller, who was suspected of running an illegal whiskey distillery. After Miller was indicted for conspiracy to defraud the government, he moved to suppress the records because there was no valid warrant. In a cursory opinion, the Supreme Court held—relying on Hoffa—that: 'The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed'. (Bedi 2013).[21] While the opinion emphasized that the records were not confidential communications and that they related to transactions including the bank as a third party, the case has taken on the status of canon and now suggests that nearly any information released to a third party, under almost any circumstance, is fair game for government agencies until a new statute addresses that issue. (Waldman 2018).[22]

The third-party doctrine strongly contrasts the Fourth Amendment and intends to create exceptions to what can be reasonable expectation of privacy (Mund 2018).[23] Some of those exceptions can be found in *Smith v. Maryland*[24] and in the very old case of *Ex parte Jackson*[25], specifically the distinction

---

15 (Call 2018).
16 Carpenter v. United States, 585 U.S. __ (2018).
17 Hoffa v. United States, 385 U.S. 293 (1966).
18 Hoffa v. United States, 385 U.S. 293 (1966).
19 Hoffa v. United States, 385 U.S. 293 (1966).
20 U.S. v. Miller, 425 U.S. 435 (1976).
21 (Bedi 2013).
22 (Waldman 2018).
23 (Mund 2018).
24 Smith v. Maryland, 442 U.S. 725 (1979).
25 Ex parte Jackson, 96 U.S. 727 (1878).

between content and non-content information. For Smith, no 'content' of the phone conversations was provided, and for Ex parte Jackson, the content of letters was not provided (Mund 2018).[26] In Ex parte Jackson, the Court found that mailed letters and sealed packages "are as fully guarded from examination and inspection, except as to their outward form and weight" (*Ex parte Jackson*).[27] Therefore, government agencies can read information printed on the cover of an envelope or a package, but they are not allowed to open it. However, courts have not yet reached an agreement on what distinguishes 'open' from 'unopen' or 'content' from 'non-content' when it comes to social media communications (Mund 2018).[28]

A subsequent challenge with respect to social media includes the concept of consent. Do individuals who make information about themselves or others available in the public domain through social media give consent just by their plain action? Depending on the technological literacy level of an individual, they may or may not know or understand how privacy settings work on the platforms they use. For example, in a study on the understanding of privacy settings of online social networks conducted by Johnson et al. (2012)[29], Facebook user settings were found to be confusing to many users, and users often believed their postings were not public when in fact they were. The study also revealed that for many users the concept of consent was unclear. Users seem to know that it is a legal contract when they purchase something, either online or in a store, but when downloading apps in social media, they rarely read the fine print.

To complicate the matter, many individuals around the world use social media. Social media platforms have revolutionized how people communicate and interact with one another. Still, many social media users continue to believe that their communications will remain private and free from any government intrusion. Yet, all digital communications seem to lose Fourth Amendment protection because users voluntarily disclose information to Internet Service Providers (ISPs). The third-party doctrine, in courts, seems to be treated as consent or waiver and thus Fourth Amendment protection does not cover the communications disclosed to a third party. It is no matter if the individual released that information only for his or her friends; the voluntary nature of the disclosure ruins all privacy protection for these communications (Bedi 2013).[30]

When the third-party doctrine is applied to information retrieved from social media, first responders may argue that internet users often have no worries about their privacy, their data, and their postings. Therefore, anybody, including government agents, may freely and easily access that information without respecting warrant requirements. As soon as an internet user posts something, the user discloses information to the Internet Service Provider, and most likely to individuals inside that user's social network. If the third-party doctrine were to govern internet use and specifically online behavior, then any content voluntarily shared online would lose all reasonable Fourth Amendment expectation of privacy (Mund 2018).[31] However, many individuals who use social media believe or perceive that privacy is still protected in their public social media posts. Unfortunately, courts have not yet recognized this misunderstanding as creating a reasonable expectation of privacy in an environment that is complicated by the third-party doctrine (Scott 2017).[32] Thus, interpreting current discussion in literature and in the courts, social media users are generally not protected by the Fourth Amendment, even if the user restricts access to their own social media content. Therefore, government agents are still allowed to obtain that information without a warrant (Scott 2017).[33]

---

[26] (Mund 2018).
[27] Ex parte Jackson, 96 U.S. 727 (1878).
[28] (Mund 2018).
[29] (Johnson et al. 2012).
[30] (Bedi 2013).
[31] (Mund 2018).
[32] (Scott 2017).
[33] (Scott 2017).

