PRIVACY DISTORTION RATIONALE FOR REINTERPRETING THE THIRD-PARTY DOCTRINE OF THE FOURTH AMENDMENT

*Saby Ghoshray**

"Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."

—Justice Brandeis[1]

I. INTRODUCTION

Smartphones, Android, Facebook, Twitter, and iChat—each represents a dimension through which post-modern individuals communicate, exhibit emotions, and form communities.[2] In essence, they live their lives wired—connected, uploaded, downloaded, and streamed online.[3] For these wired individuals, fulfilling all of the promises life has

* Dr. Saby Ghoshray's scholarship focuses on Constitutional Law, Corporate Law & Governance, Fourth Amendment jurisprudence, and Cyberspace Law, among others. His work has appeared in a number of publications including, among others, *Albany Law Review*, *ILSA Journal of International and Comparative Law*, *European Law Journal ERA-Forum*, *Toledo Law Review*, *Georgetown International Environmental Law Review*, *Temple Political & Civil Rights Law Review*, *Fordham International Law Journal*, *Santa Clara Law Review*, *Michigan State International Law Journal*, *Loyola Law Journal*, *New England Law Review*, and *Miami Law Review*. The author would like to thank Jennifer Schulke for her assistance in legal research and typing of the manuscript and his beautiful children, Shreyoshi and Sayantan, for their patience and understanding. In addition, the author would like to thank the members of the Editorial Board at Florida Coastal School of Law for their work on the final version of this Article. Dr. Ghoshray can be reached at sabyghoshray@sbcglobal.net.

1 Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

2 *See, e.g.*, *Net Impact: US Becomes a Facebook Nation*, BUS. NEWS DAILY (Apr. 6, 2011), http://www.businessnewsdaily.com/840-facebook-smartphone-majority-americans-online-.html (discussing the continuing rise in Facebook membership among people living in the United States).

3 *See, e.g.*, *id.* (describing the multitude of ways Americans use technology in their everyday lives).

to offer would mean protecting their online privacy as well.[4] Indeed, life's journey requires privacy as an essential element to fulfill its promises.[5] Can we allow the government and its law enforcement agencies to intrude upon this sacred privacy with the thinnest of excuses? Unfortunately, however, privacy violations are occurring in almost every sphere of our lives.[6] These violations are in part enabled by the technology-driven excesses of post-modern society[7] and in part aided by the shaping effect of 9/11.[8] Thus, individual privacy space in the United States has shrunk at an alarming rate during the last decade.[9]

Consider a hypothetical scenario. You are developing an intimate relationship with your partner. Physical distance prompts the majority of intimate exchanges to take place in cyberspace via Twitter, iChat, and Facebook. Should law enforcement be allowed to view, or

---

[4] *See* Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, WALL ST. J., Nov. 15, 2011, http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html (discussing—in a panel format—the impact the Internet has had on daily life and why protecting the privacy of that activity is important).

[5] *Id.* ("Our founding fathers experienced life without privacy protections under the British, when writs of assistance permitted searches of homes at the whim of customs agents. Life without privacy laws was hell under the British, and it would be even worse now, given the powerful surveillance technologies that governments around the world now possess.").

[6] *See, e.g.*, Charlie Savage, *Obama Drops Veto Threat Over Military Authorization Bill After Revisions*, N.Y. TIMES, Dec. 15, 2011, at A30, *available at* http://www.nytimes.com/2011/12/15/us/politics/obama-wont-veto-military-authorization-bill.html (discussing the uncertainty in the government over the legality of a new bill authorizing certain acts by the government that, it is feared, may lead to a dramatic loss in privacy).

[7] *See* Tal Z. Zarsky, *Law and Online Social Networks: Mapping the Challenges and Promises of User-Generated Information Flows*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 741, 742 (2008) (discussing at length the technology-driven changes in communication via social networks).

[8] *See generally* Saby Ghoshray, *Guantánamo: Understanding the Narrative of Dehumanization Through the Lens of American Exceptionalism and Duality of 9/11*, 56 WAYNE L. REV. 163 (providing an in-depth discussion of the shaping effect of 9/11).

[9] *See* Stephen J. Kobrin, *With Technology Growing, Our Privacy Is Shrinking*, PHILA. INQUIRER, Jan. 3, 2001, *available at* http://www-management.wharton.upenn.edu/kobrin/Research/ThePhiladelphiaInquirer.pdf (discussing the shrinking privacy space that has come with the advent of technology in communication).

even get a peek at these intimate exchanges? Should an agent of the government be able to review the content of your communications without a warrant? To do so would be to share your most intimate moments with law enforcement—such prospects are real, and more proximate than remote.[10] Is it not time to drag privacy law into the twenty-first century?[11] I shall explain why it ought to be done.

Emboldened by recent shifts in technology, individuals are increasingly conducting their private lives over the Internet.[12] Empowered by the ease of automation, they instantly communicate with their chosen contacts.[13] Such advancement in technology, however, has not

---

[10] Consider the following excerpt from a recent American Civil Liberties Union (ACLU) document:

> A man and woman who shared an intimate moment on a dark and secluded rooftop in August 2004 learned later that they had been secretly watched by police officers charged with conducting surveillance of nearby protest rallies.
>
> From a custom-built $9.8 million helicopter equipped with optical equipment capable of displaying a license plate 1,000 feet away, police officers tracked bicycle riders moving through the streets of the Lower East Side. Then, using the camera's night vision capability, one officer shifted the focus away from the protestors and recorded nearly four minutes of the couple's activities on the terrace of their Second Avenue apartment.
>
> "When you watch the tape, it makes you feel kind of ill," said Jeffrey Rosner, 51 [*sic*], one of the two who were taped. "I had no idea they were filming me. Who would ever have an idea like that?"

LOREN SIEGEL ET AL., N.Y. CIVIL LIBERTIES UNION, WHO'S WATCHING?: VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT 9 (2006), *available at* www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf.

[11] Regarding the reference to dragging privacy law into the twenty-first century, I generally refer to the inertia in jurisprudence that shows a systemic reluctance to bring privacy protection in cyberspace in lockstep with technological advancement. *See, e.g.*, Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1391-93 (2008) (describing problems with the Fourth Amendment in an age with computers and the Internet).

[12] *See, e.g.*, Brent Johnson, *More People are Turning to Internet Dating*, EZINEMARK (Dec. 11, 2011), http://technology.ezinemark.com/more-people-are-turning-to-internet-dating-7d3272155e72.html (discussing how people are turning more and more to the Internet, often to conduct their most intimate and personal activities, such as finding a romantic partner).

[13] *See id.*; *Online Dating: Reviews*, CONSUMERSEARCH, http://www.consumersearch.com/online-dating (last updated Feb. 2012) (providing a review of the various online

coincided with an enhancement in privacy law.[14] This reality, although recognized in scholarship, has not yet found traction in jurisprudence.[15] Wider access to automation and enhanced functionalities of cyberspace has reconfigured the way individuals interact online in practically all aspects of modern life.[16] Yet, legal protection for such private communications has not evolved accordingly.[17] Therefore, we must take an introspective look at this ever-increasing chasm between privacy law's inert contour and technology's innovative trajectory.[18]

Given that an enormous volume of personal data gets processed through the Internet at a very high frequency,[19] the role of a third party as a technology enabler has become necessary in post-modern communication.[20] Since any form of third-party involvement can provide law

dating sites and making note of the ease of automation and the ability to chat instantly with chosen contacts).

14 *See, e.g.*, Eli R. Shindelman, Note, *Time for the Court to Become "Intimate" with Surveillance Technology*, 52 B.C. L. REV. 1909, 1914 (2011) (noting the struggle courts have to protect privacy in the age of technology).

15 *See, e.g.*, Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 241 (noting that the law has fallen behind technology).

16 *See* Julia Angwin, *How Facebook is Making Friending Obsolete*, WALL ST. J., Dec. 15, 2011, http://online.wsj.com/article/SB126084637203791583.html (discussing the impact Facebook's new privacy policies may have on the way people are currently interacting on the web).

17 *See, e.g.*, Raffi Varoujian, *Legal Issues Arising from the Use of Social Media in the Workplace*, HELIUM (July 29, 2011), http://www.helium.com/items/2204838-legal-issues-arising-from-the-use-of-social-media-in-the-workplace (discussing current tensions which exist between the law and the capabilities of the Internet that have yet to be fully addressed by the law).

18 *See* Moses, *supra* note 15, at 239 (noting we must look at the tension between law and technology more broadly than we have in the past).

19 Recently an expert on data management noted, "The amount of data going through the Internet is so mind-boggling that it deals in numbers that most people are unfamiliar with. According to Cisco, which released its annual Visual Networking Index last week, traffic will reach 966 exabytes by 2015." Carl Weinschenk, *Cisco VNI: The Long Data Explosion Continues*, ITBUSINESSEDGE (June 7, 2011), http://www.itbusinessedge.com/cm/community/features/interviews/blog/cisco-vni-the-long-data-explosion-continues/?cs=47284.

20 Technology-enabled communication has moved beyond the point-to-point communication of yesteryear to a combination of distributed transmission and third-party-enabled communication, where various third-party providers are not only storing data but also processing it to make the system more efficient as well as to enhance the

enforcement with a constitutional ground for privacy intrusion, the time has come to evaluate that constitutional contour.[21] As the decades-old Electronic Communications Privacy Act (ECPA)[22] continues to be the guidepost for governmental intrusion of private communication,[23] individual privacy under the Fourth Amendment remains hijacked by the third-party doctrine.[24] As instances of such doctrinal invocation un-

---

experience of users. *See* Connie Davis Powell, *"You Already Have Zero Privacy. Get Over It!": Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146, 146 n.2 (2011) (noting details on various third-party mechanisms in communication, social media, and Internet).

[21] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly 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.").

[22] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). The Electronic Communications Privacy Act (ECPA) governs how and under what circumstances law enforcement can obtain evidence from an Internet service provider (ISP). *See* 18 U.S.C. § 2703 (Supp. IV 2010). When Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, they intended to provide guidance for law enforcement on using electronic surveillance, particularly wiretaps. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1274-75 (2004). Thus, for all intents and purposes, the 1968 Act did not have specific guidance related to electronic communications. *See id.* In 1986, to address the advances in electronic communications technology and deal with the gaps left in law, Congress passed the ECPA along with the Stored Communications Act (SCA). Electronic Communications Privacy Act of 1986: Stored Wire and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701-2712). SCA was enacted to update "existing Federal wiretapping law to take into account new forms of electronic communications such as electronic mail, cellular telephones, and data transmission by providing such communications with protection against improper interception." Electronic Communications Privacy Act of 1986: Stored Wire and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701-2712); 132 CONG. REC.14885 (June 23, 1986) (statement of Rep. Kastenmeier).

[23] *See supra* note 22.

[24] The third-party doctrine was conceived as an exception to the privacy protection enshrined in the Fourth Amendment of the U.S. Constitution. *See* Secs. & Exch. Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984). The principle can be summarized as follows: "[W]hen a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement

ravel, existing privacy law's uneven growth becomes further unglued.[25] Recent Department of Justice (DOJ) investigations involving WikiLeaks and Twitter communications[26] provide us with such a window to recognize this growing disconnect between technology's advancement and the law's inability to catch up.[27]

The saga in question began on December 14, 2010, when the DOJ obtained a court order compelling Twitter to reveal communication records of selected users associated with an ongoing WikiLeaks investigation.[28] The government sought only noncontent information

authorities." *Id.* at 743 (citing United States v. Miller, 425 U.S. 435, 443 (1976)). The evolution of the third-party doctrine, however, began in the 1970s, when the Supreme Court observed that individuals have no legitimate expectation of privacy in checks, financial statements, and deposit slips subpoenaed from an individual's bank by the government, even where the individual was given no notice of the subpoenas. *See Miller*, 425 U.S. at 442-43 & 443 n.5 (1976). The Court has solidified its holding in a subsequent opinion in *Smith v. Maryland*, where it held that people lack a reasonable expectation of privacy in the phone numbers they dial because people "know that they must convey numerical information to the phone company" and therefore, they cannot "harbor any general expectation that the numbers they dial will remain secret." Smith v. Maryland, 442 U.S. 735, 743 (1979). Jurisprudential development in *Miller* and *Smith* began the doctrinal development of the Court's formulation of a specific kind of privacy exception that has come to be known as the "third-party doctrine." *See* Orin S. Kerr, *The Case for the Third-Party Doctrine,* 107 MICH. L. REV. 561, 569-70 (2009). According to the doctrine, therefore, for any information, including personal communication, that is procured by a third party in a possessory role, an individual connected to the said information relinquishes his or her reasonable expectation of privacy in the information. *See Miller*, 425 U.S. at 443. This brings us face-to-face with the quandary of the automation age in which we live in, as much of what we do is processed by a third party and therefore, might go through a third party's possessory interest. *See infra* Part III. This is where I view the doctrinal stress on the third-party doctrine comes from. This is an area I intend to illuminate in this Article.

25 *See infra* Part III.

26 Scott Shane & John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. TIMES, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html?_r=1&hpw.

27 *See* Orin S. Kerr, *supra* note 24, at 573 (noting that "[s]cholars have responded by contending that the third-party doctrine is 'not responsive to life in the modern Information Age' ") (quoting Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002)).

28 *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11-DM-3, 2011 WL 5508991, at *1 (E.D. Va. Nov. 10, 2011).

from Twitter, pursuant to its authority under the Title 2 of the EECPA of the Stored Communications Act.[29] The authority stems from section 2703(d) (*d*-order),[30] which legalizes disclosure of communication

[29] *Id.* at *4-5.

