2015

Surveillance on the Internet: A Comparison of the United States and the European Approaches to Protection and Privacy on the Internet in the Face of Increased Government Monitoring in an Effort to Combat Domestic Terrorism

Alexander Walder

Surveillance on the Internet: A Comparison of the United States and European Approaches to Protection of Privacy on the Internet in the Face of Increased Government Monitoring in an Effort to Combat Domestic Terrorism

I. Hypothetical

Concerned with the ever present threat of terrorism and the growing influence of ISIS, the Federal Government has begun to monitor domestic accessing of websites containing ISIS based content. The Government's surveillance program begins by compiling a list of "target websites" based on the site's ISIS related content. The Government tracks who accesses these websites by identifying each IP address of every person that visits a "target site." The Government will then create a database compiling all of the IP addresses of the individuals who access these sites. The Government will then run searches within the database to identify individuals who have been frequently visiting these "target sites." If an IP address is identified as frequently visiting the "target sites," they will be deemed a "high volume" user. Once an IP address is deemed "high volume," the Government will then target that individual for further monitoring. This further surveillance will involve the Government obtaining the personal information for the user of each "high volume" IP address, as well as continually monitoring all of the IP addresses that individual accesses. The Government will conduct this surveillance without warrants.

A suit is brought by an individual who was identified as a high volume user and became aware that all of his internet browsing was being monitored. This individual is claiming that the government violated his Fourth Amendment privacy rights by obtaining his IP address through the "target website" monitoring and subsequently monitoring his "outgoing" IP addresses.

An IP address is a number that marks a "location" on the internet. Every website on the internet has only one IP address. So, for example, even a website as expansive as Google has one unique IP address that every person visiting that website connects to. Additionally, each individual who accesses the internet has a unique IP address that is assigned to them.

II. The Right to Privacy in the United States

a. Brief History of the Development of the Right to Privacy through the Fourth Amendment

The Fourth Amendment of the United States Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[1]

The United States Constitution, unlike many foreign country's constitutions, does not contain an explicit "right to privacy." While not explicitly included, the Supreme Court has found there to be a right to privacy under the Fourth Amendment.[2] The Fourth Amendment protects individual's "privacy" by not allowing for their private property be to be unreasonably searched or seized without a warrant.

Fourth Amendment privacy protection has evolved over time to allow for protection from different kinds of government invasions. In its early stages, privacy protection was limited to stopping the Government from physically encroaching on an individual's property.[3] However,

[1] U.S. CONST. amend. IV.
[2] *See Katz v. U.S.*, 389 U.S. 347 (1967).
[3] *See Olmstead v. U.S.*, 277 U.S. 438 (1928), *overruled* by *Katz*, 389 U.S. 347.

with the advent of new technologies, the Court has recognized that there can be an invasion of privacy through Government conduct that does not involve physical intrusion.[4] The move away from requiring physical intrusion for there to be a Fourth Amendment violation recognized that communication itself was private and should be protected.[5] While *Katz* was a case dealing with communication through the phone, Fourth Amendment protection has continued to evolve to protect new technologies by applying the reasoning laid out in *Katz*.

The Fourth Amendment protects against unreasonable searches of private property by the Government, unless the Government has obtained a warrant to do so. Therefore, in order to prove a Fourth Amendment violation, an individual would first need to show that there was a "search" by the Government. If they can show that there was a search and the Government did not have a warrant for that search, the burden would shift to the Government to show that their search was valid despite not having a warrant.

In our hypothetical, an individual argues that the Government conducted a Fourth Amendment "search" when they obtained his IP address. Therefore, our analysis begins with consideration of whether government conduct of this nature is considered a "search" under the Fourth Amendment.

In order to show that there was a Fourth Amendment search, it first must be shown that the Government accessed something that was protected by the Fourth Amendment. Under modern Fourth Amendment privacy doctrine, there are two ways by which a defendant can achieve this: (1) showing that the government encroached on something he had a "reasonable expectation of

[4] *See Katz*, 389 U.S. 347.