Nevertheless, a number of pieces of federal and state legislation in the United States exist that may have implications for a government or state agency to monitor social media. The 1974 Privacy Act, for example, regulates how the government maintains and shares information with federal agencies and individuals (Lane 2009).[34] However, there is no clarity in this act regarding how data is being collected or used, specifically since this act predates the Internet. In 2011, a System of Records Notice discusses how the Department of Homeland Security (DHS) suggests to self-regulate monitoring social media[35] by allowing the DHS, the Office of Operations Coordination and Planning (OPS), and the National Operations Center (NOC) to provide common operating practices for government agencies. It also ensures that first responders and decision-makers receive important disaster-related information quickly, correctly, and hopefully, completely. This information sharing system does have an effect on individual privacy and will need to be carefully balanced with respect to collection, planning, coordinating, reporting, and analyzing homeland security information coming into and going out of OPS. A few exceptions to this information sharing process exist; those exceptions are considered routine uses. Routine uses may include (a) sharing information with the Department of Justice (DOJ) for legal advice, (b) information sharing with a congressional office at the request of an individual, (c) records management at the National Archives and Records Administration (NARA), (d) with DHS contractors, including private entities in their role of aiding OPS in their mission, and (e) with agencies, organizations or individuals for auditing purposes.[36] Furthermore, information can be shared with persons during a security or information compromise or breach when there could potentially be a risk of harm to an individual, and certainly with news media in the interest of the public.[37]

The Privacy Office of the DHS has a very clearly defined cybersecurity and privacy definition[38] and views privacy as something more than just the compliance with existing laws. Rather, privacy considerations should include the concept of public trust and confidence-building. In this way, the government's actions are transparent, and it could be assumed that it has acted responsibly with respect to data collection and maintenance.

One approach that may help to gain a better insight of the way the DHS regards privacy with respect to digital data is the Fair Information Practice Principle (FIPP), which was created in 2008, by the DHS. The FIPP includes eight principles that help and guide first responders to best manage data with a focus on digital data. The first three principles are transparency, individual participation, and purpose specification and can be summarized by providing transparency and individual participation in the process of using personally identifiable information (PII) relating to the collection, use, dissemination, and maintenance of data.[39] This means that, when practical, individuals should be involved in the data collection process and the way the data is being used by seeking individuals' consent. According to this set of principles, the DHS mechanisms should be transparent with respect to the mechanisms used for accessing and using data. It should be clearly articulated to the ISP and the internet user, what the data will be used for.[40]

Principles 4, 5, and 6 are data minimization, data quality and integrity, and use limitation. This set of principles states that the DHS could and should only collect information that is relevant and

---

34 (Lane 2009).

35 Department of Homeland Security (2011). Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records. FR Doc. No. 2011-2198, 2011. Available online: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf (accessed on 26 April 2019).

36 Department of Homeland Security: Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records. FR Doc. No. 2011-2198, 2011. Available online: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf (accessed on 26 April 2019).

37 Department of Homeland Security: Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records. FR Doc. No. 2011-2198, 2011. Available online: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf (accessed on 26 April 2019).

38 Department of Homeland Security: Cybersecurity & Privacy. Retrieved from: https://www.dhs.gov/sites/default/files/publications/privacy_cyber_0.pdf (accessed 20 November 2019).

39 (The White House 2012).

40 (Department of Homeland Security 2012).

necessary to accomplish a specific purpose. The DHS should also only retain data as long as it is necessary and only use it for the exact purpose intended. In all of the attempts to collect data, the data quality should be assured with respect to accuracy, relevance, timeliness, and completeness.[41]

The final two principles are security and accountability. The DHS should protect all PII using safeguards against any risks, including unauthorized access, destruction, loss, modification, and unintended or inappropriate disclosure.[42] The DHS should further audit the use of PII to assure compliance with the eight principles.

3. First Responders

First responders for this discussion are operationally defined as individuals that observe or arrive at a potential crime or accident scene and have the qualifications to act in response to the incident. These individuals may include law enforcement officers, firefighters, paramedics, medical doctors, or nurses. Bystanders that are capable of providing help but are not considered in their official professional role, may not be included in the definition of first responders in this discussion.

In order to enhance access to information by first responders, further legislation may need to be considered. For example, the Electronic Communications and Privacy Act, 18 U.S. Code § 2511—interception and disclosure of wire, oral, or electronic communications, places strict limits on the interception of phone calls and prohibits electronic communication service providers or their employees from divulging information to a third party, unless prior consent is given. The code provides a list of constraints with a number of exceptions that could allow legal monitoring options.[43] Section 2511(1)(e), specifically, was added as one of the miscellaneous provisions in the Violent Crime Control and Law Enforcement Act of 1994. It prohibits (i) intentional disclosure of the contents of a wire, oral, or electronic communication, intercepted by certain authorized procedures, (ii) knowing or having reason to know that the information was obtained through interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly interfere with a duly authorized criminal investigation. While these constraints do not necessarily apply directly to social media, they do give some insight into how to handle private communications.