[30] *See* 18 U.S.C. § 2703(d) (2006 & Supp. IV 2010). The "*d*-order" refers to section 2703 of the ECPA. The language points to specific terms like "[c]ontents of wire or electronic communications" and "[r]ecords concerning electronic communication service or remote computing service" that identify the types of information obtainable under the Act. *Id.* Implication of *d*-order involves the ability to obtain a range of noncontent and content information without a search warrant. *See id.* These include subscriber information, transactional information, and specific content. *Id.* "The PATRIOT Act specifically amended Section 2703(d) of the ECPA to authorize state courts of 'competent jurisdiction' to issue legal process under various sections of the ECPA unless 'prohibited by the law of such State.'" LEONARD DEUTCHMAN & SEAN MORGAN, AM. PROSECUTORS RESEARCH INSTITUTE, THE ECPA, ISPS & OBTAINING E-MAIL: A PRIMER FOR LOCAL PROSECUTORS 7 (2005), *available at* http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf (quoting 18 U.S.C. § 2703(d)). Although originally intended for e-mails, the amendment of the PATRIOT Act allows for voicemail to be "considered the content of stored wire communications." *Id.* at 11. A publication by the American Prosecutors Research Institute outlines the types of legal procedures available under the ECPA. "Three types of legal process are available under the ECPA to obtain content and records information: ECPA warrants, 2703(d) court orders, and subpoenas." *Id.* at 13 & n.9 (noting that "the ECPA warrant is not a search warrant in the traditional sense, as a law enforcement officer does not have to be present at the execution of the ECPA warrant") (internal citations omitted). Section 2703(d) states in part:

> 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.

18 U.S.C. § 2703(d).

> "In addition, depending upon the type of information sought, 2703(d) court orders and subpoenas may require notice to the subscriber. Generally, the more personal the information sought, e.g., e-mail content, the higher the burden of proof for law enforcement to obtain the requisite legal process." The ECPA warrant must be supported by probable cause, the 2703(d) court order by 'specific and articulable facts,' and a subpoena typically by relevance."

DEUTCHMAN & MORGAN, *supra* note 30, at 13 (quoting 18 U.S.C. § 2703(d)) (citations removed). The publication further clarifies the intent of *d*-order as follows in this context:

records to the relevant authorities upon establishing reasonable grounds for seeking such information.[31] While the *d*-order mandates the information to be relevant and material to an ongoing investigation, the statutory standard is of a lower threshold than that of the probable cause standard.[32] While the DOJ's attempt to seek noncontent or "envel-

> The three types of legal process are also inclusive in a hierarchical manner, i.e., with an ECPA warrant, law enforcement can collect all types of information obtainable using a 2703(d) court order or subpoena. Likewise, with a 2703(d) court order, law enforcement can collect all types of information obtainable using a subpoena. Finally, the recent decision of *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) for those states within the jurisdiction of the U.S. Court of Appeals for the Ninth Circuit recently narrowed the available legal process to obtain e-mail content to an ECPA warrant . . . .

Id. at 13.

[31] 18 U.S.C. § 2703(d).

[32] *Id.* The crux of the threshold matter involves the significant difference between a search warrant and a *d*-order, which is that a search warrant must specifically describe items that are evidence of a crime. *See* Groh v. Ramirez, 540 U.S. 551, 557 (2004) (discussing the particularity requirement for a search warrant). A *d*-order only requires "reasonable grounds" for the belief that the item to be seized is "relevant" to a criminal investigation. 18 U.S.C. § 2703(d). Therefore, by removing the link between items sought by law enforcement and the commission of actual crime, the *d*-order broadens the scope of the order with a concomitant attenuation of threshold. *Cf.* Solove, *supra* note 27, at 1109 (discussing similar dangers in computer-matching techniques utilized by the government). In its broader invocation, law enforcement can obtain all sorts of transactional records, including IP addresses, times, and descriptions of all activities on the system, database, and server. DEUTCHMAN & MORGAN, *supra* note 30, at 11-12. This would expand targets of investigations to include all other users communicated with, all sites visited, and all files accessed, among others. *See id.* Under the premise of a *d*-order, law enforcement can submit an "Emergency Disclosure Request Form" articulating potential for imminent danger without specifying or connecting requested items with actual crime. *See* 18 U.S.C. § 2702(b)(8), (c)(4) (2006 & Supp. IV 2010); *see also* FACEBOOK, INC., FACEBOOK LAW ENFORCEMENT GUIDELINES 5 (2010), http://www.nd.gov/dhs/services/mentalhealth/prevention/pdf/fb-us-le-guidelines-2010.pdf (showing a sample "Emergency Disclosure Request Form"). Thus, in the name of averting potential danger, a *d*-order can make the case for reasonableness in the context of the information sought, a much lower threshold than an actual search order, by simply sending a fax on law enforcement agency letterhead, thereby making a mockery of constitutional privacy protection of targeted individuals. *See* 18 U.S.C. § 2702(b)(8), (c)(4).

ope"[33] information regarding private communications might be of tangential significance from a privacy perspective, its broader implication is significant in more ways than not.[34] Below, I will explain why this is.[35]

On November 11, 2011, Judge Liam O'Grady of the U.S. District Court for the Eastern District of Virginia upheld the magistrate judge's order,[36] essentially rejecting all WikiLeaks petitioners' claims.[37] The petitioners challenged the government's order on grounds that warrantless disclosure of such "envelope" information would violate the Fourth Amendment's protection against intrusion upon private communication.[38] In response, the court invoked the third-party doctrine based on the argument that the WikiLeaks petitioners had agreed to Twitter's terms of use involving the applicable privacy policy.[39] The court reasoned that the petitioners' involvement with a third party precluded them from Fourth Amendment protection.[40] This is an example of postmodern communication suffering from privacy violation on account of judicial construction based on a doctrinal framework that has not kept up with the passage of time.[41] In my view, this is constitutionally incomplete and doctrinally unsound.[42]

---

[33] S*ee* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2105 (2009) (noting, "envelope," is a reference to various noncontent information that is used in the processing of information content).

[34] *See* Solove, *supra* note 27, at 1109 (arguing that the government can utilize dossiers of personal information for nefarious purposes).

[35] *See infra* notes 36-42 and accompanying text.

[36] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11-DM-3, 2011 WL 5508991, at *1 (E.D. Va. Nov. 10, 2011); *see also* Somini Sengupta, *Twitter Ordered to Yield Data in WikiLeaks Case*, N.Y. TIMES, Nov. 10, 2011, http://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html.

[37] *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2011 WL 5508991, at *1.

[38] *Id.* at *5.

[39] *See id.* at *22.

[40] *See id.* at *21.

[41] *See* Orin S. Kerr, *supra* note 24, at 573 (discussing how the Fourth Amendment applies narrowly to the Internet communications and how the third-party doctrine is an anachronism in the "modern Information Age.").

[42] As Justice Marshall explained in *Smith v. Maryland*, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all." Smith v. Maryland, 442 U.S. 735, 749

For starters, there is a universal recognition of privacy as the steppingstone for fulfilling the promise of individual liberty.[43] However, the judicial construction above attempts to destabilize this privacy framework by triggering an exclusionary feature of the constitutional doctrine that relies on an essential feature of a post-modern societal norm.[44] Post-modern communication depends on a third party for its data processing needs.[45] How does the post-modern individual retain individual privacy—especially if an essential element of communication can trigger constitutionally sanctified governmental intrusion? This facial inconsistency calls for a reevaluation of the constitutional framework the government uses for privacy intrusion.[46] As legal debates cut across both sides of the argument, it is time to examine the privacy distortion rationale of the third-party doctrine.[47] This Article examines

(1979) (Marshall, J., dissenting). Daniel Solove also argued that the third-party doctrine confuses privacy as "total secrecy[,]" Solove, *supra* note 27, at 1086, and Richard Posner argued that "[o]ne must not confuse solitude with secrecy[,]" RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006)).

43 *See* Scott Ness, Comment, *The Anonymous Poster: How to Protect Internet Users' Privacy and Prevent Abuse*, 2010 DUKE L. & TECH. REV. 8, ¶ 1 (noting that the right to privacy is recognized in the Universal Declaration of Human Rights).

44 *See generally In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2011 WL 5508991 (ruling that the third-party doctrine applies to Twitter).

45 Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard*, The Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 769 (2011).

46 *See infra* note 47 and accompanying text.

47 The need for reinterpreting or completely overhauling the third-party doctrine has been argued from both sides of the aisle. *See* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1250-54 (1983) (noting arguments both for and against the third-party doctrine). In the context of scholarship criticizing the doctrine there remains two distinct groups. I consider the first group as trailblazers who began the movement of professing the doctrinal difficulties against technological advancement beginning in the 1980s. *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy"*, 34 VAND. L. REV. 1289, 1315 (1981) (arguing that most citizens would believe the numbers they dialed on their phone would be private and not subject to a search); Loewy, *supra* note 47, at 1269 (noting the third-party doctrine may allow the government to use evidence obtained from installing an "electronic eavesdropping device" in a person's home illegally); Scott E. Sundby, "*Everyman"'s Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1758 (1994) (arguing a court in a different time may have reached different conclusions about privacy rights contained in the Fourth Amendment).

While these articles questioned the doctrine's continued viability even before the mass assimilation of cyberspace enabled social media, the second group has been more persuasive in their argument because of the very same reasons. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-64 (2007) (arguing that two rationales, normative and descriptive flaws, depict the inherent problems with the acquisition of information through the third-party doctrine); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19-21 (2008) (arguing that the Fourth Amendment currently provides limited to non-existent protection of information held on third-party private servers and that the most viable form for protecting this information could be through legislative, administrative, or technological means); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 211-15 (2006) (arguing that third party sources called collectors are constantly retaining data that the original consumer likely thought was protected, but the government may now attempt to legally acquire through the third-party doctrine); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 7-9 (arguing that courts have failed to address the constitutional protection of new electronic communications due to a lack of competence, and that courts should evaluate these communications based on whether an individual should be entitled to view their communication as a private one); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 981-85 (2007) (arguing that information placed in the hands of a third-party should still receive a reasonable expectation of privacy); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113 (2008) (arguing that the belief that exposure of information to a third party, known as the stranger doctrine, does not equate to exposing the information to the government, and that such an interpretation would almost result in the end of the Fourth Amendment); Solove, *supra* note 27, at 1093–94 (arguing that the Internet collects and maintains a substantial amount of data that the government may acquire through the third-party doctrine). On the other hand, scholars have argued passionately as to why the doctrine should retain continued relevance in jurisprudence. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 460 (2008) (arguing that the current trend in Supreme Court jurisprudence is to reduce the protection of privacy rather than expand it, with the exception of in the actual home, and that to reverse this course "would require a fundamental shift in the Court's jurisprudence"); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 519–22 (2007) (arguing that judges should use a policy model when determining the reasonable expectation of privacy by weighing the particular governmental activity against the privacy and security interests and then opt for the better rule); Kerr, *supra* note 24, at 573 (arguing that the third-party doctrine ensures neutrality in Fourth Amendment rulings, and ensures that wrongdoers are not able to hide their wrongdoings through use of a third party).

the debate surrounding the third-party doctrine's continued viability against the law's expected response to post-modernity.[48]

The mode of communication has changed from the founding period.[49] In their conception of the Fourth Amendment, the Framers could have never envisioned how automation would reshape the modes of individual exchanges. Indeed, the evolving view of post-modern community is a far cry from the Framers' analytic view.[50] As we ponder over the governmental intrusion in our technology-fueled privacy space, we must attempt to understand how the original intent of the Framers may contradict with aspirations of today's society.[51] Is it possible for the post-modern individual to relinquish his or her smartphone, do away with texting, or give up chatting via cyberspace? Perhaps the only way today's individual can immunize herself from the dreaded lock of the third-party doctrine is by rejecting the elemental dimensions of communications. Or, should this be necessary? To analyze this quandary, this Article examines the third-party doctrine's continued viability by proceeding along two distinct threads of inquiry.[52] In Part I, I analyze the factors that have contributed towards stressing the contours of the third-party doctrine.[53] The development then leads to further identifying the societal bounds of privacy space in the post-modern era to determine whether the old doctrine is still viable against an onslaught of technological advancement.[54]

Part II describes the emergence of a newer and more restrictive paradigm in law that attempts to retrace the foundational steps of the third-party doctrine.[55] Although the doctrinal journey is inconsistent with realities on the ground, the philosophical reasoning for this retracing is

---

48 *See infra* Parts II-IV.

49 *See, e.g.*, Cate, *supra* note 47, at 456-59 (describing the great technological advances over the last few decades).

50 *See infra* Part II.

51 *See e.g.*, Jules Lobel, *"Little Wars" and the Constitution*, 50 U. MIAMI L. REV. 61, 72 (1995) (arguing that the Constitution should be interpreted as a "living document," and when fundamental societal changes occur, the Constitution can be interpreted based on society's current needs).

52 *See infra* Parts II, III.

53 *See infra* Part II.

54 *See infra* Part III.

55 *See infra* Part II.

significant.[56] In this part, I analyze the reasons and examine societal factors that contributed to the law's evolution in this direction.[57] Part III examines how this traditional Fourth Amendment doctrine is hopelessly inadequate to account for the invasion of privacy brought upon by technological advancement.[58] Here, I explore in detail two distinct phenomena: first, an examination of the disparity between the technological space in which society is evolving and the trajectory of Fourth Amendment jurisprudence signaling a tangible distortion in the law's evolution;[59] second, the meaning of privacy within the context of postmodern individual aspiration evaluated to observe the law's inertia in cyberspace.[60] Finally, Part IV concludes that the third-party doctrine may be inadequate in dealing with the technological advancement of the cyber era and, therefore, we must abandon the traditional analysis based on the decades-old notion of the third-party doctrine.[61]

II. Examining the Current Contour of the Third-Party Doctrine

Waves of requests for customer data from law enforcement agencies are inundating today's communication service providers[62]—a phenomenon that has become too familiar and can be considered an organic outgrowth of the shaping effect of 9/11.[63] But, how and why is this occurring? By allowing individuals to share e-mails, photographs, spreadsheets, and love letters, the ease of automation has made interaction among individuals seamless, smooth, and instantaneous.[64] Increasing varieties of private communications has also enhanced individuals' exposure to targeted intrusion by law enforcement.[65] With an explosion

---

[56] *See infra* notes 62-74 and accompanying text.

[57] *See infra* notes 66-71 and accompanying text.

[58] *See infra* Part III.

[59] *See infra* Part III.C-D.

[60] *See infra* notes 216-26.

[61] *See infra* Part IV.

[62] Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. Times, Jan. 10, 2011, at A1.

[63] *See id.*

[64] *See* Powell, *supra* note 20, at 146.