[5] *Id.*

privacy" or (2) that the government "physically occupied private property for the purpose of obtaining information."[6]

Since there was no physical occupation here, in order to prove that there was a search Defendant would need to meet the requirements of *Katz*.[7] In his concurring opinion in *Katz,* Justice Harlan laid out a two-part test for analyzing whether an individual has a reasonable expectation of privacy.[8] This test contains a subjective and objective prong, first requiring that the individual subjectively believed that he had a right to privacy and second that that expectation of privacy was one that society accepts as reasonable.[9]

Analysis of whether there was a "reasonable expectation of privacy test" will frequently involve employing the third-party doctrine as stated in *Smith v. Maryland*.[10] Under the third-party doctrine, information loses its Fourth Amendment protection once it is voluntarily shared with a third-party.[11] However, recognizing the potential for a complete erosion of Fourth Amendment protection as a result of the third-party doctrine, the Supreme Court in *Smith* limited their holding based on whether the information was "content of communication."[12] Even if disclosed to a third-party, any information that is deemed to be "contents of communication" will retain its Fourth

---

[6] *See Katz*, 389 U.S. 347, *see also United States v. Jones*, 132 S.Ct. 945 (2012).
[7] In *Jones*, the Court applied the physical intrusion test to GPS tracking of an individual's car by the Government. *Jones*, 132 S.Ct. 945, 953. While the GPS signals were sent electronically, the police physically placed the GPS device on his car, making it a physical intrusion on his private property. *Ibid.* The *Jones* Court discussed the future application of the two tests, stating that when the surveillance only involves the transmission of electronic signals, then the *Katz* test still applies. *Ibid*.
[8] *Katz*, 389 U.S. at 361.
[9] *Ibid*.
[10] 442 U.S. 735 (1979).
[11] *Id*. at 743-44.
[12] *U.S. v. DiTomasso*, No. 14-cr-160 (SAS), 2014 WL 5462467 at * 3 (S.D.N.Y. Oct. 28, 2014)(citing *Smith*, 442 U.S. at 741).

Amendment protection.[13] On the other hand, if the information is deemed to be "the ancillary information that the act of communication incidentally discloses," then the information loses its Fourth Amendment protection once it is disclosed to a third-party.[14] Today, the distinction between "content" and "non-content" is also frequently described as the difference between "data" and "metadata."[15]

Since its holding was announced, *Smith* has served as the starting point for evaluation as to whether information is "content" and thus still protected despite third-party disclosure. Courts have attempted to analogize modern technologies and surveillance methods with the factual situation in *Smith* to reach this decision.[16]

In *Smith*, the government, without a warrant, caused the telephone company to install a "pen register" at its offices to record the numbers dialed on the home phone of the defendant.[17] The government used the phone numbers dialed by the defendant to confirm their suspicion that he was the one making phone calls associated with a crime.[18] This dialing information was used to obtain a warrant to search Defendant's home, who was later convicted.[19] The Court in *Smith* rejected the defendant's argument that there was a Fourth Amendment violation, based on the conclusion that the installation of the pen register did not constitute a "search."[20] In reaching this holding, the Court concluded that the phone numbers dialed were not "contents" of the phone call

---

[13] *Ibid*.
[14] *Ibid*.
[15] *DiTamasso* 2014 WL 5462467 at *3.
[16] *See e.g.*, *U.S. v. Forrester*, 512 F.3d 500, 509 (9th Cir. 2007); *American Civil Liberties Union v. Clapper*, 959 F.Supp.2d 724, 749-52 (S.D.N.Y. 2013).
[17] *Smith* 442 U.S. at 737.
[18] *Ibid*.
[19] *Id.* at 737-38.
[20] *Id.* at 745-46.

that was made, so there was no protection due to the disclosure of the dialed numbers to the phone company.[21]

The holding in *Smith* says that there is no reasonable expectation of privacy for "non-content" that is disclosed to a third-party.[22] The rationale behind this holding is that the objective prong of the *Katz* test is not met because it is no longer reasonable to expect that the information will remain private because you cannot control what that third-party will do with the information.[23]

The importance of the determination of whether something is "contents" under the third-party doctrine cannot be overstated. Once something is "not protected" by the Fourth Amendment, it can be freely obtained by the Government without a warrant. If the information is not protected, then there is no "search" in obtaining it and the burden will not shift to the Government to have to argue that a warrant was not necessary.

b. Development of the Right to Privacy with Respect to Modern Technology

1. Standard that Has Been Applied

With respect to modern technology, as long as there is no physical intrusion by the Government, courts continue to apply the *Katz* "reasonable expectation of privacy" test to determine whether the information obtained by the Government is protected by the Fourth Amendment.[24] Additionally, *Smith* has been applied to almost every surveillance case involving

[21] *Ibid*.
[22] *Forrester*, 512 F.3d at 509.
[23] *Ibid.*
[24] *See e.g., U.S. v. Christie*, 624 F.3d 558, 573-74 (3rd Cir. 2010), *Forrester*, 512 F.3d at 509.

information from internet or cell phone use, as all such communication is relayed through a third-party, whether it be an internet service provider ("ISP") or cell service provider.[25]

2. The Internet and the "Content" vs. "Non-Content" Distinction

In our hypothetical, the Government compiled the IP addresses of every person who visited a "target site." Since the internet use was conveyed through an ISP, the third-party doctrine of *Smith* would have to be considered. This leaves the question or whether an IP address is "content" under *Smith*. Courts that have addressed this issue have concluded an IP address is not content.