An additional example of legislation regarding the use and surveillance of online activities is the Stored Communications Act (SCA)[44], which may also play a considerable role when first responders use existing data. Atkinson explains that the SCA prohibits an ISP from sharing a stored communication of one of their customers unless lawful consent of the originator or an addressee or intended recipient of such communication is obtained. However, this statute is quite different from the Electronic Communications and Privacy Act 18 U.S.C. § 2511(1) mentioned above, because it makes it an offense to access a stored communication even though it is not in transmission.[45]

For example, in *Commonwealth v. Risley*[46] the police questioned a woman's rape claim when her Fitbit smartwatch contradicted her statement. Risley faced three misdemeanor counts for prompting an emergency response and manhunt (Chauriye 2016).[47] However, it has not been clearly decided what category of technology a Fitbit smartwatch falls under, as the legal procedure may be affected differently. Furthermore, even more importantly so, can or should the police use data obtained from the alleged victims smartwatch against the alleged victim herself. Fitbit's privacy policies seem to allow the Fitbit corporation to share users' data with third parties, but do users read all the privacy and

---

41 (Department of Homeland Security 2012).
42 (Department of Homeland Security 2012).
43 18 U.S. Code § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited.
44 18 U.S. Code § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited.
45 18 U. S. Code § 2701. Unlawful access to stored communications.
46 Commonwealth v. Risley, CP-36-CR-0002937, (2015).
47 (Chauriye 2016).

small print information in a contract? However, consumer privacy experts also expressed concerns that the information collected by companies like Fitbit can do analytics based on the data obtained and may include major conclusions about an individual's personal life. Can a First Responder access videos, selfies, audio files on a smartphone to provide better help? (Chauriye 2016)[48]

Nevertheless, even though some surveillance or monitoring activities can be considered legal under specified circumstances, and therefore very helpful to first responders, some of those activities may still not be appropriate from a government policy perspective.

The DHS certainly continues to be aware of these issues and believes that self-imposed limitations on monitoring activities suffice. These self-imposed limitations are included in the DHS's System of Records Notice and are binding.[49] However, they continue to be criticized by the House of Representatives.[50] Self-imposed limitations would allow the DHS to decide on their own which legal restrictions to implement in their efforts to address challenges with respect to challenges such as disaster responses, information technology infrastructure protection, border security, or transportation security. For example, principles 4, 5, and 6 of the FIPPs state, as previously discussed, that the DHS could and should only collect information that is directly relevant and necessary to accomplish a specific purpose and to only retain it as long as it is necessary to accomplish that specific purpose. Specifically, these limitations add additional constraints for first responders.

Another privacy challenge for first responders comes into play when attempting to use private citizens to report on potential threats. The DHS—Office of Public Affairs 'unsuccessfully' developed the 'See Something, Say Something' Campaign[51] with the intent to engage the public in protecting their communities through awareness-building, partnerships, and other outreach. More specifically, if somebody sees something that should not be there or observes some behavior that does not seem quite right or some suspicious objects, they should say something, or report it. The campaign attempted to underline that informed, alert communities could be instrumental in keeping communities safe. However, this campaign failed because of challenging and unresolved privacy concerns, and the fact that private citizens are not necessarily considered first responders.

Nevertheless, the definition of 'volunteer' still needs to be clarified. For example, if a public entity calls for volunteers, we can certainly speak of a First Responder type of definition. Is the individual then properly trained? A civilian who considers themselves a 'volunteer' may very well not be considered a First Responder for legal purposes. Self-declared first responders may trigger self-justice with all its consequences, and if individuals neglect or refuse to act as first responders or to provide their support at a critical site, the tort of negligence may come into play. Negligence is defined as 'a legal wrong that is suffered by someone at the hands of another who fails to take proper care to avoid what a reasonable person would regard as a foreseeable risk' (Prosser 1941).[52] The tort of negligence includes four elements, namely duty, breach, causation, and damages. This concept then makes it even harder for first responders to know exactly when to act.