[65] *See* Sara E. Brown, Comment, *An Illusory Expectation of Privacy: The ECPA Is Insufficient to Provide Meaningful Protection for Advanced Communication Tools*, 114 W. Va. L. Rev. 277, 278 (2011).

of community formation via smartphones, Facebook, Twitter, MySpace, and the like, content and noncontent information has become extremely abundant and enticing for law enforcement.[66] Even if we concede, for the purpose of this discussion, that prevention of terrorism and combating crime depends on access to information, the absence of standards borne out of asymmetric interpretation by judges would make confusion worse confounded.[67] This is where the shaping effects of 9/11 take center stage.[68] Law enforcement agencies including the DOJ have called for individuals' expectation of privacy to be subjugated by their investigative needs.[69] With post-9/11 legislative excesses granting broad surveillance power,[70] the judiciary has made wiretapping and snooping on private citizens even easier.[71] Even think tanks contribute their part in professing the investigative need for excessive law enforcement surveillance.[72] This backdrop to the legal landscape is contextually significant for an understanding of how the contours of privacy in twenty-first-century America have developed.[73] And, the case in point involving WikiLeaks and Twitter is the prism through which I shall evaluate the need to reinterpret the third-party doctrine of the Fourth Amendment.[74]

---

66 *Id.*

67 *Cf.* Lindsay Mather, Comment, *The "Other" Parent: Protecting the Rights of Noncustodial Parents in Emergency Removal Situations*, 79 U. CIN. L. REV. 1189, 1207-08 (2011) (noting that a lack of standards can lead to officials being uncertain of the law). The saying, "Confusion worse confounded" implies confusion made even worse. This term was made famous from the epic poem of the 17th Century by John Milton. *See* JOHN MILTON, PARADISE LOST 133 (Univ. of Chi. 1989).

68 *See generally* Ghoshray, *supra* note 8 (providing an in-depth discussion of the shaping effect of 9/11).

69 *See* Saby Ghoshray, *Untangling the Legal Paradigm of Indefinite Detention: Security, Liberty and False Dichotomy in the Aftermath of 9/11*, 19 ST. THOMAS L. REV. 249, 264 (2006).

70 *Id.* at 273.

71 Kyle Sommer, Note, *Riding the Wave: The Uncertain Future of RFID Legislation*, 35 J. LEGIS. 48, 72-73 (2009).

72 Helft & Miller, *supra* note 62 ("'When your job is to protect us by fighting and prosecuting crime, you want every tool available,' said Ryan Calo, director of the consumer privacy project at the Center for Internet & Society at Stanford Law School. 'No one thinks D.O.J. and other investigative agencies are sitting there twisting their mustache trying to violate civil liberties. They're trying to do their job.'").

73 *Id.*

74 *See infra* notes 75-84 and accompanying text.

In a series of disclosures, WikiLeaks unveiled some uncomfortable truths about international diplomacy.[75] As the inner workings of Guantánamo Bay,[76] the coalition force atrocities in Iraq and Afghanistan,[77] and the failure of United Nations (UN) investigations of wartime

---

[75] *See* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 327-28 (2011) ("The contents of the overwhelming majority of released cables ranged from the genuinely important (e.g., Saudi and Gulf state support for a U.S.-led attack on Iran to prevent proliferation; Yemeni acquiescence in U.S. bombing on its own territory; U.S. spying on UN staff; U.S. intervention in Spanish, German, and Italian prosecution processes aimed at U.S. military and CIA personnel over human rights abuses of citizens of those countries; the known corruption and ineptitude of Afghan President Hamid Karzai) to the merely titillating (Libyian leader Muammer Gadaffi's Ukranian nurse described as a "'voluptuous blonde'"). Although none broke ground in a way that was likely to influence U.S. policy in a fundamental way, this was not always true of other countries. The most ambitious speculations, in the *New York Times* and *Foreign Policy*, suggested that WikiLeaks' cables' blunt descriptions of the corruption of Tunisian President Ben Ali helped fuel the revolution that ousted him in January 2011.") (footnote omitted); Scott Shane, *Cables from American Diplomats Portray U.S. Ambivalence on Tunisia*, N.Y. TIMES, Jan. 16, 2011, at A14; Scott Shane, *Keeping Secrets Wikisafe*, N.Y. TIMES, Dec. 12, 2010, at WK1; Elizabeth Dickinson, *The First WikiLeaks Revolution?*, FOREIGN POL'Y (Jan. 13, 2011, 6:17 PM), http://wikileaks.foreignpolicy.com/posts/2011/01/13/wikileaks_and_the_tunisia_protests; David Leigh & Luke Harding, *WikiLeaks: Strained Relations, Accusations–and Crucial Revelations*, GUARDIAN (Jan. 31, 2011), http://www.guardian.co.uk/world/2011/jan/31/wikileaks-embassy-cables-publication; David Leigh, *How 250,000 US Embassy Cables Were Leaked*, GUARDIAN (Nov. 28, 2010), http://www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked; *US Embassy Cables: The Background*, BBC NEWS (Nov. 29, 2010), http://www.bbc.co.uk/news/world-us-canada-11862320; *WikiLeaks Embassy Cables: The Key Points at a Glance,* GUARDIAN (Dec. 7, 2010), http://www.guardian.co.uk/world/2010/nov/29/wikileaks-embassy-cables-key-points.

[76] *See* Benkler, *supra* note 75, at 319; Marisa L. Porges, *'We Cannot Deal with These People': WikiLeaks Shows True Feelings on Guantánamo*, CHRISTIAN SCI. MONITOR (Nov. 30, 2010), http://www.csmonitor.com/Commentary/Opinion/2010/1130/We-cannot-deal-with-these-people-WikiLeaks-shows-true-feelings-on-Guantanamo.

[77] *See* C.J. Chivers et al., *View is Bleaker than Official Portrayal of War in Afghanistan*, N.Y. TIMES, Jul. 26, 2010, at A1; Nick Davies & David Leigh, *Afghanistan War Logs: Massive Leak of Secret Files Exposes Truth of Occupation*, GUARDIAN (Jul. 25, 2010), http://www.guardian.co.uk/world/2010/jul/25/afghanistan-war-logs-military-leaks; Chris McGreal, *Wikileaks Reveals Video Showing US Air Crew Shooting Down Iraqi Civilians*, GUARDIAN (Apr. 5, 2010), http://www.guardian.co.uk/world/2010/apr/05/wikileaks-us-army-iraq-attack; *WikiLeaks Posts*

brutalities in Iraqi villages[78] became the focal point of global discourse,[79] the U.S. government needed to put a stop to WikiLeaks' publications.[80] Not only did the DOJ want to stop such disclosures, it

Video of 'US Military Killings' in Iraq, BBC NEWS (Apr. 6 2010), http://news.bbc.co.uk/2/hi/americas/8603938.stm.

[78] *See WikiLeaks Posts Video of 'US Military Killings' in Iraq*, *supra* note 77; McGreal, *supra* note 77.

[79] *See DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon*, U.S. DEPARTMENT OF DEF. (Nov. 30, 2010), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4728 ("Now, I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer, and so on. . . . Many governments–some governments deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, as has been said before, the indispensable nation. So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another. Is this embarrassing? Yes. Is it awkward? Yes.") (statement of former Defense Secretary Gates).

[80] Benkler, *supra* note 75, at 331-32. In the spirit of continued distortion of facts, overemphasizing the fallout of national security, post-WikiLeaks disclosures saw the administrative machinery in full swing to discredit, dismember, and ultimately mute WikiLeaks. *See id.* at 313. Amazingly, yet predictably, the Obama Administration found willing allies in both conservative media and politicians in their well-concerted fight against WikiLeaks. *Id.* Prof. Benkler has captured the mood of the Administration and its conservative allies in the following excerpts from his working draft article:

> The invitation by Secretary Clinton and Vice President Biden to respond to dissemination of confidential information as an assault on our national pride and integrity, on par with terrorism, was complemented by calls to use the techniques that the U.S. has adopted in its "War on Terror" against Julian Assange or Wikileaks as a site. Bob Beckel, the Fox News commentator who had been a Deputy Assistant Secretary of State in the Carter Administration and had been campaign manger to Walter Mondale, said, "'A dead man can't leak stuff . . . . This guy's a traitor, he's treasonous, and he has broken every law of the United States. And I'm not for the death penalty, so . . . there's only one way to do it: illegally shoot the son of a bitch.'" This proposal was met with universal agreement by the panel on the program. Republican Representative Peter King, then-incoming Chairman of the House Homeland Security Committee, sought to have WikiLeaks declared a foreign terrorist organization. Right-wing commentators picked up this line. William Kristol wrote in the *Weekly Standard*:
>
> > Why can't we act forcefully against WikiLeaks? Why can't we use our various assets to harass, snatch or neutralize Julian Assange and his collaborators, wherever they are? Why can't we disrupt and destroy WikiLeaks in both

planned to retaliate by making connected individuals criminally liable.[81] Therefore, this section traces the causal nexus between unreasonable adherence to the third-party doctrine in the WikiLeaks investigation and the shaping effect of 9/11.[82] By examining how the post-9/11 landscape has unreasonably and asymmetrically enhanced the overarching tendencies of law enforcement, this Article notes that, by granting broader surveillance power to law enforcement, Fourth Amendment jurisprudence is being erroneously applied.[83] In the following discussion, I argue for the recognition that the third-party doctrine has come to a breaking point, driven more by the shaping effect of 9/11 than the individual's use of technology to subvert law.[84]

A. Shaping Effect of 9/11 and Stress on the Third-Party Doctrine

The post-9/11 landscape differs from any other significant historical event in a unique way.[85] September 11 both introduced an existential threat and reenergized American exceptionalism through a faulty construction that had lingering and debilitating effects on jurisprudence.[86] Although American exceptionalism broadly refers to the opinion that the United States is structurally, fundamentally, and

> cyberspace and physical space, to the extent possible? Why can't we warn others of repercussions from assisting this criminal enterprise hostile to the United States?
>
> He concludes with the remarkable statement: "Acting together to degrade, defeat, and destroy WikiLeaks should be the first topic discussed at today's White House meeting between the president and the congressional leadership. (citations omitted) (alterations in original).

Id. at 331-32 (quoting *Fox News' Bob Beckel Calls for 'Illegally' Killing Assange: 'A Dead Man Can't Leak Stuff*,' HUFFINGTON POST (May 25, 2011, 7:15 PM), http://www.huffingtonpost.com/2010/12/07/fox-news-bob-beckel-calls_n_793467.html & quoting William Kristol, *Whack WikiLeaks*, WKLY. STANDARD (Nov. 30, 2010, 8:25 AM), http://www.weeklystandard.com/blogs/whack-wikileaks_520462.html).

81 Benkler, *supra* note 76, at 365.

82 *See infra* Part II.A.

83 *See e.g.*, Ateqah Khaki, ACLU, *Surveillance in Post-9/11 America*, BLOG OF RTS. (Oct. 13, 2011, 3:40 PM), http://www.aclu.org/blog/national-security/surveillance-post-911-america (arguing that "it is time to stop loosening privacy standards").

84 *See infra* Part II.A-B.

85 *See infra* notes 86-102 and accompanying text.

86 *See* Ghoshray, *supra* note 69, at 261-64 (discussing the illegitimacy of post-9/11 detentions at Guantánamo and subsequent challenges raised at the Supreme Court).

qualitatively different from other nations,[87] society in general may have misconstrued its true connotation of exceptionalism post-9/11,[88] since the elements of imperialism and warmongering continued to reverberate, not only through Guantánamo, but also through the law's general domestic contour.[89] Intuitively, the events of 9/11 represented an overpowering national shame, a defeat of massive proportion, something the country has not seen since the 1941 attack on Pearl Harbor.[90] However, the enormity of 9/11 much surpassed Pearl Harbor in the magnitude of

---

[87] *See* Harold Hongju Koh, *America's Jekyll-and-Hyde Exceptionalism*, *in* AMERICAN EXCEPTIONALISM AND HUMAN RIGHTS 111, 111-15 (Michael Ignatieff ed., 2005); SEYMOUR MARTIN LIPSET, AMERICAN EXCEPTIONALISM: A DOUBLE-EDGED SWORD 17-20 (1996).

[88] Here I refer to the false sense that percolates the mindset of common citizens, which has manifested in both virulent anti-immigrant sentiment and also a misconstrued meaning of exceptionalism in the mind of the common American, and can be seen through the mass hysteria and debilitating fear that has gripped the citizens since 9/11. *See, e.g.*, Margareth Etienne, *Making Sense of the Ethnic Profiling Debate*, 80 MISS. L.J. 1523, 1524-25 (2011) (discussing the detention of Arab and Muslim foreign nationals following 9/11). In my view, this psychosis is borne out of America's perpetual quest for invulnerability and faulty conception of freedom that becomes synonymous with the threat of insecurity. *See* Harold Hongju Koh, *Foreword: On American Exceptionalism*, 55 STAN. L. REV. 1479, 1497 (2003). American citizens are living in cultural isolationism, accentuated by the successive administration's policy of imbibing an exaggerated version of patriotic fervor that gives rise to bellicose nationalism, misidentified as American exceptionalism. *See* Leslie Gielow Jacobs, *Bush, Obama, and Beyond: Observations on the Prospect of Fact Checking Executive Department Threat Claims Before the Use of Force*, 26 CONST. COMMENT. 433, 438-39 (2010) (noting the Bush Administration invoked patriotism to build support for foreign policy initiatives). This is a framework where voices of dissent and individuality get submerged by a manufactured sense of insecurity, which allows the proliferation of a faulty sense of differentiation from citizens of the world. In this construct, the inability of the American people to take the blinders from their eyes disables them from seeing the abrogation of civil liberties, both domestically and dealing with the overall detention mechanism.

[89] *See* Ghoshray, *supra* note 8, at 218-19.