As discussed above, IP addresses can be used to identify both the individual who is using the internet as well as the websites which that user visits. Courts have discussed IP addresses in both contexts. In *Christie,* the court monitored a particular website to see what IP addresses were "incoming," ultimately using the IP address to find out personal information on the individual who accessed the monitored site.[26] In *Forrester*, on the other hand, the court was looking at "outgoing" IP addresses and thus monitoring the websites the individual was visiting.[27] In both cases, the same conclusion was ultimately reached: individuals have no reasonable expectation of privacy for their IP addresses, and therefore they are not protected under the Fourth Amendment.[28]

In *U.S. v. Forrester,* the Ninth Circuit evaluated the constitutionality of a government surveillance program that, among other things, obtained the IP addresses of websites the defendant visited.[29] The government had applied for and received court permission to install a "mirror port"

[25] *See e.g., Forrester*, 512 F.3d at 509-511, *Clapper*, 959 F.Supp.2d 724, 749-52.
[26] *Christie*, 624 F.3d at 573-74.
[27] *Forrester*, 512 F.3d at 510.
[28] *Christie* 624 F.3d at 574; *Forrester* 512 F.3d at 510.
[29] *Forrester* 512 F.3d at 509.

at the ISP connection facility.[30] The "mirror port" recorded the internet activity of the defendant and allowed the government to learn the "to and from" of his email communications, the IP addresses of the websites he visited, and the total volume of information sent to or from his account.[31]

The court ultimately rejected the defendant's constitutional challenge to the surveillance because they concluded that there was no Fourth Amendment "search."[32] The court applied the third-party doctrine and determined that the "mirror port" was not "content" as it was analogous to the pen register in *Smith*.[33] The court reached this conclusion by determining that an IP address is voluntarily conveyed to the ISP and that an IP address does not contain any more information about the contents of communication than phone numbers dialed.[34] While the court recognized that the nature of the communication could potentially be deduced based on the website name, they concluded that this does not distinguish the case from *Smith* because that could also be done with phone numbers dialed.[35]

In *Christie*, the Third Circuit determined that there was no violation of the Fourth Amendment when the government recorded defendant's IP address and subsequently used the IP address to get the defendant's personal information.[36] Here, the defendant was convicted of crimes related to his involvement in the distribution of a child pornography through a website.[37] The government began monitoring the website and obtained the IP addresses of those who accessed

[30] *Id*. at 505.
[31] *Ibid*.
[32] *Id.* at 509.
[33] *Id.* at 510.
[34] *Ibid*.
[35] *Ibid*.
[36] *Christie* 624 F.3d at 574.
[37] *Id.* at 562.

it.[38] Once the IP addresses were identified, the government brought the IP address information to the ISP to obtain the personal details of the individual who the IP address was assigned to.[39] The defendant in this case was one of the individuals who was identified through this process.[40] The court applied the third-party doctrine and concluded that the defendant had no reasonable expectation of privacy in his IP address, and therefore the government's conduct did not constitute a "search."[41]

The distinction between "content" and "non-content" information has also applied to similar situations involving statutory, as opposed to Fourth Amendment, violations. Despite applying different law, courts have reached the same general conclusion, IP addresses are not "content" of internet communication.

In addressing such a statutory claim, The United States District Court for the District of Massachusetts analyzed what constituted "content" with respect to obtaining IP addresses of websites recorded through a pen register.[42] The requirements for obtaining a "pen register" were laid out in 18 *U.S.C.* § 3127(3).[43] Included in these requirements is that the pen register cannot record the "contents of communication."[44] The court also applied 18 *U.S.C.* § 2510(8), which defines "contents" to "include[] any information concerning the substance, purport or meaning of that communication.[45]

---

[38] *Id.* at 563.
[39] *Ibid*.
[40] *Ibid*.
[41] *Id*. at 573-74.
[42] *In re Application of United States for an Order Authorizing use of A Pen Register and Trap*, 396 F.Supp.2d 45, 48 (D.Mass.2005).
[43] *Id*. at 47.
[44] *Ibid*.
[45] *Id.* at 48.