In *Caparo Industries PLC v. Dickman*[53] a test was established to decide whether a 'duty of care' exists with respect to a particular relationship, often a necessary element of establishing a claim of negligence. The test required three elements to exist in order to establish such a duty: (a) harm must be a reasonably foreseeable result of the defendant's conduct, (b) a relationship of proximity must exist, and (c) it must be fair, just, and reasonable to impose liability.[54] As a result, mere bystanders would

---

48 (Chauriye 2016).
49 Available online: https://www.dhs.gov/system-records-notices-sorns (accessed on 28 April 2019).
50 Subcommittee on Counterterrorism and Intelligence. DHS Monitoring of Social Net- working and Media: Enhancing Intelligence Gathering and Ensuring Privacy. 16 February 2012. Washington, D.C.
51 Department of Homeland Security. If You See Something, Say Something. Available online: https://www.dhs.gov/see-something-say-something (accessed on 28 April 2019).
52 (Prosser 1941).
53 Caparo Industries PLC v. Dickman (1990) 2 AC 605.
54 Caparo Industries PLC v. Dickman (1990) 2 AC 605.

not be required to intervene or to help an injured individual. Nevertheless, there are exceptions that remain. For example, if an individual starts to provide help, they are required to continue providing help until somebody else who is better qualified steps in and takes over, but when is that exact point where help is provided?

With respect to social media use, the concept of negligence and the duty of care may imply that a private citizen who reads a questionable social media posting may need to continue their support once they communicated an intent to assist the distressed individual and possibly reported the incident. Examples for such a situation might include cyber-bullying, cyber-stalking, cyber-slander or -defamation, or the suspicion of planning terrorist activities. To advance the concepts and challenges of social media use further, first responders will need to be constantly aware of the credibility, authenticity, and reliability of the information obtained and used for their emergency responses. One possible approach to assess these attributes of information could be the establishment of a reputation system similar to eBay's, which operates arguably the most successful and widely known online reputation system, which includes feedback from buyers and data on the history of the buyers and sellers. Such a system could be feasible, and private citizens could become formally recognized as first responders using internet platforms. These individuals may need training to respond appropriately to emergencies. Nevertheless, the usefulness of reputation systems with respect to disaster response has limits. For example, a participant who has had a chance to develop a positive reputation through interactions prior to the occurrence of a disaster will be considered a 'valuable' resource, while others who may in fact have very useful information but no prior positive reputation might not be considered valuable 'resources'.

4. Conclusions

The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures (Lane 2013).[55] However, the third-party doctrine complicates and contradicts Fourth Amendment rights as it creates a complex set of exceptions to what many researchers, especially Fourth Amendment researchers, believe a fundamental right.

The Supreme Court still needs to take a clear stance on how the third-party doctrine impacts communications on social media sites. There continues to be disagreements in literature between lower courts and higher courts, Fourth Amendment scholars, and third-party doctrine scholars about whether the doctrine should even apply at all. Some appellate courts have adopted the third-party doctrine when applying the Fourth Amendment to Internet communications. Other courts try to distinguish between content and non-content information within the communication (Bedi 2013).[56] Many researchers suggested solutions that include better laws to protect Internet communications but also suggest complete reconceptualization of how the Fourth Amendment should work in the digital age and go so far as to argue to eliminate the third-party doctrine (Bedi 2013).[57]

As both the Fourth Amendment and the third-party doctrine contradict and inhibit access to information by first responders, and ultimately may put citizens at risk, transparent and clear legislation needs to be considered so information can be communicated effectively and successfully to first responders. Some attempts exist to introduce more clarity; for example, the Electronic Communications and Privacy Act 18 U.S. Code § 2511—interception and disclosure of wire, oral, or electronic communications, places some strict limits on the interception of phone calls. This act, for example, prohibits electronic communication service providers or their employees from divulging information to a third party, unless prior consent is given. The code provides a detailed list of constraints with a number of exceptions that could allow legal monitoring options.[58] While these

---

55 (Lane 2013).
56 (Bedi 2013).
57 (Bedi 2013).
58 18 U.S. Code § 2511. *Interception and disclosure of wire, oral, or electronic communications prohibited*.

constraints do not necessarily apply directly to social media, they do give some transparent insight into how to handle communications that are intended to be private.

Social media use, as well as the use of third-party information by first responders and the monitoring of those media by government agencies continue to raise privacy concerns. Social media users often do not recognize or acknowledge that they disclose considerable amounts of data while posting information, with or without considering the concept of consent. As discussed in this paper, first responders are often put into peculiar situations when using and responding to data obtained via social media or from smartphones. In cases of serious emergencies, time works against the first responder, and the first reaction of the first responder is to help fix the problem, rather than concerning themselves with the legal framework that comes with the use of personally identifiable information. The authors of this paper therefore favor obtaining search warrants prior to engaging in any kind of action that could reasonably be considered an intrusion of privacy. They suggest that it is important to understand that the warrant must not only be lawfully obtained, but must also be executed in a timely and accurate manner (*United States v. Jones*).[59] Most first responders are aware that the process of obtaining a search warrant is not typically very time-consuming or complicated, therefore providing a strong rationale for obtaining such documentation. The authors therefore believe that it may not be necessary to develop new laws to address conflicts between the Fourth Amendment and the third-party doctrine with respect to obtaining digital data, but rather propose to continue to observe case law during the next few years.