[90] *See* Donna Miles, *Pearl Harbor Parallels 9-11*, MILITARY.COM (Dec. 7, 2006), http://www.military.com/NewsContent/0,13319,120133,00.html (noting the attack on Pearl Harbor "stood as the most devastating enemy attack on U.S. soil" until September 11, 2001). *See generally* THE PEARL HARBOR PAPERS: INSIDE THE JAPANESE PLANS (Donald M. Goldstein & Katherine V. Dillon eds., 1993) (discussing the attack on Pearl Harbor).

existential threat it presented.[91] Enmeshed in the post-9/11 fear psychosis,[92] the new manifestation of American exceptionalism traveled from the masses to the military establishment, from the administrative parlance to the security establishment in an ambience of mass paranoia, where every citizen wanted to embrace an entity that would insulate them from this existential threat.[93] Restrictive covenants in law enforcement became such an entity, whereby encroaching upon individual liberty was seen as the existential need for security.[94] Post-9/11's shaping effect on domestic law must be understood in this deeper context.[95]

The existential threat presented by 9/11 not only brought forth paralytic psychosis,[96] but it also temporarily decoupled the populace from that entrenched feeling of exceptionalism.[97] The feeling of defeat was so deep in the populace[98] that the human construct needed a mecha-

---

91 *See, e.g.*, John D. Ashcroft, *Luncheon Address: Securing Liberty*, 21 REGENT U. L. REV. 285, 288 (2008-2009) (noting the attack on Pearl Harbor was an attack on a military institution and the attack of a civilian target on 9/11 caused a number of other concerns for the country).

92 *See* Ghoshray, *supra* note 8, at 195-96.

93 *See id.*

94 *Id.*

95 *See supra* notes 86-95 and accompanying text.

96 *See* Ghoshray, *supra* note 8, at 195-96.

97 *See id.*

98 This can be understood from the framework of American exceptionalism. A misconstrued notion of "exceptionalism" manifested itself in developing a distorted sense of vulnerability post-9/11, which provoked a mad quest for "invulnerability" within the social construct. *See* Koh, *supra* note 88, at 1497. While literature is replete with references, media has carefully crafted the image that "America is a world unto itself," such that the physical attack of 9/11 magnified multifold in its psychological impact domestically. *See* Paul Dibb, *America – a World unto Itself*, ON LINE OPINION (Jan. 29, 2007), http://www.onlineopinion.com.au/view.asp?article=5428. Despite the advancement of technology narrowing the physical gap between the United States and the rest of the world, America has become both a very *involved, yet surprisingly aloof nation* as it relates to international affairs. *Compare* Tom Koch, *Care, Compassion, or Cost: Redefining the Basis of Treatment in Ethics and Law*, 39 J.L. MED. & ETHICS 130, 135 (2011) (noting that the United States has spent more than a trillion dollars to support the invasions of Afghanistan and Iraq over the past ten years), *with* Aya Gruber, *An Unintended Casualty of the War on Terror*, 27 GA. ST. U. L. REV. 299, 302 (2011) (noting that America has become more isolationist after 9/11). This isolationist viewpoint, therefore, not only accentuates America's sense of vulnerability, but also provides a snapshot of how the national collective

nism to deal with the decoupling in order to feel normal again.[99] Resorting to a security-centric mindset and promoting war hysteria was the mechanism advanced by the government.[100] Against this backdrop, the administration and law enforcement promoted an environment where the judiciary may have inadvertently advanced the security agenda of law enforcement.[101] The natural outcome is restrictions in individual liberty with a concomitant retrenchment of contours of privacy.[102]

With this understanding of 9/11's contribution as rigorously shaping jurisprudence, it is easier to see how the prevailing mindset may have contributed to overextending the already fragile framework of the third-party doctrine related to the Fourth Amendment.[103] Justices of the Supreme Court duly noted in 1928 that applying an outdated and largely static law can become both difficult and incongruent with evolving technology.[104] In the jurisprudential legacy of the Fourth Amendment, the third-party doctrine has been rather latent in the pre-Internet era[105] and has evolved through a series of opinions ranging from organ-

consciousness may have been manipulated into developing an existential vulnerability, while developing an intensely defeatist attitude that requires an earth-shattering response. *See* Ghoshray, supra note 8 , at 218-20.

99 *See* Ghoshray, *supra* note 8, at 195-96.

100 *See* Koh, *supra* note 89, at 1497 ("In the name of preserving American power and forestalling future attack, the United States government has instituted sweeping strategies of domestic security, law enforcement, immigration control, security detention, govermental secrecy and information awareness at home . . . through strategies of preemptive self-defense if necessary.") (internal citations omitted).

101 *See* Thomas Crocker, *Still Waiting for the Barbarians: What is New about Post-September 11 Exceptionalism*, 19 LAW & LITERATURE 303, 308-09 (noting that the Supreme Court decisions in *Hamdi v. Rumsfeld* and *Hamdan v. Rumsfeld* were mere "procedural solutions that leave unasked and unanswered the underlying substantive questions about what is being done through this perhaps new exceptionalism").

102 *See id.* at 309.

103 *See* Henderson, *supra* note 47, at 982-83 (discussing the increase in access to third-party information after September 11, 2001).

104 *See* Olmstead v. United States, 277 U.S. 438, 472-73 (1928).

105 Although *Olmstead* did not directly address or introduce the third-party doctrine, it did sow the seeds of what would eventually become such. United States v. Miller, 425 U.S. 435, 443 (1976) (stating the third-party doctrine). *See generally Olmstead*, 277 U.S. 438 (discussing the expectation of privacy regarding information disclosed to third parties). The *Olmstead* Court, in observing that telephone wires extending beyond a citizen's property were no more protected from government monitoring than

ized crime,[106] bootleggers,[107] government informants,[108] bank records,[109] and telephone directories.[110] In each of these cases, the Court shaped and refined the contours of the Fourth Amendment; yet, it did not provide formalistic validity to the third-party doctrine until *Smith v. Maryland.*[111] Observing that the Fourth Amendment protection did not apply to dialed telephone numbers, on grounds of their existence having been predisclosed to a third party, the Court deflated the privacy contours for individuals.[112] Its implication, however, would go

---

the highways under which they were constructed and along which they were stretched, introduced the concept of information that has been shared *a priori* before eventual intervention by law enforcement. *Id.* at 465. Law enforcement would not violate individual privacy if it took advantage of any fruit of technology that has exposed private content to entities outside of a person's immediate surroundings. *See id.* at 465-66. The holding of *Olmstead* essentially opened the door for a more formalistic construction that the Fourth Amendment does not protect any information willingly disclosed to a third party and obtained by the government from the said third party. *See Miller*, 425 U.S. at 443. And, the Court developed its formalistic construction through a series of cases beginning in the 1950's involving undercover agents and third parties. *See, e.g.*, On Lee v. United States, 343 U.S. 747, 757-58 (1952) (holding that the use of "false friends" or informers was an issue of credibility rather than an issue of evidence).

106 *See* Hoffa v. United States, 385 U.S. 293, 296 (1966).

107 *See Olmstead*, 277 U.S. at 455.

108 *See* Lewis v. United States, 385 U.S. 206, 206-07 (1966); Lopez v. United States, 373 U.S. 427, 430 (1963); *On Lee*, 343 U.S. at 749.

109 *See Miller*, 425 U.S. at 436.

110 *See* Smith v. Maryland, 442 U.S. 735, 736-37 (1979).

111 *Id.* at 743-44.

112 The crux of the matter was to consider whether use of a pen register to record the phone numbers that have been dialed from a landline violated the Fourth Amendment. *Id.* at 736-37. Although installation of a pen register for the purpose of extracting information that was not apparent would otherwise constitute a "snooping" mechanism, the Court held it did not amount to a privacy violation. *See id.* at 745-46. The Court justified its holding by construing that people, in general, do not have any actual expectation of privacy in the numbers they dial, in part due to the fact that the telephone company retains the information for legitimate business purposes. *Id.* at 743. The Court said that telephone users

> typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these

further than originally intended.[113] By its continued invocation for the next several decades, *Smith* continued to illuminate the concept of individual privacy in a complex, increasingly connected, and highly automated world—one much different than existed during *Smith*.[114] The Court's emphasis on an individual relinquishing his or her reasonable expectation of privacy for information disclosed to a third party[115] has continued to assist law enforcement in intruding upon individuals, especially today.[116] Thus, a careful delineation will separate circumstances

> circumstances, harbor any general expectation that the numbers they dial will remain secret.

Id.

113 *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (holding there was "no legitimate expectation of privacy in records held by a third-party cell phone company identifying which cell phone towers communicated with defendant's cell phone at particular points in the past").

114 *See id.* (reasoning that *Smith* and the third-party doctrine "should be extended to cell-site data").

115 *See Smith*, 442 U.S. at 742.

116 *See, e.g.*, *Benford*, 2010 WL 1266507, at *3. *Smith* opened the door for the government to argue that the holding in *Smith* logically extends to cases involving other variants of call directories and private records. *Id.* at *3. While government lawyers could argue that an individual relinquishes an expectation of privacy by disclosing information to a third party, a defendant's lawyers could argue that other records might disclose more information than that revealed in a pen register as in *Smith*. Brief of Amici Curiae at 7-8, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 630 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866619. Therefore, the application of *Smith* would depend on how the courts would equate a *Smith* defendant's reasonable expectation of privacy in the contents of a pen register with those of other personal items capable of record keeping. *See, e.g.*, United States v. Hynson, No. 05-576-2, 2007 WL 2692327, at *5 (E.D. Pa. Sept. 11, 2007) (equating the holding in *Smith v. Maryland* to cell phone companies). However, several courts have relied on *Smith v. Maryland* to hold that a person does not have a reasonable expectation of privacy in the records of incoming and outgoing calls contained on a cell phone. *See, e.g.*, *id.*; United States v. Solomon, No. 02:05cr385, 2007 WL 927960, at *3 (W.D. Pa. Mar. 26, 2007); United States v. Perez Alonzo, No. CRIM03 221(1),(2) A, 2003 WL 22025863, at *2 (D. Minn. Aug. 27, 2003). For example, in *Securities Exchange Commission v. Jerry T. O'Brien*, the Court observed, "[W]hen a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities." Secs. & Exch. Comm'n v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984). Similarly, the Supreme Court in *United States v. Miller* observed, that individuals have no legitimate expectation of privacy in checks,

falling under such assertions from scenarios involving cyberspace or automation, as they invariably require the involvement of third parties for the processing needs of communication.[117] Therefore, we must focus on the unannounced element of *Smith v. Maryland*—a recognition that revolves around the quality of the interception made by a third party.

Blanket application in the post-modern era compels us to evaluate the continued relevance of the third-party doctrine based on precedent such as *Smith*.[118] Jurisprudence is failing to account for the incongruence between community formation online and the context of precedent opinions.[119] There is a fundamental disconnect between societal evolution as manifested via current activities on the Internet and the contextual origination of earlier opinions.[120] The precedents emerged before high-frequency Internet-driven activities came to everyday prominence.[121] In the high-frequency Internet-activated paradigm, sophisticated computer technology enables access and eases transmission of voluminous personal data, all within the blink of an eye.[122] Thus, a third party may have a possessory interest in such data, but they may be

financial statements, and deposit slips that have been shared with third parties and obtained by the government, despite the said individual having no knowledge of government activities. United States v. Miller, 425 U.S. 435, 442-43 & 443 n.5 (1976).

117 Rubenfeld, *supra* note 47, at 115.

118 *See id.* at 112, 115.

119 *See id.* at 103.

120 *See id.* at 115. *Smith* is very specific to content of a telephone directory that has been shared with a third party and accessed via a pen register—a scenario fundamentally different than those involving processing products of recent technological innovation such as the content of text messages, e-mails, photographs, and other information commonly retained on cell phones but not shared with the cell phone provider. *See Smith*, 442 U.S. at 741-42. For these reasons, the conception of a reasonable expectation of privacy that emanated from *Smith* is structurally different from those that may arise from records maintained in cell phones, smartphones, and Facebook and Twitter accounts. *See* Rubenfeld, *supra* note 47, at 112-15 (discussing problems with the third-party doctrine in modern times).

121 *See* Rubenfeld, *supra* note 47, at 115 ("[M]odern Fourth Amendment 'expectations of privacy' analysis cannot even sustain its inaugural case—Katz.").

122 *See* Ann Bartow, *Copyrights and Creative Copying*, 1 U. OTTAWA L. & TECH. J. 75, 83 (2003-2004) (noting the "voluminous flow of information facilitated by the internet").

in contact with the data for only a few microseconds—not sufficient time to inspect or have any meaningful activities to have any quality disclosure.[123] Yet, courts have failed to note the qualitative difference in third-party involvement—a difference that must stem from meaningful disclosure opportunity.[124] There is, however, a difference between a third party that acts as an enabler for processing and a third party that can act as an interceptor that can review data.[125] While the former is part of technology's role in furtherance of communication, the latter is an active communication between entities.[126] Therefore, a necessary ingredient to act as a conduit in the communication process must be separate from actual participation in communications where both the sender and recipient are active participants.[127] The conflation of this necessity of Internet-driven activities with the desired immunity from the third-party doctrine is of grave concern and will be addressed in adequate detail in Part III.[128] In the remaining part of this section, I examine how the qualitative difference identified above results in undue stress on the third-party doctrine.[129]

B. Stressing the Third-Party Doctrine—Judicial Over Emphasis or Doctrinal Failure

Regardless of the broader implications of the 9/11-shaping effect discussed earlier, the stress on the third-party doctrine can be understood by developing a deeper insight into broader provisions of the privacy element of the Fourth Amendment.[130] The Fourth Amendment's recognition of the individual right to privacy was solidified under the framework designed in *Katz*,[131] which remains the predominate anchor

---

123 *See* THE INFO. SOC'Y ALLIANCE, INTERNET TECHNOLOGY EXPLAINED: HOSTING, CACHING AND MIRRORING 1-2 (1999), http://www.eurim.org.uk/activities/netgov/9911paperinternettech.pdf.

124 *See supra* note 123 and accompanying text.

125 THE INFO. SOC'Y ALLIANCE, *supra* note 123, at 1-2 (describing how some data is transferred almost instantly from one third party to the next, while other third parties host the data on their servers).

126 *See id.*

127 *See supra* notes 125-26 and accompanying text.

128 *See infra* Part III.

129 *See infra* Part II.B.

130 *See infra* notes 134-58 and accompanying text.