Under the pen register sought by the government, the ISP would be required to provide them with the incoming and outgoing IP addresses of the particular account which is subject to the pen register.[46] The court held that the IP address of websites visited, on its own, did not contain "contents of communication."[47]

However, the court went on to identify closely related information that would could be obtained through the pen register that would cross the line into being "content."[48] Specifically, the court discussed a potential issue if the user entered search terms, and those search terms appeared in a URL recorded by the pen register.[4950] In applying the statutory definition of "content" to this type of URL, the court stated that "the 'substance' and 'meaning' of the communication is that user is conducting a search for information on a particular topic."[51] In so holding, the court drew a distinction between search terms and a website name, concluding that while an IP address is not protected, search terms crossed the line into being "contents" and thus are protected by the Fourth Amendment.[52]

The approach of *In re Application* has been discussed in the Fourth Amendment context in *Forrester*.[53] There, the court discussed how a URL might be different from an IP address because it identifies the specific page on a website that the individual viewed.[54] Also, the footnote

---

[46] *Ibid*
[47] *Ibid*.
[48] *Id.* at 48-49.
[49] *Id.* at 49.
[50] A URL identities the specific page within a website, as opposed to the IP address, which captures only the name of the website. As discussed by the court, in certain situations a URL also has the potential to contain search terms entered by a user.
[51] *Id.* at 49.
[52] *Id*. at 50.
[53] 512 F.3d at n.6.
[54] *Ibid*.

addresses how certain URLs containing the search terms that the user inputted immediately before accessing the website would contain "contents."[55] Thus, the concept of information similar to IP addresses being contents has been explored in the Fourth Amendment context as well.

Regardless of whether it is an "incoming" or "outgoing" IP address, or whether it is in the context of a statutory or constitutional claim, IP addresses have not been considered "content of communication." Despite this consensus view thus far on IP addresses, courts have continued to move in the direct of considering more information closely related to IP addresses to be content. As discussed, *infra*, other factors are also pulling in the direction of constitutional protection for IP addresses.

3. Other Modern Surveillance and the Fourth Amendment

Though dealing with a different technology, the recent district court decisions addressing the bulk telephony metadata collection program ("telephony program") could impact future analysis of internet usage surveillance.

In *Klayman*, the court rejected the application of *Smith* to the telephony program in granting a preliminary injunction to stop the collection based on a potential Fourth Amendment violation.[56] Since there was no physical intrusion, the court applied the *Katz* "reasonable expectation of privacy" test.[57]

The court determined that it is very likely that the plaintiffs had a "reasonable expectation of privacy" with respect to the specific metadata collection program at hand in this case. The court

[55] *Ibid*.
[56] *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C. 2013).
[57] *Id*. at 30.

reaches this conclusion by not apply *Smith*.[58] The court ultimately concludes that the factual scenario here is so substantially different from that in *Smith* that it does not apply.[59]

The Court went to great lengths to distinguish the factual situations in *Smith* from the one at hand. The Court discussed how the *Smith* Court could not have predicted how phones would be used today when they contemplated their decision.[60] Further, they discussed how the pen register in *Smith* was short-term and very fixed in nature, while the collection here is expansive and long-term.[61] The Court also noted the difference in the relationship the Government had with the phone company, with today's situation being an ongoing almost contractual situation as opposed to a one time collection of information.[62] Finally, the court reasoned that the most important distinguishing factor was that the "nature and quantity of the information contained in people's telephony metadata is much greater" in the telephony program than what was collected in *Smith*.[63] The court discussed how due of the pervasiveness of cell phones in our lives, the metadata, while the same type of information as in *Smith*, allows the Government to glean much more information about a person from the metadata today than they did in 1979.[64]

Having rejected the application of *Smith*, the court determined whether there is a reasonable expectation of privacy without consideration of the third-party doctrine. In doing so, the court accepts plaintiffs' statement that they subjectively expected privacy.[65] The court the concluded

[58] *Id.* at 37.
[59] *Ibid*.
[60] *Id.* at 31.
[61] *Id.* at 32.
[62] *Id.* a 32-33.
[63] *Id.* 33-34.
[64] *Id.* 35-36.
[65] *Id.* at 37.

that the expectation was objectively reasonably.[66] However, in doing so, the court makes clear that its decision is not that individuals have a reasonable expectation of privacy to all metadata, just that they have a reasonable expectation of privacy against the particular surveillance method used by the government in the telephone program.[67]

In *Clapper*, the Southern District of New York reached the opposite conclusion with respect to the same telephony program.[68] This opposite holding was reached because the *Clapper* court determined that *Smith* was applicable to analysis of the telephony program.[69]

The *Clapper* court discusses how the metadata here is not different in any significant way from the metadata at hand in *Smith*.[70] The court rejected plaintiffs' argument that the information in the current case allows for a rich mosaic to be created, because it would require multiple steps by the government outside of the telephony program to create such a picture.[71]