Nevertheless, some policymakers still seem to argue that individuals who post information online are sufficiently internet savvy to fully understand that a government agency may have the right to use that information without a warrant. Others believe it is unsettling to know that a government agency may be quietly investigating information posted on social media without such a warrant or consent.

In times where local and international terrorism and mass shootings are of great social concern, it becomes increasingly challenging to dissect what information is good and useful and what information hinders first responders in their duties, and what information should never enter the public sphere. What kind of information first responders should have access to is also becoming increasingly controversial. Is the right to privacy outweighing the right to live peacefully, without threat and fears, without jeopardizing ones' health and safety? Policymakers still have much work to do. Confusion about legal paradigms with respect to privacy should be minimal or, even better, eliminated. Citizens need to feel safe, and their information needs to be safe. Monitoring all activities online may very well be possible from a technical perspective but is likely not the answer to combatting terrorism. We must find a way to introduce a better balance between the protection of our privacy and information and the protection of our lives.

Author Contributions: conceptualization, K.S.; investigation, K.C.V.; methodology, K.S. and K.C.V.; resources, A.D.C.; writing—original draft, K.S.; writing—review and editing, K.S. and K.C.V. All authors have read and agree to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Bedi, Monu. 2013. *Facebook and Interpersonal Privacy: Why the Third-Party Doctrine Should Not Apply*. Boston: College, Law Review, vol. 54/1.

Bedi, Monu. 2014. *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*. Boston: University, Law Review, vol. 94, pp. 1810–80.

---

[59] United States v. Jones, 132 S.Ct. 945 (2012).

Call, J. 2018. *Carpenter v U.S: Obtaining Extensive Cell Site Location Data is a Search*. Radford: Virginia Criminal Justice Bulletin, vol. 3, no. 2.

Chauriye, Nicole. 2016. Wearable devices as admissible evidence: Technology is killing our opportunities to lie. *Catholic University Journal of Law and Technology* 24: 2–27.

Clancy, Thomas. 1998a. What does the Fourth Amendment Protect: Property, Privacy, or Security? *Wake Forest Law Review* 33: 307.

Clancy, Thomas. 1998b. What does the fourth amendment protect: Property, privacy, or security? *Wake Forest Law Review* 33: 2–50.

Department of Homeland Security. 2011. Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records. Theodora Update January 6, 2011. Available online: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf (accessed on 26 April 2019).

Department of Homeland Security. 2012. DHS Testimony on Social Networking and Media Monitoring. Available online: https://publicintelligence.net/dhs-testimony-on-social-networking-and-media-monitoring/ (accessed on 20 November 2019).

Johnson, Maritza, Michelle Madejski, and Bellovin Steven. 2012. A study of privacy setting errors in an online social network. Paper presented at 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (SESOC 2012), Lugano, Switzerland, March 19–23.

Lane, Frederic. 2009. *American Privacy: A 400-Year History of Our Most Contested Right*. Boston: Bacon Press.

Lane, Frederic. 2013. *American Privacy—The 400-Year History of Our Most Contested Right*. Boston: Bacon Press.

Mund, Brian. 2018. Social media searches and the reasonable expectation of privacy. *Yale Journal of Law & Technology* 19: 2–25.

Prosser, William L. 1941. *Handbook of the Law of Torts*. Baton Rouge: Louisiana Law Review, vol. 4, Number 1, November.

Scott, Jeramie. 2017. Social Media and government surveillance: The case for better privacy protections for our newest public space. *Journal of Business & Technology Law* 12: 151.

Swire, Peter. 2014. Testimony before the House Committee on the Judiciary. Hearing on: Examining Recommendations to Reform FISA Authorities. Available online: https://fas.org/irp/congress/2014_hr/020414swire.pdf (accessed on 4 February 2019).

The White House. 2012. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available online: http://docshare.tips/white-house-data-privacy-report-_576bf97ab6d87fc5918b4a09.html (accessed on 21 June 2019).

Waldman, Rachel. 2018. Government Access to and Manipulation of Social Media: Legal and Policy Challenges. *Howard Law Journal* 61: 1–28.