131 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

for the broader doctrinal implications of the Fourth Amendment.[132] According to *Katz*, the Fourth Amendment guarantees the individual privacy protection via a two-step procedure.[133]

We must first identify whether a targeted individual has a subjective expectation of privacy.[134] This subjective expectation of privacy is then evaluated by determining whether an individual's expectation of privacy is a reflection of society's objectively reasonable expectation of privacy.[135] Therefore, this framework involves an equality mechanism whereby collective objective parameters factor in to make a deterministic evaluation of an individual's subjective expectation.[136] If we look through this construction, we can clearly see how the shaping effect of 9/11 can have disastrous consequences for an individual's privacy interest.[137] First, the original construction, with its two components, a subjective and an objective part, is inherently complex.[138] The individual does have a subjective expectation, which is more fundamental in nature.[139] Yet, we are reliant upon a collective evaluation to identify its true contour, which could have some inherent distortion potential via

---

132 Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 McGeorge L. Rev. 1, 1 (2009).

133 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

134 *Id.* While echoing similar understanding of Justice Harlan's famous test in *Katz*, Peter Winn observed,

> [In] Justice Harlan's concurrence on its merits, we have seen that in working on the reasonable expectation of privacy test, he refined the test in his own way, adding both a subjective and an objective component. Perhaps he thought that the subjective component was needed to clarify that, although an objective expectation of privacy might exist, a subjective expectation might not, as when a person in his (objectively private) home is overheard intentionally speaking in a loud voice out of on [sic] open window. . . . Perhaps Justice Harlan felt the subjective component of the test was still needed to mirror the old trespass element that an intrusion lack permission. However, when applying the test in subsequent cases, even Harlan himself only referenced the objective component.

Winn, supra note 133, at 11.

135 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

136 *Id.*

137 *See infra* notes 138-41 and accompanying text.

138 Harper, *supra* note 11, at 1381-82.

139 *See id.* at 1386 (noting that people intend to hide their intimate moments that occur inside the home).

conflation.[140] Second, since the deterministic evaluation of an individual's expectation is dependent on society's view, the broader distortion potential depends on the collective consciousness—an area that has been suspect since 9/11, which I analyze in further detail below.[141]

Emboldened by the collective consciousness that, in exigent times basic liberties could be temporarily suspended,[142] law enforcement inherited a heightened expectation to intrude upon individual privacy.[143] Within this paradigm resides the overarching existential fear that has germinated an alarmist variant of national security mindset.[144] Furtherance of this version of national security has the potential to make society oblivious to the ill effect of privacy abrogation.[145] As a result, individual privacy may become subservient to the excesses of a security mechanism—a scenario that would advance overarching surveillance by law enforcement.[146] The judiciary further bolsters this phenomenon by overemphasizing the materiality of evidence in direct abrogation of individual privacy rights.[147]

Evolution of post-9/11 individual privacy under the Fourth Amendment must therefore be viewed through the lens of two compet-

---

[140] *See id.* at 1382 (noting that courts have ignored the holding in *Katz* and instead focused solely on the reasonable expectations language from Justice Harlan's concurrence).

[141] *See infra* notes 142-67 and accompanying text.

[142] *See* Ghoshray, *supra* note 8, at 219 n.309.

[143] *See, e.g.*, John W. Whitehead & Steven H. Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives*, 51 AM. U. L. REV. 1081, 1083 (2002) ("[U]nder the guise of stopping terrorism, law enforcement officials and government leaders have now been given the right to conduct searches of homes and offices without prior notice, use roving wiretaps to listen in on telephone conversations, and monitor computers and e-mail messages . . . .") (citations omitted).

[144] *See generally* Ghoshray, *supra* note 8 (discussing this phenomena at length).

[145] *Id.* at 218 n.301; Whitehead & Aden, *supra* note 143, at 1084.

[146] *See* Whitehead & Aden, *supra* note 143, at 1083-84.

[147] In case after case since 2001, judges in the federal court system have observed that temporary suspension of individual privacy interests can be allowed if doing so would further law enforcement investigative objectives. *See* Emanuel Gross, *The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—The Proper Balance*, 37 CORNELL INT'L L.J. 27, 71-72 (2004).

ing interests.[148] The first involves law enforcement's criminal prosecution interest, while the second revolves around an individual's right to privacy interest.[149] Historically, judicial adjudication in a given context depends on which interest retains primacy over the other.[150] Thus, contextual relevance within a systemic framework is important in the evaluation of these two competing interests.[151] If an external stimulus is introduced in such a system, be it an advancement of technology or a societal development, judges would consider the shaping effect of the new stimulus to evaluate the competing merits of the two interests.[152] Therefore, if the stimulus appears to expand the contours of individual privacy, judges would tend to restrict that contour for furtherance of law enforcement investigations.[153] In addition, more often than not, the judiciary would be keen on emphasizing the probative value of evidence over extending the privacy contours of an individual.[154] Here, by adjudicating a higher threshold of materiality on the interception of personal

148 Nick J. Sciullo, *The Ghost in the Global War on Terror: Critical Perspectives and Dangerous Implications for National Security and the Law*, 3 DREXEL L. REV. 561, 580 (2011).

149 *Id.*

150 *See* Gross, *supra* note 143, at 71.

151 *See id.* at 68.

152 James D. Phillips & Katharine E. Kohm, *Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right to Privacy*, RICH. J.L. & TECH., Fall 2011, at 10 (arguing that advances in technology have led to Supreme Court decisions that have created confusion in Fourth Amendment privacy law).

153 *Cf.* Gross, *supra* note 143, at 68 (noting that the *Katz* Court eliminated the trespass rule for determining whether law enforcement violated the Fourth Amendment due to changes in technology).

154 I refer to the general legal environment that emerged post-9/11, in which simple criminal offenses have been upgraded to include serious charges against individuals on either questionable legal precedents or incomplete evidence. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RL 31377, THE USA PATRIOT ACT: A LEGAL ANALYSIS, 51-52 (2002); Andrew Ayers, *The Financial Action Task Force: The War on Terrorism Will Not Be Fought on the Battlefield*, 18 N.Y.L. SCH. J. HUM. RTS. 449, 458 (2002); Whitehead & Aden, *supra* note 144, at 1084-85; Marc Cooper, *Uncensored Gore: The Take-No-Prisoners Social Critic Skewers Bush, Ashcroft and the Whole Damn Lot of Us for Letting Despots Rule*, L.A. WKLY., (Nov. 20, 2003), http://www.laweekly.com/2003-11-20/news/uncensored-gore/. *See generally* Ghoshray, *supra* note 70 (discussing the government's use of the "Laws of War" model and "unlawful combatant" status).

communication data, judges are more likely to provide law enforcement with much wider latitude than necessary.[155]

This explains why judges may be more prone to use the procedural framework of the third-party doctrine, without adequately reviewing the contextual relevance and relationship of the doctrine to applied cases.[156] The outcome is both excessive and asymmetrical in the process of judicial determination.[157] Scholars may not have adequately addressed this commoditization of the doctrine and the resulting stress that occurs.[158] Like all structural forms, anything that is used inappropriately and overbearingly risks failure borne of fragility. The same is true of the third-party doctrine, resulting in the doctrine approaching a naturally progressive breaking point—an aspect that might not have found sufficient traction in contemporary discourse.[159]

Furthermore, the evaluative aspect of the Fourth Amendment's expectation of privacy rests on a competitive framework.[160] There are legitimate unanswered questions, and each of these questions would lead to separate reasonable expectations from its unreasonable counterparts.[161] Who determines society's reasonable expectations? How do we measure such reasonableness? In an environment where the masses

---

155 *See supra* note 157 and accompanying text.

156 Here I refer to the scenarios where the tendency may arise for a desired outcome, especially when exigencies of national security are invoked by the administration, as has been the case since 9/11. *See* Victor Hansen, *Use and Misuse of Evidence Obtained During Extraordinary Renditions: How Do We Avoid Diluting Fundamental Protections*, 35 NOVA L. REV. 281, 304 (2011) (arguing for a review process to ensure that trial courts do not ignore the law "to reach a desired outcome"). In situations like that, the judiciary may resort to strict constructionist formulation of statutes or adhere to old doctrines that may not be applicable to specific cases they are called upon to adjudicate. Solove, *supra* note 27, at 1086. This can cause both over usage of a particular doctrine or inconsistent rulemaking based on application of unsound laws. *Id.* at 1122.

157 *See supra* note 156 and accompanying text.

158 *See supra* note 47 and accompanying text.

159 *See supra* note 47 and accompanying text.

160 *See* Sciullo, *supra* note 148, at 580.

161 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (stating that an individual's interest in privacy involves determining whether an individual's subjective expectation of privacy is one that society is willing to recognize as "reasonable").

are inundated with false information, propaganda, and fear-mongering,[162] is it even possible to objectively define a reasonable expectation? In this context, the shaping effect of 9/11 is instrumental in developing a proper context through which to address these issues.

Since 9/11, each successive administration has carefully introduced and propagated a specter of gloom and doom, resulting in a sustained ambiance of existential fear.[163] Against this background of fear, individuals naturally gravitate to a more existentially driven mindset, consequently foregoing basic tenets of liberty.[164] Along the way, the original conception of privacy has become attenuated because of the overpowering psychosis of fear.[165]

I would argue, therefore, that the shaping effect of 9/11 is not only significant in understanding the judiciary's overtly conservative construction of legal contours, but is also instrumental in distorting the perception of the individuals that comprise society.[166] Therefore, if society's view is distorted and becomes infected with a false sense of vulnerability, could society objectively determine what its own reasona-

---

[162] *See* Marjorie Cohn, *Trading Civil Liberties for Apparent Security is a Bad Deal*, 12 CHAP. L. REV. 615, 637 (2009) (arguing that following 9/11 the Bush Administration attempted to maintain a state of fear in the United States).

[163] *See id.* Here I refer to the domestic aspiration that emerges as a faulty manifestation of American exceptionalism, an area I examined in greater detail in an earlier work. *See generally* Ghoshray, *supra* note 8 (providing an in-depth discussion of the shaping effect of 9/11). The central argument here is that the attacks of 9/11 have shaken the core of the American psyche and persona to such an alarming extent that any invocation of national security will allow for executive excesses to become palatable to the domestic constituency. *See* Gross, *supra* note 147, at 73. The Wikileaks investigation follows the same expected trajectory—a viewpoint that has also been shared by other scholars. *See generally* Benkler, *supra* note 76 (describing the controversy surrounding Wikileaks and the legal consequences). For a detailed legal landscape post-9/11, *see generally* Ghoshray, *supra* note 8. As I argued earlier, the "all-pervasive fear of terrorism impregnated deep within the American psyche" since 9/11 has been manifested in the post-9/11 legal landscape. *See* Ghoshray, *supra* note 69, at 251. Some of these manifestations involve indefinite detention, excessive domestic surveillance, and expansive governmental reach in breaching individual privacy, which implies snooping on private telephone calls, Facebook messages and Twitter feeds. *See* Whitehead & Aden, *supra* note 143, at 1083.

[164] *See* Gross, *supra* note 147, at 73.

[165] *See id.*

[166] *See supra* notes 133-65 and accompanying text.

ble expectation of privacy is? The societal framework has changed significantly since 9/11, and therefore its reasonable expectations of privacy have a much lower standard than Justice Harlan's construction in *Katz* originally envisioned.[167]

Moreover, whether the *Katzian* construction of privacy is reasonable or not,[168] it has to go through two distinct processes.[169] First, as I have examined earlier, privacy is evaluated based on societal recognition of what is considered legitimate or illegitimate.[170] Second, judicial acquiescence must sanction this societal evaluation as it ultimately depends on judicial determination.[171] As I articulated earlier, the post-9/11 legal landscape erroneously distorts that judicial construction.[172] Arguably, if the judiciary ever finds such societal recognition to be illegal, the determination should be viewed through its true objective—that of subjugating privacy interests to the advancement of law enforcement's investigative objective. Therefore, society's attenuated expectation of privacy can significantly contribute to over usage of the third-party doctrine.[173]

The discussion above provides us with a roadmap to understand contemporary judicial construction regarding the third-party doctrine.[174] Clearly, judicial constructions have been advanced to establish a deterministic outcome in this construct; yet, we must recognize usage of the third-party doctrine is not an end to a means but rather a means to a desired end.[175] Such usage is not a legitimate constitutional construction as it unnecessarily burdens the doctrine by overusing and stressing it to its breaking point of doctrinal resiliency.

---

167 Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 157 (2005).

168 *See supra* note 134.

169 *See infra* notes 171-72 and accompanying text.

170 *See supra* notes 130-39 and accompanying text.

171 *See* Freiwald, *supra* note 47, ¶ 8 (noting the difficulty courts have in determining reasonable expectations of privacy in the modern age).

172 *See supra* note 163 and accompanying text.

173 *See* Derek M. Alphran, *Changing Tides: A Lesser Expectation of Privacy in a Post 9/11 World*, 13 RICH. J.L. & PUB. INT. 89, 129-30 (2009).

174 *See supra* notes 130-73 and accompanying text.

175 *See supra* notes 130-73 and accompanying text.

III. THIRD-PARTY DOCTRINE: BREAKDOWN OR DEBILITATING STRESS?

The third-party doctrine dictates that an individual relinquishes his or her expectation of privacy with respect to communications with third parties.[176] Despite three decades of uninterrupted existence, this exclusionary provision of the Fourth Amendment now finds itself perched on shaky ground.[177] The doctrine has become significantly problematic[178] because we live in an era where a significantly larger portion of personal information and communication is processed in cyberspace via automation.[179] A particular interest of this section is to examine the third-party doctrine's vulnerability to identify why the doctrine continues to transmogrify into the Achilles's heel of Fourth Amendment jurisprudence.[180]

A. Anatomy of the Breakdown

A significantly increasing number of scholars have identified the third-party doctrine as the weakest link in the causal chain of constitutionally-mandated privacy protection for individuals.[181] While advanc-

176 *See supra* notes 103-17 and accompanying text.

177 *See*, *e.g.*, Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1092 (2006) (noting that in modern times there is a greater need to "disclose information to third parties"); Matthew D. Lawless, Comment, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, UCLA J.L. & TECH., Spring 2007, at 3-4 (arguing that the third-party doctrine needs to be updated to match the world's changing technologies); *see also infra* Part IV (describing the uncertainty that Internet technology and other information-sharing resources have created in Fourth Amendment jurisprudence).