Finally, the court considered the current landscape of related decisions, first making clear that the Supreme Court has not overruled *Smith*.[72] The court then addressed the *Klayman* decision, stating their belief that the court in that case addressed hypothetical issues down the road and mistakenly focused on the expansion of the use of the telephone.[73] The *Clapper* court acknowledges that there is a changing technological landscape, but states that the facts at hand only concerns the telephone as it is used in the traditional sense.[74] Ultimately, the court concludes

---

[66] *Ibid*.
[67] *Ibid.*
[68] *Clapper*, 959 F.Supp.2d 724.
[69] *Id.* at 750-51.
[70] *Id.* at 750.
[71] *Id.* at 750-52.
[72] *Id.* at 752.
[73] *Ibid*.
[74] *Ibid*.

that since *Smith* controls, the NSA's metadata collection program does not violate the Fourth Amendment.[75]

4. Other Approaches that Courts have Considered

Recently, however, the court has begun to question to applicability of *Smith* in the face of changing technologies and societal trends.

The applicability of *Smith* to modern technologies was questioned in a case in front of the United States Supreme Court in the concurrence in *U.S. v. Jones*.[76] This case dealt with the installation of a GPS tracking device on a car by the government, and was ultimately deemed to be a search based on the physical trespass that occurred when the device was installed. Despite agree with the application of the physical intrusion test to the case at hand, in a concurring opinion, Justice Sotomayor questioned the third-party doctrine's merit with respect to modern technologies.

In her concurrence, Sotomayor addresses the potential harms that could come from allowing extensive governmental surveillance.[77] Namely, she identifies that "awareness that the Government may be watching chills associational and expressive freedoms."[78] Further, she recognizes that "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse" and may alter the relationship between government and citizens.[79] Along with this, she notes that there are potential issues that could arise from allowing extensive executive power in this area without oversight from another branch.[80]

---

[75] *Ibid.*
[76] 132 S. Ct. at 954 (Sotomayor J., concurring).
[77] *Id.* at 956.
[78] *Ibid.*
[79] *Ibid.*
[80] *Ibid.*

Sotomayor goes on to discuss how it might be time to reconsider the third-party doctrine in light of changes in both technology and how society interacts with technology.[81] She discusses how people reveal a great deal of information about themselves to third-parties in carrying out mundane tasks based on the nature of current technologies.[82] Sotomayor further states that she would "doubt that people would accept without complaint the warrantless disclosure of every Web site they had visited in the last week, or month, or year."[83] Finally, she discusses how secrecy should no longer be a prerequisite for privacy.[84] She argues that just because something is disclosed to some member of the public for a specific purpose, it should not for that reason alone, lose its Fourth Amendment Protection.[85] However, since the case was resolved based on the physical intrusion, Sotomayor ultimately concluded that this is an issue that must be decided another day.[86]

In *DiTomasso*, the court determined that the defendant had a reasonable expectation of privacy in the contents of his email and chat room communications despite agreeing to terms of service with the websites that they would monitor his activity.[87] The court reached this conclusion by determining that the defendant's recognition that he would be monitored by the service providers did not mean that he consented to being searched by the Government.[88] The court

[81] *Id*. at 957.
[82] *Ibid*.
[83] *Ibid*.
[84] *Ibid*.
[85] *Ibid*.
[86] *Ibid*.
[87] *DiTomasso*, 2014 WL 5462467 at *5-6.
[88] *Ibid*.

applied the reasoning from Justice Sotomayor's concurrence in *Jones*, in reaching the conclusion that the third-party doctrine was inapplicable to the case at hand.[89]

c. How the "Reasonableness" of an Unwarranted Search is Evaluated

A warrantless search is *per se* unreasonable.[90] However, a warrantless search will be valid if it falls under one of the court recognized exceptions to the warrant requirement.[91] As was the case in *Klayman*, discussed *infra*, the exception that could apply to the search in our hypothetical is the "special needs" exception.

The special needs exception involves a balancing test, weighing the individual's privacy right against the government interest at stake. However, the preliminary question that needs to be asked when applying the special needs doctrine is, whether the search serves a purpose independent of normal law enforcement needs.[92] Since the search in this case is aimed at protecting against terrorist attacks, this threshold question would be easily satisfied.

A court will apply a three part balancing test to determine whether the warrantless search is justified and therefore valid under the special needs exception.[93] The three factors are: (1) the nature of the privacy interest allegedly compromised by the search; (2) the character of the intrusion impose by the government; and (3) the nature and immediacy of the government's concerns and the efficacy of the search in meeting them.[94]

---

[89] *Id.* at *6.
[90] *City of Ontario, Cal. V. Quon*, 130 S. Ct. 2619, 2630 (2010).
[91] *Ibid.*
[92] *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000).
[93] *Klayman*, 957 F.Supp.2d at 38 (quoting *Bd. of Educ. V. Earls*, 536 U.S. 822, 830-34 (2002).
[94] *Ibid*.

In *Klayman*, the court analyzed whether the government's warrantless bulk metadata collection program would be deemed valid as a reasonable search under the Fourth Amendment.[95] The court applied the "special needs" doctrine based on the conclusion that this suspicionless search could only be justified if there was a government need beyond normal law enforcement.[96] Thus, the court applied the three part balancing test, to determine whether the warrantless search was valid due to a "special need."[97]

The court in *Klayman* quickly addressed the first two factors, concluding that the plaintiffs have a significant expectation of privacy and that the bulk metadata collection program significantly intruded on that expectation.[98] The court then addressed the third factor, and concluded that the government interest was to increase the speed of investigating terrorism as opposed to generally protecting against terrorism.[99] The court went on to state that the program was not effective in increasing the speed of investigations, citing the lack of evidence of the bulk metadata collection having stopped or aided in stopping any imminent terrorist attacks.[100] Based on this reasoning, the court concluded that the plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the government interests in collecting and analyzing the metadata in question.[101]

---

[95] *Klayman*, 957 F.Supp.2d at 37-38.
[96] *Id*. at 38.
[97] *Id*. at 38-42.
[98] *Id.* at 39.
[99] *Id*. at 39-40.
[100] *Id*. at 40-41.
[101] *Id*. at 41.

III. European Approach to the Right to Privacy on the Internet

The right to privacy is explicitly stated in Article Seven of the Charter of Fundamental Rights of the European Union ("Charter"). Article Seven provides that "Everyone has the right to respect for his or her private and family life, home and communications."[102] Additionally, under Article Eight, the Charter provides "protection of personal data:"

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[103]

The European Court of Human Rights ("ECHR") recently ruled on a case that dealt with a mandate that service providers retain data that would be accessed by the government.[104] The court applied a proportionality test in determining that the legislation authorizing the data retention was invalid as it was not limited to what was strictly necessary to achieve the government's purpose.[105]

The legislation at hand mandated that service providers retain certain user information related to both telephone and internet communications, including the IP addresses of users.[106] The legislation made clear that the substance of communications were not to be retained.[107]

---

[102] *Charter of Fundamental Rights of the European Union*, Art. 7.
[103] *Charter of Fundamental Rights of the European Union*, Art. 8.
[104] *Digital Rights Ireland Ltd. V. Ireland*, C-293/12 (Eur. Ct. H. R. April 8, 2014).
[105] *Id.* at ¶ 69.
[106] *Id.* at ¶ 26.
[107] *Ibid.*

The ECHR concluded that this data, among other things, made it possible to know the identity of the user and who the user was communicating with.[108] The ECHR determined that the data as a whole might allow precise conclusions about the individual to be drawn, including habits of daily life, activities carried out, and social relationships they are involved in.[109]

The ECHR then discussed how fundamental rights of individuals are harmed by this retention program.[110] Specifically, the ECHR focused on Articles Seven and Eight of the Charter.[111] The ECHR discusses how it does not matter if the information is sensitive or whether the person conceived of the information as being protected, all that matters is there was an interference with these rights by retaining this data and providing it to the government.[112]

The ECHR then discussed whether there was a "general interests" that this legislation achieved.[113] The ECHR discussed how the material object of the legislation was to contribute to the fight against serious crime, including terrorism, and the ultimate goal was to enhance public security.[114] The ECHR concluded that this was a "general interest."[115]

Since there was both an infringement of a fundamental right and a general interest, the ECHR applied a proportionality test.[116] Under this test, the legislation must not "exceed the limits

---

[108] *Ibid.*
[109] *Id*. at ¶ 27.
[110] *Id*. ¶ 32.
[111] *Id*. at ¶ 31.
[112] *Id*. at ¶ 33.
[113] *Id*. at ¶ 38.
[114] *Id*. at ¶ 42.
[115] *Ibid.*
[116] *Id*. at ¶ 46.

of what is appropriate and necessary in order to achieve [its] objectives."[117] Essentially, the legislation may only infringe on individual rights where it is "strictly necessary."[118]

The ECHR found that the legislation was not limited to what was strictly necessary to achieve the general interest so it was invalid. Specifically the ECHR was concerned with the broad application of the surveillance and the failure of the legislation to focus the data gathering towards the prevention of crime.[119] Despite the governmental interest in prevention of terrorism, the ECHR was unwilling to uphold the wide-sweeping surveillance legislation under proportionality review since the legislation "entail[ed] a wide-ranging and particularly serious" interference with the individual's protected rights in their privacy and data.[120]

IV. Future of Right to Privacy on the Internet in Light of Concerns of Terrorism

a. How Should the "Reasonable Expectation of Privacy" Standard be Applied in Future Cases?