178 *See, e.g.*, DeFilippis, *supra* note 177, at 1092; Lawless, *supra* note 177, at 3-4.

179 *See, e.g.*, Phillips & Kohm, *supra* note 152, at 10 (noting the changes in technology, including the data storage and personal information on the Internet, that have "muddled [the] legal standard for privacy").

180 *See infra* Part III.

181 *See* United States v. Crews, 445 U.S. 463, 471 (1980) (observing that a defendant must make a prima facie showing of a causal nexus between the Fourth Amendment violation and the evidence he seeks to suppress). However, as has been documented in scholarship and in recent cases, this causal nexus is continuously under stress due to the exclusionary roadblock the third-party doctrine presents. *See, e.g.*, DeFilippis, *supra* note 177, at 1092; Lawless, *supra* note 177, at 3-4. Arguably, in a significant proportion of the cases, law enforcement and prosecutors can show existence of third-

ing the doctrinal failure in some cases,[182] or advocating its near demise in other cases,[183] these commentators have advanced a number of propositions while formulating a variety of rationales.[184] Whether doctrinal difficulties or fatal flaws, the central theme of such arguments relies on the recognition that the explosion of technology, advancement of communication mechanisms, and widespread access of various exchange mediums have resulted in increases in both frequency and volume of personal information in transit.[185] Such transmissions rely on a third-party communication provider or carrier for adequate processing between the origin and destination points.[186] Here a third party is simply a conduit[187] or, more importantly, a necessary router that simply stores,

---

party interference on available evidence and preclude a defendant from invoking the Fourth Amendment protection.

[182] *See* Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. MEM. L. REV 233, 289 (2010).

[183] *See* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 51 (2011), http://www.uiowa.edu/~ilr/bulletin/ILRB_96_Henderson.pdf.

[184] *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 642-43 (2011).

[185] In his article, Matthew Tokson noted,

> The Third Party Doctrine precedents, and *Smith* in particular, are problematic in an age where an ever-growing proportion of personal communications and transactions are carried out over the Internet. Internet users, now comprising eighty percent of U.S. citizens, generate enormous amounts of personal data online, virtually all of it accessible to third-party Internet service providers ("ISPs") or websites. E-mails, web-surfing histories, credit card and address information, and search term records are all routinely stored by online entities and are potentially available to the government, or even to private parties that purchase customer information for marketing purposes. With the Fourth Amendment inapplicable to this mass of easily obtainable personal information, government investigators could monitor the communications of individuals and organizations on an unprecedented scale.

Id. at 585 (internal citations omitted); *see also Annual Internet Survey by the Center for the Digital Future Finds Large Increases in Use of Online Newspapers*, USC ANNENBERG SCH. (April 28, 2009), http://annenberg.usc.edu/NewsandEvents/News/090429CDF.aspx (describing the significant increase in the number of people reading online newspapers in the year 2009 as compared to the year 2007).

[186] *See* THE INFO. SOC'Y ALLIANCE, *supra* note 123, at 1-2.

[187] *See id.*

identifies, and redirects communication.[188] The involvement of a third party should be seen from this dispassionate context, borne out of technical necessity and devoid of emotional attachment. Judicial invocation of the third-party doctrine within contemporary Fourth Amendment analysis, often times, does not capture this distinctive, yet significantly qualitative, characteristic of the communication carrier.[189] Scholarship has identified and addressed this apparent disconnect in various ways.[190]

Some scholars favor the creation of a hierarchical Fourth Amendment protection for personal communication by creating a two-tiered system that makes a bright-line distinction between the information content and the "envelope" information.[191] In this construction, privacy interests would apply to the content component of information, while no such interest can attach to its noncontent component.[192] Here, noncontent or "envelope" information could consist of the identification of the recipient and sender, the time and place of origin, the destination, and other revealing information.[193] In a sense, this line of reasoning identifies the "envelope" as distinct from specific informational content and therefore attaches a lower threshold of privacy compared to content information.[194] Courts have accordingly given hierarchical relevance to individual privacy interests by distinguishing between content and noncontent information.[195] For example, in *Ex parte Jackson*, the Court observed that the "envelope" does not have third-party exception[196] and, therefore, is open to law enforcement interception without a warrant.[197]

---

188 *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528-29 (2006) ("In the Information Age, much of what we do is recorded by third parties."); *see also* Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 910-12 (2004) (noting that the content of telephone calls are not stored).

189 *See* Swire, *supra* note 188, at 910-12.

190 *See supra* note 47 and accompanying text.

191 *See* Tokson, *supra* note 33, at 2112-13.

192 *Id.*

193 *Id.*

194 *Id.* at 2116.

195 *Id.* at 2112.

196 *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (observing that, while letters sent by mail were protected by the Fourth Amendment, information related to header, destination, and origin—collectively the "envelope" information—on packages were not).

197 *See id.* Following the lines of argument in *Ex parte Jackson*, courts observed that, despite its technological sophistication, the government's surveillance of e-mail

As we evaluate the recent court observation in the WikiLeaks issue, it is instructive to revisit the Supreme Court formulation in *Smith*.[198] Although *Smith* was a judicial response to a specific law enforcement issue, its broader construction continues to reverberate today, albeit somewhat incongruently in recent cases.[199]

Rejecting the petitioner's argument in the case involving WikiLeaks and Twitter, the lower court denied Fourth Amendment rights mainly based on an exception to the third-party doctrine.[200] In rejecting the petitioner's argument centering on the violation of the inner sanctum of a person's residence, the court identified a distinction between the individual context of *United States v. Karo*[201] and those of the selected Twitter users.[202] The court distinguished the Fourth Amendment violation in *Karo* from those violations involving the government's requests to subpoena Twitter accounts because, in *Karo*, the federal agents were monitoring the inside of a private residence.[203] The court observed that providing Twitter account information did not amount to a violation of individual privacy inside a private residence.[204] In finding disconnect between *Karo*'s factual construction and the current scenario, the court relied on the doctrinal implication of *Smith*.[205] The court's observation on the Twitter users, that by providing information during subscription they lost their reasonable expectation of pri-

addresses is not necessarily different conceptually from viewing physical mail. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741 (1979) (distinguishing *Katz* in part based on the content/noncontent distinction); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (noting an e-mail has "an outside address 'visible' to the third-party carriers that transmit it to its intended location"); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008) (concluding that the privacy interests in letters and e-mail are the same).

198 *See supra* notes 111-12 and accompanying text.

199 *See supra* note 24.

200 *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11-DM-3, 2011 WL 5508991, at *22 (E.D. Va. Nov. 10, 2011); *see supra* note 24.

201 United States v. Karo, 468 U.S. 705 (1984) (involving the interior of a home where homeowners intended to conceal their activities).

202 *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2011 WL 5508991, at *16 (noting that Internet users transmit their IP addresses onto the public Internet).

203 *Id.*

204 *Id.*

205 *Id.* at *16-17.

vacy, has a fatal flaw as I explain below.[206] Understanding the full implication of the third-party doctrine against a backdrop of the technological advancement is important here.[207] Unfortunately, courts have followed a trajectory of predictable discourse without fully evaluating the technological reality.[208] By rejecting the petitioner's analogy between the beeper surveillance and IP address location tracking, the court clearly understood the revealing information from *Karo*'s surveillance to be more intrusive than intended.[209] Thus, the threshold question to consider is as follows: do the petitioners relinquish the right of privacy by transmitting their Twitter IP address location from the confines of private spaces into the openness of cyberspace? This requires more than the surface-level analysis that the court engaged in.[210]

First, the current status of the technology has enabled individuals to use any available medium—Twitter postings and updates for the present instance—as a means of revealing private emotions and information about their lives.[211] These information updates are only designed for the consumption by people these individuals designated.[212] Just because a person transmits information into cyberspace should not imply that the person has relinquished his or her right to privacy.[213] This is because life in the twenty-first century occurs in cyberspace.[214] By disclosing certain information through certain modes like Twitter,

---

206 *See infra* text accompanying notes 211-20.

207 *See generally In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2011 WL 5508991, at *17 (noting the effect of the third-party doctrine when a person discloses private information over the Internet).

208 *See* Tokson, *supra* note 33, at 2116-17, 2149-50.

209 *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2011 WL 5508991, at *16.

210 *See* Tokson, *supra* note 33, at 2150 ("[T]he purpose or subject matter of certain communications might be exposed simply through the disclosure of an IP address.").

211 *See* Powell, *supra* note 20, at 146.

212 *About Public and Protected Tweets*, TWITTER HELP CENTER, https://support.twitter.com/groups/31-twitter-basics/topics/113-online-safety/articles/14016-about-public-and-protected-tweets (last visited Feb. 29, 2012).

213 *See infra* notes 214-15 and accompanying text.

214 *See* JENNIFER CHEESEMAN DAY ET AL., U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003 1 (2005), *available at* http://www.census.gov/prod/2005pubs/p23-208.pdf.

individuals choose to reveal information that they feel comfortable with.[215]

Second, the communication framework as it exists today is not self-sustaining within intended recipients and its originator.[216] Such communication requires a carrier that a third party must manage and sustain.[217] The potential loss of privacy on account of third-party involvement would have been more relevant had there been a provision allowing an individual the option to do away with a third party and yet maintain the existing communication protocol.[218] This situation is similar to an individual's involvement with providers of other essential services, such as medical or legal services.[219] Just because a third party comes in the form of a technological service provider does not attenuate that service provider's designated role as an enabler of both forming a community and conducting online life in the twenty-first century.[220] This awareness and the recognition of its specific scope within the con-

---

[215] *See 86% of Internet Users Want to Prohibit Online Companies from Disclosing Their Personal Information Without Permission*, PEW INTERNET (Aug. 21, 2000), http://www.pewinternet.org/Press-releases/2000/86-of-Internet-Users-Want-to-Prohibit-Online-Companies-From-Disclosing-Their-Personal-Inf.aspx.

[216] *See* Sean M. O'Brien, Note, *Extending the Attorney-Client Privilege: Do Internet E-Mail Communications Warrant A Reasonable Expectation of Privacy?*, 4 SUFFOLK J. TRIAL & APP. ADVOC. 187, 206 (1999). *See generally* Tokson, *supra* note 33, at 2114 (during transmission, e-mails, and web-surfing communication, unlike traditional letters, are exposed to third parties).

[217] *See* O'Brien, *supra* note 216, at 206. *See generally* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557-58, 1562-63 (2004) (discussing how commercial servers own routers that are used by individuals to send e-mails and store photos).

[218] *See* Mulligan, *supra* note 217, at 1562-63 (discussing the lack of privacy regarding e-mail communications); O'Brien, *supra* note 216, at 204-06 (noting that sending an e-mail is a fast and convenient form of communication, but raises privacy concerns); Kobrin, *supra* note 9, at 2 (discussing the choice individuals have regarding the impacts of using technology).

[219] *See, e.g.*, René Reyes, *Do Even Presidents Have Private Lives?: The Case for Executive Privacy as a Right Independent on Executive Privilege*, 17 KAN. J.L. & PUB. POL'Y 477, 488 (2008) (noting that conversations with doctors and lawyers are private and cannot be used in court).

[220] *See, e.g.*, Mulligan, *supra* note 217, at 1572-73 (discussing how the Internet has become a place and how individuals use the Internet in their daily life).

struction of the third-party doctrine are certainly missing within contemporary legal discourse.

In the context of the third-party doctrine, a favorite construction of the judiciary is the *Karo-Knotts* framework.[221] The Court upheld Fourth Amendment rights in *Karo* by finding intrusive elements in beeper surveillance where police revealed activities inside a private dwelling.[222] In contrast, in *United States v. Knotts*,[223] the Court rejected the Fourth Amendment claims on the grounds that the usage revealed critical facts about the interior of the premises that the government was interested in knowing, as such information could not have been obtained without a warrant.[224] The *Karo-Knotts* framework fundamentally rests on revealing physical encroachment inside a private dwelling.[225] Until the mass acclimatization of cyberspace activities, physical intrusion was seen as the tipping point in privacy violation.[226] Now that cyberspace has indeed become a de facto dwelling, why must the physical intrusion continue to be a delineating factor in identifying when privacy violation occurs? While society continues to dwell in both virtual and nonvirtual mediums, why could Fourth Amendment rights be triggered only in a nonvirtual mode? Thus, the first step in alleviating the post-modern doctrinal stress from the third-party doctrine would revolve around giving due recognition to this disconnect—an area I clarify below.[227]

---

221 *See* Engel, *supra* note 182, at 277-78; William Curtiss, Note, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139, 159 n.103 (2011).

222 *Karo*, 468 U.S. at 727-28.

223 United States v. Karo, 468 U.S. 705, 727-28 (1984).

224 *Id.* at 284-85.

225 *See, e.g.*, David H. Goetz, Note, *Locating Location Privacy*, 26 BERKELEY TECH. L.J. 823, 832 (2011) ("Taken together, *Knotts* and *Karo* are generally understood to mean that the government is free to place a tracking device on a suspect's car without a warrant and track the suspect's movements on public roads, but cannot obtain information about a suspect's home from such a device without a warrant.").

226 *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1010 (2010) (noting that a search is triggered for Fourth Amendment purposes when officers enter enclosed spaces).

227 *See infra* Part III.B.

B. Origination of the Doctrinal Stress

I do not see any material distinction among differing variants of technology-enabled surveillance devices, beepers, thermal imaging devices, and global positioning systems (GPS); all of them can have similar impact when intruding into physical space within the privacy of a person's dwelling.[228] So, we must get to the next level of abstraction by invoking the interior of a private space to identify what is being protected.[229] Intruding into the inner confines of a private residence instantly reveals an individual's private behavioral norms, private expressions, thoughts, and emotions.[230]

---

[228] It can be argued that there may not be a conceptual difference between beeper technology and GPS technology, except for the elegance of design and speed of communication. Ramya Shah, *From Beepers to GPS: Can the Fourth Amendment Keep Up with Electronic Tracking Technology?*, 2009 U. ILL. J.L. TECH. & POL'Y 281, 285. Others have noted,

> In many ways, beeper technology was in the 1980s what GPS technology is today. In the past, courts dealt with the use of beepers as tracking devices. While beepers are smaller and less sophisticated than GPS devices, their use as law enforcement tools is strikingly similar to the use of GPS devices. Both types of devices can be concealed on a suspect's vehicle and allow police to obtain information relating to the suspect's location and movements. To analyze electronic tracking through the use of beepers, courts focused on Fourth Amendment concerns, trying to determine whether or not a search occurred. In order to answer this question, courts focused, among other, [sic] things on the method of attachment of the beeper, the monitoring of the beeper for tracking purposes, the expectation of privacy in public and private places, and the enhancement of police officers' senses.