Despite recent questioning of its long term sustainability, the third-party doctrine announced in *Smith* is the current standard of the United States Supreme Court. While under the current landscape a court will almost certainly find that an individual does not have a reasonable expectation of privacy to their IP address, there are strong policy reasons to change to a standard that protects this information.

---

[117] *Ibid.*
[118] *Id.* at ¶ 52.
[119] *Id.* at ¶¶ 57-60.
[120] *Id.* at ¶ 65.

The concurring opinion of Justice Sotomayor in *Jones* provides a forward thinking perspective on the scope of the Fourth Amendment's privacy protections. Sotomayor focuses on the changes that have occurred in the dynamic between society and technology.

Today, the internet use is so extensive that it occupies a major role in both work and social lives of a significant portion of Americans. The internet has become the dominant and at times exclusive means of communication, research, socialization, and expression for many Americans. Additionally, some content, including much of the information on ISIS, is only available through the internet.

One major problem with the continued growth of internet use in society today is that individual privacy is being sacrificed along the way. Unless a highly skilled individual goes to great lengths to avoid using one, accessing the internet is only possible by using an ISP. While this does not present a problem in terms of using the internet, this reality has major implications on the ability of the Government to monitor internet use.

Since all internet access is achieved through an ISP, all communications on the internet is necessarily conveyed through a third-party. Therefore, all communication on the internet is subject to analysis under *Smith*. As discussed above in *Forrester* and *Christie*, under this analysis, courts have exclusively held that IP addresses are not "content," and thus not protected by the Fourth Amendment. Therefore, any government surveillance that involves obtaining IP addresses is not a "search" and thus never requires a warrant. This conclusion by the courts places the privacy of internet users at great risk.

There are two primary reasons why the court reaches this conclusion. First, court continue to apply the *Smith* doctrine, despite it being inapplicable to the technologies of today. Along with this, courts fail to recognize that IP addresses are "content of communications."

The *Smith* doctrine is inapplicable to the technology of today because it fails to account for the inescapable requirement to relay communication through a third-party. This reality calls into question one of the basic premises of *Smith*, that disclosures to the third-party are voluntary. It cannot be argued that a person voluntarily chooses to send information to their ISP when accessing the internet. However, the voluntariness can be called into question because of the lack of alternatives to the third-party disclosure. As discussed in Justice Sotomayor's concurrence in *Jones*, forcing individuals to choose between, accessing the internet while being monitored and not accessing the internet at all, chills expressive freedoms. Third-party disclosure on the internet is not truly voluntary. Similar to the discussion in *DiTomasso*, the recognition by individuals that they have to disclose information to their ISP should not mean that they are agreeing to disclose their information to the government. As the pervasiveness of the internet in our lives continues to grow, the "voluntariness" of the third-party becomes more questionable. Since voluntariness was a focus of the *Smith* holding, it is time for the Court to reconsider the application of the third-party doctrine to the internet and related technologies.

However, if the *Smith* doctrine continues to be applied to the internet, IP addresses should be considered "content of communications" and thus receive Fourth Amendment protection based on the vast amount of information that can be gleaned from monitoring them. Under current analysis, IP addresses have been analogized with phone numbers that are dialed on a phone. This comparison fail to take into account the expansive picture that can be painted by compiling the IP addresses an individual accesses. As was recognized by the European Court of Human Rights,

tracking an IP address can result in the acquiring of a detailed picture of an individual's life. While the European approach was supported by provisions in their Charter protecting the right to privacy and the right to protection of personal data, the Fourth Amendment must be the source of privacy protection in America. Therefore, courts should abandon the narrow interpretation of what IP addresses contain, and adopt the reasoning of the ECHR.

The conclusions of the ECHR recognize the resulting picture that can be drawn from analysis of large amounts of IP addresses or other metadata in today's world. While an IP address will not show the details of the website or the exact links that are followed while the individual is on the website, there is a great deal that can be revealed in the name of the website itself. Though some IP addresses will not reveal any information on the user, such as www.google.com, there are others that could be very telling and thus allow the government access into private matters. For instance, an individual who is dealing with alcohol abuse might visit websites such as www.quitalcohol.com or www.alcoholrehab.com. Clearly, obtaining these IP addresses would allow the government to know that this individual has an interest in alcohol recovery. The same result could occur with IP addresses related to any number of private issues, such as sexual orientation, gender identity, religious beliefs, and abortions.

An argument has been made that this information can also be gleaned from the phone numbers that are dialed, as was the case in *Smith*. For instance, the government could glean the same alcohol abuse information if an individual that was being monitored dialed the phone number of an alcohol rehabilitation facility. While this is true to some extent, the main difference between the pen registers in *Smith* and the monitoring today is scale, both in terms of individual use and government surveillance.

By determining that IP addresses are not protected by the Fourth Amendment, the courts allow unchecked government surveillance of all internet activity. This approach fails to recognize the privacy interests that are at stake by leaving unprotected the vast amount of information that can be gleaned from IP addresses.

The Court should adopt an approach that more appropriately addresses whether there is a reasonable expectation of privacy, which can be achieved by not focusing on whether the information was disclosed to a third-party. A shift in focus away from disclosure to a third-party will eliminate the content vs. non-content distinction. Instead, the court should return to the basic principles of *Katz* and evaluate whether there is a reasonable expectation of privacy considering both the subjective and objective prongs. While this will involve more balancing of objectiveness by individual courts, it is better than operating under the continued assumption that there is no expectation of privacy as a result of disclosure to an internet service provider.

b. If There is a "Search," How will the Reasonableness of that Search be Evaluated in Light of the Government Interest In Preventing Terrorism?

If it was determined that there was a "search" in the monitoring of our hypothetical, the next step would be to analyze whether the search is valid despite being warrantless. As discussed above, the most likely means of finding the warrantless search valid is under the "special needs" exception.

Analysis under the special needs exception involves a three factor balancing test: (1) the nature of the privacy interest allegedly compromised by the search; (2) the character of the

intrusion impose by the government; and (3) the nature and immediacy of the government's concerns and the efficacy of the search in meeting them.

Considering the first factor, the privacy interest at stake is significant. The interest at stake here is very similar to that of *Klayman*. This is not a case where the environment of the search makes it so there is a diminished expectation of privacy. Instead, examples of when there has been found to be a diminished expectation of privacy under the special needs exception include searches while is on public transportation and while entering into private property such as sports stadiums. While it is clear that the first factor weighs in favor of the search being deemed unreasonable, the lack of diminished expectation of privacy is not determinative on its own.

Next, the court will look to the character of the intrusion of the privacy right. As was the case in *Klayman*, if it is deemed to be a "search," the surveillance at issue would be quite an invasive search. The protected content of the individual's IP address would be fully obtained by the government every time one of the monitored sites is accessed. A further inquiry into the IP address would lead to personal information being obtained, and further surveillance of the IP address would lead to extensive information being obtained about the individual's life.

The major factor weighing in favor of the special needs doctrine applying to the search is that the government interest is protecting against terrorism. There is no doubt that everyone will agree that terrorist prevention is of the highest priority among government interests.

In light of *Klayman*, in which the court framed the government's goal in the telephony program quite narrowly as only being aimed at increasing the speed of investigating terrorism, the primary question would be what the government interest is in the hypothetical. While much of the *Klayman* reasoning is sound and forward thinking, its framing of the government interest is

extremely narrow. It seems likely that future courts to address this issue will move towards a broader reading of the government purpose. With this belief in mind, it seems that the government interest in the hypothetical would be identification of potential terrorist threats.

While this government interest in mind, the court would have to analyze whether the program was efficient in achieving this goal. In *Klayman*, the court looked to the failure of the telephony program to assist in the prevention of any imminent terrorist attacks. A similar analysis would likely occur in our hypothetical.

Having considered the factors individually, the court would then have to weigh all three factors against each other in a balancing test. Based on the above discussion, the court will likely be left with a weighing of a full-fledged privacy interest of the individual against a Government interest in preventing terrorism.

When a similar analysis was done by the ECHR under proportionality review, they reached the conclusion the legislation did not adhere to the requirement of encroaching on individual rights only when it is "strictly necessary" to do so. Under this approach, it seems likely that the hypothetical program would fail as the European statute did. However, it is less clear whether such a result would follow under the special needs balancing test, which applies a less restrictive standard to government intrusion on individual's privacy rights.

V. Conclusion

The current privacy protection for internet content in America fails to account for the realities of modern technology and government surveillance abilities. In order to better protect the privacy on individuals who access the internet, the American approach should follow the lead of

Europe and begin to protect the spectrum of personal information contained in internet browsing data.