Id. (citations omitted).

[229] *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may by constitutionally protected.") (citations omitted).

[230] *See* Kyllo v. United States, 533 U.S. 27, 38 (2001) (noting that thermal imaging may "disclose . . . at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on.").

The Fourth Amendment, through its *Karo-Knotts* framework, presents us with a bulwark against intrusion of the inner sanctum.[231] Does not today's instant and technologically-enabled communication reveal qualitatively similar information? Individuals can express their emotions through text messages or tweets.[232] They reveal the inner workings of their minds by bringing to the surface private norms and behaviors that they would only share with their chosen community.[233] Life continues to evolve in the twenty-first century by conduct through chosen modes in cyberspace and through smartphones, much the same way it occurs inside a private dwelling.[234] Therefore, if privacy interests belong to those private spaces, explicitly designated under the *Karo-Knotts* framework, then why should the same privacy interests not be extended to the owners and users of such communication mediums as Twitter, Facebook, and smartphones?

A point of critical concern is whether *Smith* continues to be viable.[235] Looking at the supervising dictum in the recent Twitter case, the court uses a strict constructionist approach by rejecting the legitimate expectation of privacy information of an individual who voluntarily

---

[231] *See* Engel, *supra* note 182, at 276 (stating that insofar as police can view individuals, as with binoculars, there is no reasonable expectation of privacy but this stops short of the total type of surveillance, which could be permitted by twenty–four-hour GPS monitoring).

[232] *See, e.g.*, Tina Rosenberg, *Everyone Speaks Text Message*, N.Y. TIMES, Dec. 11, 2011, at MM20, *available at* http://www.nytimes.com/2011/12/11/magazine/everyone-speaks-text-message.html?_r=1&scp=21&sq=texting&st=cse (explaining that even languages with obscure syllabaries may be expressed through electronic forums).

[233] *See, e.g.*, Yuki Noguchi, *Life and Romance in 160 Characters or Less*, WASH. POST, Dec. 29, 2005, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/28/AR2005122801430.html (discussing the efficacy of using electronic means to convey intimate feelings).

[234] *See, e.g.*, Nick Yee et al., *The Unbearable Likeness of Being Digital: The Persistence of Nonverbal Social Norms in Online Virtual Environments*, 10 CYBERPSYCHOLOGY & BEHAV. 115, 117 (2007), *available at* http://vhil.stanford.edu/pubs/2007/yee-nonverbal.pdf (discussing the modalities through which people in virtual, online spaces engaged in intimate, yet nonverbal, communication analogous to real-world communication).

[235] *See supra* notes 198-200 and accompanying text.

shares that information with a third party.[236] It is extremely important to understand both the relevance and context of *Smith* and the point of time in technological development when this judicial construction emerged.[237] In addition, it is instrumental to extrapolate that judicial construction against the point of time in today's technology.[238] *Smith* makes it clear that disclosure of information to a third party is a necessary condition that will automatically signal a relinquishment on the part of that individual.[239] More often than not, courts have continued to make judgments regarding individuals' Fourth Amendment interests,[240] relying on the ironclad doctrine.[241] The pace of technology,[242] symmetrizing of the individuals inside that society,[243] and their assimilation

---

[236] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11–DM–3, 2011 WL 5508991, at *17 (E.D. Va. Nov. 10, 2011) (order granting an order to turn over information).

[237] *See infra* notes 250-53 and accompanying text.

[238] *See infra* notes 254-59 and accompanying text.

[239] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[240] *See* U.S. CONST. amend. IV (ensuring "[t]he 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.").

[241] *See, e.g.*, *Smith*, 442 U.S. at 743-44 (stating that, despite any subjective or contextual considerations, the party who discloses to a third party assumes the risk of disclosure). I opine that this lack of specificity and contextual delineation in a blanket application of the doctrine results in current doctrinal stress.

[242] *See* ARI SCHWARTZ ET AL., CTR. FOR DEMOCRACY & TECH, DIGITAL SEARCH & SEIZURE: UPDATING PRIVACY PROTECTIONS TO KEEP PACE WITH TECHNOLOGY 3 (2006), *available at* https://www.cdt.org/publications/digital-search-and-seizure.pdf.

[243] By symmetry in this context, I draw attention to the symmetrizing pattern with which the U.S. Administration and law enforcement officials have conducted a massive campaign of misinformation within a framework, as I have shown elsewhere and others scholars have noted as well, where a single-minded agenda of national security was advanced to pass almost anything. *See* Saby Ghoshray, *False Consciousness and Presidential War Power: Examining the Shadowy Bends of Constitutional Curvature*, 49 SANTA CLARA L. REV. 165, 180 (2009). Continued practice has imposed upon individuals within the society an artificial sense of security that is difficult to erase. *See id.* In much the same way as in physical dynamical phenomenon, the inertia acts upon a physical object to prevent any change from its initial status. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 638 (11th ed. 2003) (defining inertia as "indisposition to motion, exertion or change"). Here I refer to the monolithic tendency of an individual within a symmetric social order to follow the lead, or as often referred to as "like lambs to the slaughter." Ghoshray, *supra* note

into a more interactive high-frequency level of information processing and instant communication-driven lifestyle[244] apparently did not deter the judiciary from deviating from such an ironclad principle.[245] This is facially contradictory because there are two elements that separate the *Smith* construction from today's applicability.[246] *Smith* held that there is one necessary condition to complete the communication—voluntarily disclosing such information to a third party.[247] This particular necessary condition is concomitant with a much deeper necessary condition that the Court failed to address. The necessary condition I am referring to is the continued evolution of human existence.[248] The necessity of voluntarily disclosing information can provide a benchmark, if disclosing such information is driven by arbitrariness or has a built-in choice involved in such disclosures.[249]

The hard fact is today's technology, and many individuals' immersion into it, compels us to look deeper into the problem.[250] Without voluntarily disclosing information, today's individual will not be able to communicate with his or her community and will not be able to live in

---

244, at 180. Robot-like, the collective needs of an individual thus "are driven by an artificially created rationality." *Id.*

> Individuals under the influence of a dominating power, whose societal needs have been carefully designed and sublimated into its deeper consciousness, suffer from the effects of bounded rationality. In this existence, the individual rationalizes not only her false needs of security, but also her requirement of symmetry within the environment, in such a way that rationality cannot extend the artificial barrier imposed upon her current consciousness. This distorted rationality is therefore a vital ingredient in the perpetuation of symmetry.

Id.

244 *See* SCHWARTZ ET AL., *supra* note 243, at 7.

245 *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11–DM–3, 2011 WL 5508991, at *17 (E.D. Va. Nov. 10, 2011) (order granting an order to turn over information).

246 *See infra* notes 247-49 and accompanying text.

247 *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

248 *See* Yee et al., *supra* note 234 at 117 (discussing the intimate nature of online communication modalities as comparable with real-world communications).

249 *See, e.g.*, Kerr, *supra* note 24, at 587 (discussing why the third-party doctrine should be considered a form of consent law rather than merely relying on reasonableness expectation considerations where disclosure implies consent).

250 *See infra* notes 259-62 and accompanying text.

society.[251] As a result, such an individual will be unable to pursue his or her livelihood—because every aspect of the individual's life depends on adopting some fundamental societal conventions.[252] One of the primary conventions is the act of providing personal information to a communication provider.[253] Does such a disclosure incur the loss of a reasonable expectation of privacy? The blind adoption to the third-party doctrine mutes this key question.

Existing judicial construction revolves around a distinction between two issues.[254] The first issue is whether an individual loses privacy protections under the Fourth Amendment by sharing information with a third party, voluntarily or involuntarily.[255] Second, the hackneyed construction of the Fourth Amendment posits that voluntarily sharing such information would render unreasonable any expectation of privacy in the communicative aspect of such individuals.[256] This would imply that, if the individual shares information with the third party in an involuntary manner, he or she would continue to retain the reasonable expectation of privacy.[257] This voluntary-involuntary distinction falls flat on its face when confronted with the stark reality that the post-

---

[251] *See, e.g.*, Bissera Zankova, *Dialogue, Understanding and Social Cohesion*, *in* LIVING TOGETHER: A HANDBOOK ON COUNCIL OF EUROPE STANDARDS ON MEDIA'S CONTRIBUTION TO SOCIAL COHESION, INTERCULTURAL DIALOGUE, UNDERSTANDING, TOLERANCE AND DEMOCRATIC PARTICIPATION 21, 26-28 (Yasha Lange ed., 2009), *available at* http://www.coe.int/t/dghl/standardsetting/media/doc/livingtogether_en.pdf (discussing the necessity of intercommunication in modern times and the positive and negative impacts of Internet-based technology).

[252] This includes disclosing some private information to third parties that requires further protections of law. *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-02, 113 Stat. 1338, 1436-37 (codified as amended at 15 U.S.C. §§ 6801-6802 (Supp. IV 2010)) (requiring nonpublic information to be respected by institutions to which it was disclosed and forbidding such an institution from disclosing other private information unless notice has been provided).

[253] *See, e.g.*, *Privacy Policy*, VERIZON, http://www22.verizon.com/privacy (last updated Sept. 2011) (discussing the type of information collected by Verizon and the method of securing the privacy of the disclosing party).

[254] *See infra* notes 255-56 and accompanying text.

[255] *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) (discussing the reasonableness of a privacy expectation after disclosure).

[256] *See id.* at 743-44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[257] *See id.*

modern individual conducts life through the enabling means of the Internet and may, indeed, have a fundamental right to Internet access.[258] Other scholars have highlighted the individual's fundamental right to the Internet,[259] yet a comprehensive explication in contextualizing fundamental right with the negation of the implication of the third-party doctrine is somewhat missing in the dialectics.

Another area that requires some analysis is the judiciary's continued reliance on the container doctrine,[260] yet courts fall short of adapting this doctrine to the emerging communication molds.[261] In crafting its container doctrine in the 1970s, the Court clarified certain Fourth Amendment search and seizure law by developing a jurisprudence based on a physical-container analogy.[262] In such a construction, if there is a physical container inside another physical container, law enforcement cannot access the internal container without a warrant.[263] Clearly, this right of privacy inside the contents of a physical container emanated from a recognized right to the contents of a physical entity that a person finds private and personal.[264] As the technology evolved since the original construction and the life of an individual began to

---

258 *See* Mark Lemley et al., *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011), http://www.stanfordlawreview.org/online/dont-break-internet; *see, e.g.*, Joshua F. Clowers, *I E-vote, U I-vote, Why Can't We All Just Vote?!: A Survey of the Changing Face of the American Election*, 42 GONZ. L. REV. 61, 92 (2006-2007) ("The past decade's Internet revolution has demonstrated that we are in fact capable as a society of conducting major aspects of our lives via the Internet.").

259 *See* Lemley et al., *supra* note 258.

260 *See* CYNTHIA Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1405 (2010) ("[T]he Container Doctrine is fast becoming a historical relic.").

261 *See id.* at 1460 ("Permitting warrantless, suspicionless searches of laptops is inconsistent with the Container Doctrine's insistence that law enforcement officers obtain judicial authorization before searching a container.").

262 *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 11 (1977) (finding it unreasonable for the government to search a double-locked footlocker without a warrant).

263 *Id.*

264 *See, e.g.*, Robbins v. California, 453 U.S. 420, 426 (1981) ("The contents of Chadwick's footlocker and Sanders' suitcase were immune from a warrantless search because they had been placed within a closed, opaque container and because Chadwick and Sanders had thereby reasonably 'manifested an expectation that the contents would remain free from public examination.' Once placed within such a

evolve within personal computers, courts eventually applied the physical-container doctrine to electronic data.[265] Indeed, thus far the courts have rather consistently held that inspection of a personal computer requires a warrant.[266] However, as in the instant case,[267] the courts have clearly and emphatically distinguished between Twitter accounts and personal computers by relying on file-storage hierarchy inside a personal computer.[268] Let us dissect this analogy for further clarity.[269]

Like personal articles and belongings are stored at times in an ordinary fashion in a file cabinet, personal information is stored in a hierarchy inside a personal computer.[270] The same can be applied to how a person's individual life evolves centering on a Facebook or Twitter account.[271] A person could arrange specific, relevant, and contextual

container, a diary and a dishpan are equally protected by the Fourth Amendment.") (internal citations omitted) (quoting *Chadwick*, 433 U.S. at 11).

265 *See, e.g.*, United States v. Roberts, 86 F. Supp. 2d 678, 688 (S.D. Tex. 2000) ("Several courts have analogized the Fourth Amendment protection appropriately afforded an individual's computer files and computer hard drive to the protection given an individual's closed containers and closed personal effects."); United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (noting that a computer memo book "is indistinguishable from any other closed container, and is entitled to the same Fourth Amendment protection.").

266 *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (finding that commercial ISP subscribers have a reasonable expectation of privacy in the contents of e-mails, which deserve Fourth Amendment protection requiring the government to obtain a warrant); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (describing the protection afforded to closed-computer files and hard drives as similar to that of closed containers and closed personal effects, where a warrant is required because of the owner's expectation of privacy in the contents of the container).

267 *See supra* notes 28-29 and accompanying text.

268 *See* Tokson, *supra* note 33, 2112-17 (describing the content/"envelope" distinction and the legal protections afforded to each).

269 *See infra* notes 279-85 and accompanying text.

270 Trulock v. Freeh, 275 F.3d 391, 410 (4th Cir. 2001) (Michael, J., concurring in part and dissenting in part) ("Courts have not hesitated to apply established Fourth Amendment principles to computers and computer files, often drawing analogies between computers and physical storage units such as file cabinets and closed containers.").

271 *See* Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 371 (2011) (describing how a Facebook account stores private content in which a user manifests an expectation of privacy, as opposed to "envelope" information).

information hierarchically inside his or her Facebook—both revealing information about that person and evolving along such information with the expressive means that such a medium provides.[272] Similarly, through a series of Twitter feeds, exchanges with designated individuals, and responding to self-identified messages, an individual's private life takes shape in the Twitter world.[273] There is a need to protect the identity and detailed information of a file cabinet and a personal computer;[274] similarly, the same layer of privacy must extend to a Facebook and Twitter account so that an individual is able to evolve and live life without law enforcement interference.

By now, it is clear that there is a fundamental disconnect between the judiciary's understandings of the private space illuminated by technological advancement versus the actual essence of life, the way it is being conducted on the Internet.[275] That is why commentators assailed this existing tendency of adopting the third-party doctrine as monolithic—monolithic in its failure to be flexible in its understanding, in its focusing within a narrow spectrum.[276] Even the Supreme Court has recently recognized this rapid societal change and its cause for caution, as it noted:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . .
>
> . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.[277]

Precisely along the lines of this recognition, and as I have argued earlier in this Article, the communicative needs of today's individ-

---

272 *See id.*

273 *See* Rafe Needleman, *Newbie's Guide to Twitter*, CNET (March 15, 2007, 4:15 PM PDT), http://news.cnet.com/newbies-guide-to-twitter/.

274 *See supra* notes 268-70 and accompanying text.

275 *See supra* note 120 and accompanying text.

276 *See* Henderson, *supra* note 183, at 41-43.

277 City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629-30 (2010).

ual revolves around his or her self-expression and self-identification, which must have the precedent of adhering to the norms of a communication provider.[278] Penalizing those for following the legitimate technological norms of sharing information should not prompt the alternate remedy of shutting down their self-expression and self-identification.[279] Doing so would be tantamount to the individual losing the right to life as a broader sense as I shall explain below.[280]

What was legitimate and justified for the Supreme Court in the era between 1960 and 1980 may not be congruent in the modern era.[281] Where the societal norms and technological norms dictate that third parties must manage more qualitatively and quantitatively personal information, the doctrinal contours of the third-party doctrine must be reinterpreted.[282] Clearly, in the current construction of the third-party doctrine, the judiciary is equating apples with oranges. An individual technology user's interaction with her communication provider is qualitatively different from the same user's interaction with law enforcement entities.[283] While the former interaction, that of sharing subscriber information, is a steppingstone of preprocessing the need to complete communication,[284] the latter interaction is much more meaningful, much more qualitatively significant in its intrusive nature, and the outcome that may result from such interaction is qualitatively different from any outcome that comes from user interaction with his or her service provider.

C. Back to the Basics – Dissecting Katz

The preceding discussion identifies the need to reevaluate the third-party doctrine and its continued significance in today's technological framework.[285] Taking a renewed look at the fundamentals of the

---

278 *See supra* Part II.

279 *See Quon*, 130 S. Ct. at 2630 (opining that following proper technological behavior would bolster an expectation of privacy).

280 *See infra* notes 281-84.

281 *See supra* notes 106-10 and accompanying text.

282 *See supra* notes 150-53 and accompanying text.

283 *See infra* notes 284 and accompanying text.

284 *See* THE INFO. SOC'Y ALLIANCE, *supra* note 123, at 1-2.

285 *See supra* Part II.B.

privacy interests under the Fourth Amendment,[286] I am drawn to the *Katz* holding. If there is a subjective expectation of privacy by the individual,[287] then the Fourth Amendment privacy interests must be evaluated at the next level of abstraction that requires evaluating the scope qualitatively and quantitatively.[288] An individual's subjective expectation of privacy must be evaluated and the means of evaluation is dependent on identifying society's reasonable expectation—an objective framework.[289] Therefore, the crux of the issue relies on identifying society's recognizable, reasonable expectations.[290] This is where the third-party doctrine presents a deterministic factor into the prevailing equation for two reasons.[291]

First, the third-party doctrine implies that, because an individual shared information with a third party, that individual's subjective expectation, by the construction itself, becomes null and void.[292] That means sharing triggers a voiding of such objective expectation.[293] The second analysis pertains to judicial determination.[294] This entails the second phase of the construction to evaluate the nature, scope, and quantitative element in that subjective expectation.[295] What makes that subjective expectation a reasonable expectation?

The judiciary can preempt any societal aspirations by simply adjudicating that the identified reasonable expectation is not legitimate.[296] There are specific exigent circumstances that can render such expecta-

286 *See* U.S. CONST. amend. IV.

287 *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

288 *See id.* at 362 (reasoning that although the particular search was unreasonable, there could be an instance where an "interception of a conversation one-half of which occurs in a public telephone booth [is] reasonable in the absence of a warrant").

289 *Id.* at 361.

290 *Id.*

291 *See infra* notes 292-95 and accompanying text.

292 *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

293 *See id.*

294 *Katz*, 389 U.S at 362 (Harlan, J., concurring).

295 *See* United States v. Miller, 425 U.S. 435, 442 (1976) ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."); *Katz*, 389 U.S. at 362 (noting that the nature of a conversation in a phone booth is to be kept private).

296 *See supra* Part II.

tion illegitimate by the judiciary on account of various societal and contemporary factors, as I have discussed in detail about the shaping effect of 9/11.[297]

Moreover, evaluation or recognition of society's reasonable expectation has been the subject of debate for reasons other than getting to the core of the third-party doctrine.[298] In this context, scholarship, at times, might have straddled the periphery of the third-party doctrine, instead of entering into the core of the argument.[299] For example, debates surrounding whether third-party interaction with the user is conducted by human interaction or via automated agent[300] do not quite get to the bottom of the doctrinal difficulties faced by the emergence of technology. Moreover, the third-party doctrine has been subject to criticism by some scholars on grounds that third-party interaction is predicated predominately on automated interaction, leading to conjecture on its lack of validity,[301] an assertion that does not quite get to the core issues faced in the Internet era. Thus, stepping away from the dichotomy between human interaction and an automated interaction, I see this to be an unnecessary debate that pushes the core doctrinal issues into superfluous territory. The fact remains fundamentally the same—if any interaction with a third party is fundamental to the existence of evolving life in the technological era, there should be no invocation of a third-party doctrine.[302] I dissect this further in the next section where I want to bring in the core values of privacy.[303]

D. Rejection of the Third-Party Doctrine: Against the Broader Privacy Fundamentals

I would like to extricate the conversation surrounding the third-party doctrine from a mere rehearsal of surface-level perturbation.[304] Rather, I want to confront the core privacy concern. These core privacy fundamentals, although emanated from a much deeper right-to-life in-

297 *See supra* Part II.

298 *See infra* notes 299-301 and accompanying text.

299 *See supra* note 47 and accompanying text.

300 *See* Tokson, *supra* note 184, at 586.

301 *Id.* at 586-87.

302 *See id.* at 584.

303 *See infra* Part III.D.

304 *See infra* notes 305-12 and accompanying text.

terpretation, have advanced for more than a century.[305] Long before the technological onslaught of the post-modern era, Justice Warren and Justice Brandeis invoked a deeper fundamental right to privacy[306] that has since been muted somewhat under the attack of states' heightened interests.[307] Emboldened by the shaping effect of 9/11,[308] premised on an exigency of situation framework, this liberty interest has been muted under superior state interests.[309] As the concept of the third-party doctrine has become relatively status quo in the minds of the judiciary, I want to remind the legal community of the nearly forgotten words of Justice Brandeis that are more relevant today than ever before: "[N]ow the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession—intangible, as well as tangible."[310] In the development of their basic premise, Warren and Brandeis formulated a paradigm where they used the right to privacy as "precedent" to establish the broader "right to be let alone."[311] With their original construction, the right to privacy was a plea for privacy in the midst of nineteenth-century technology.[312] Indeed, it seems that one hundred years of development in the privacy space has caused a sudden stoppage of the law's development alongside with technological advancement, something we must awaken to.

Warren and Brandies' conception of privacy originated from the recognition of the sacrosanct realms "of private and domestic life."[313]

---

305 *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-95 (1890) (discussing the need for privacy as technology developed in 1890).

306 *See id.* at 193.

307 *See* Goshray, *supra* note 8, at 195 n.150.

308 *See supra* Part II.

309 *See, e.g.*, Michael Posner, *Human Rights in the Post-September 11 Environment*, 5 SEATTLE J. SOC. JUST. 181, 183 (2006) (noting the Bush Administration felt the law was a luxury society couldn't afford, rather than a necessity, during the War on Terror).

310 *See* Warren & Brandeis, *supra* note 305, at 193.

311 *See* Powell, *supra* note 20, at 148 (quoting Warren & Brandeis, *supra* note 308, at 193).

312 *See* Warren & Brandeis, *supra* note 305, at 195-96.

313 *See id.* at 195.

The broader connotation of the right to be left alone indicates a deeper understanding of an individual's right of privacy within the confines that an individual creates.[314] Extrapolating this right to privacy would imply that these sacrosanct fundamentals would equally extend to the interior of the physical space called home and within the confines of the home-like community of connected individuals—be it within the Twitter community, the Facebook community, the MySpace community, or any other online community.[315] Just because technology has allowed the quantity and frequency of information to skyrocket does not necessarily preclude individuals from exercising their right to be left alone.[316] In this expanded concept of privacy, technological neutrality as espoused elsewhere cannot insulate the third-party doctrine from its inevitable obsolescence.[317] Indeed, technology and associated changes in social norms have created a necessity for more information to reside with the third party.[318] However, as I have indicated, the qualitative interactions and asymmetry with those interactions—between the user and the provider and the user and law enforcement—should be the benchmark to decide the continued applicability of the third-party doctrine.[319]

The explosion of technology has changed the way post-modern individuals conduct business, either through a means of automation or within cyberspace.[320] Life has changed. Despite the changes in activities, we must accept their analogous counterparts to truly understand the broader implication of the third-party doctrine.[321] Entering a bookstore is similar to ordering a book online.[322] Entering a shoe store and buying

---

314 *See id.* at 205.

315 *See supra* note 20 and accompanying text.

316 *See* Chip Walter, *A Little Privacy, Please*, SCI. AM. (June 17, 2007), http://www.scientificamerican.com/article.cfm?id=a-little-privacy-please.

317 *See* Kerr, *supra* note 24, at 561.

318 *See supra* Part III.

319 *See supra* notes 281-84 and accompanying text.

320 *See* Tokson, *supra* note 184, at 584-86.

321 *See infra* notes 322-27 and accompanying text.

322 *See, e.g.*, Alice Hines, *Walmart, Kmart, Sears, and eBay Offering 'Real' Online Shopping*, DAILY FIN. (Nov. 18, 2011, 6:30 AM), http://www.dailyfinance.com/2011/11/18/walmart-kmart-sears-and-ebay-offering-real-online-shopping/ (noting that online shopping and shopping in the store are so similar that some corporations are developing online shopping capabilities in their stores).

shoes is analogous to clicking a button, entering private information, and completing the purchase.[323] Just because a way of life has changed does not mean the outgrowth of these altered lifestyles should cause the loss of fundamental liberties.[324] Trying to purchase items online may cause these individuals to leave identifying information with the third party—acts that must not necessarily imply that such individuals have relinquished their privacy rights.[325] We must recognize that these individuals would likely have retained their privacy rights had they gone to the shoe store and paid with cash.[326] The law must be reconfigured to reflect this recognition and that must begin with reconceptualizing the third-party doctrine.[327]

We must recognize, therefore, that updating Facebook, using Twitter, and texting to express ranges of emotions are essential and integral activities performed inside the interior of the individual's physical space, called the private dwelling.[328] Just like the inside of the private dwelling provides an inner sanctum that an individual can evolve into his desired existence, updating Facebook and Twitter and texting are all components of post-modern existential being.[329] Like the individuals evolving inside the home have the full complement of Fourth Amendment privacy rights without the deleterious influence and attenuated nuance of the third-party doctrine,[330] individuals evolving within Facebook, MySpace, and Twitter should also possess the right to be left alone.

---

323 Online shopping is increasing. *See* Teresa Novellino, *E-commerce Doesn't Stop for Christmas*, PORTFOLIO.COM (Dec. 28, 2011, 10:01 AM), http://www.portfolio.com/views/blogs/executive-style/2011/12/28/online-shopping-up-16-percent-on-christmas-day (noting that during the 2011 holiday season there was a fifteen percent increase in online shopping from the corresponding days in 2010).

324 *See* Tokson, *supra* note 184, at 587.

325 *See, e.g.*, James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 5 (noting that privacy is important to those who shop online and those consumers want "more control over access to their personal information and subsequent use of the information after it is obtained").

326 *See id.* at 14.

327 *See supra* Part III.C.

328 *See supra* note 20 and accompanying text.

329 *See supra* note 20 and accompanying text.

330 *See supra* notes 275-80 and accompanying text.

IV. CONCLUSION

As we bask in the limitless possibilities of the hyper-technological era, we are rather disadvantaged in observing the growing disconnect between two important aspects of post-modern life.[331] On one side is all that technology provides, in terms of newer modicums of societal norms and innovative modes of individual expression.[332] On the other side resides the status quo, the stale law, the corpus of legal trajectory that is unable to evolve lockstep with the collective aspiration of humanity in protecting the deeper confines of individual privacy and unique individuality.[333]

Therefore, I argue that the third-party doctrine of the Fourth Amendment has come to a breaking point, more driven by the shaping effect of 9/11 than the individual's use of technology to subvert the law, more via disconnect with growing advancement of technology than owing to the doctrine's inability to sustain the law's original aspirations.[334] By examining the existing lament in legal scholarship regarding the continued viability of the third-party doctrine, this Article reveals an uncultivated dimension that is absent in contemporary discourse.[335] By adequately explaining the right of privacy through the prism of the right to life within the context of life evolving in cyberspace, I question the continued applicability of the third-party doctrine.[336] Detailing the modes of the automation world in which post-modern individuals navigate, existing judicial construction of the third-party doctrine may not suffer from a fatal flaw but indeed needs a facelift.[337] Is the judiciary ready?

---

331 *See infra* notes 332-33 and accompanying text.

332 *See* Zarsky, *supra* note 7, at 748.

333 *See generally* Moses, *supra* note 15.

334 *See supra* Part II.

335 *See supra* Part III.A.

336 *See supra* Part III.

337 *See supra* Part III.