

I AGREE: WHY SOCIETY’S DEPENDENCE ON E-MAIL IN THE FACE
OF NON-NEGOTIABLE TERMS OF SERVICE AND PRIVACY POLICIES
REQUIRES FOURTH AMENDMENT PROTECTIONS

*John Melloy III**

INTRODUCTION

It has been over fifty years since the first message was sent over the ARPANET, the small precursor to the Internet.¹ Today, billions of e-mails are sent to users around the world²—each with almost no legal protection for the personal, business, or otherwise private information contained in each message. The Internet has exploded beyond just communications to encompass entire facets of everyday life, including finance, health, and shopping, to name a few. Many routine services are now found on the Internet, operated and provided by private companies. For example, Google dominates the e-mail market through its Gmail service,³ meaning much of the public is dependent on Google to correspond with loved ones, create online accounts, and apply for jobs. This gives a company like Google access to enormous amounts of personal information, access that the user agreed to provide when they created an account.⁴ This model is common on the Internet: a private company offers some service, users agree to their terms and conditions by accessing or registering for that service, and those users provide

* George Mason University Antonin Scalia Law School, J.D. expected, 2025.

¹ See ARPANET, DARPA, <https://www.darpa.mil/about-us/timeline/arpamet> (last visited Oct. 30, 2022).

² The Radicati Group, *Number of Sent and Received E-mails per Day Worldwide from 2017 to 2026*, STATISTA, <https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/> (last visited Oct. 30, 2022).

³ Matthew McNulty, *Email Ranked: Look at What Provider is Tops in America*, FOX BUSINESS (Oct. 11, 2019, 1:36 AM), <https://www.foxbusiness.com/technology/email-providers-ranked-americas-choice>.

⁴ See, e.g., *Google Privacy & Terms*, GOOGLE, <https://policies.google.com/privacy?hl=en-US> (last visited Dec. 22, 2022); *Microsoft Privacy Statement*, MICROSOFT, <https://privacy.microsoft.com/en-us/privacystatement> (last visited Dec. 22, 2022).

personal information to the company by using that service as defined by those terms and conditions.⁵

This model directly conflicts with current Fourth Amendment jurisprudence. The Fourth Amendment protects an individual “against unreasonable searches and seizures” by the government.⁶ The Supreme Court has explained that this language specifically protects people and what they wish to preserve as private.⁷ Beginning in 1967, the Court created and expounded upon the “reasonable expectation of privacy”⁸ test, and now uses the test to determine whether something is or should be protected by the Fourth Amendment, including electronic communications, financial records, and GPS location data.⁹ At the same time, the Court also defined the third-party doctrine. This doctrine states that users do not have a reasonable expectation of privacy for information they have voluntarily provided to a third party and, therefore, forfeit any Fourth Amendment protection for that information.¹⁰ Thus, the standard model of Internet services falls squarely outside the protections granted by the Fourth Amendment, as users are dependent on providing information to third parties to use their services.

Nearly fifty years after its decisions outlining the reasonable expectation of privacy test, the Supreme Court in *Carpenter v. United States* defined an exception to the third-party doctrine, one which has the potential to have a huge impact on the Internet privacy landscape.¹¹ The Court found that individuals maintain a reasonable expectation of privacy regarding their cell-site location information (“CSLI”), even though this information is maintained by their cell providers—a third party.¹² Three factors supported this decision: (1) the “deeply revealing nature” of the CSLI data, (2) the sheer scale of the reach it granted law enforcement, and (3) the “inescapable and automatic nature” of the data

⁵ See David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, THE GUARDIAN (Mar. 3, 2017 8:38 AM), <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>.

⁶ U.S. CONST. amend. IV.

⁷ See *Katz v. United States*, 389 U.S. 347, 351 (1967).

⁸ *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

⁹ See, e.g., *United States v. Jones*, 565 U.S. 400 (2012); *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

¹⁰ *Miller*, 425 U.S. at 443.

¹¹ See *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

¹² *Id.* at 2217.

collection.¹³ Much of the discussion in the aftermath of *Carpenter* has been focused on the first two factors, drawing analogies between the incredibly revealing and easily abused nature of CSLI to many other types of information—such as health, genetic, and facial recognition data—to argue that these too deserve exceptions to the third-party doctrine.¹⁴

Yet the third factor, that the data is automatic and inescapable, is equally as important. It does not matter how revealing an individual's e-mail data is, for example, because the individual voluntarily giving it to Google invokes the third-party doctrine and, therefore, prevents any Fourth Amendment protection. Despite this apparent huge invasion of privacy, Google's Gmail is still the most widely used e-mail service,¹⁵ and alternatives such as Microsoft Outlook involve the very same third-party doctrine and loss of Fourth Amendment protection. Additionally, third-party e-mail providers exacerbate this issue by using take-it-or-leave-it terms of service and privacy policies as gateways to the services they provide. As most of society still requires some form of e-mail for everyday life,¹⁶ users are effectively required to further forfeit their privacy rights to their own information. Thus, providing personal information to these third parties for essential Internet services such as e-mail is not truly voluntary and, therefore, is just as inescapable as the CSLI in *Carpenter*.

¹³ *Id.* at 2223.

¹⁴ See, e.g., Emmanuel Abraham Perea Jimenez, Note, *The Fourth Amendment Limits of Facial Recognition at the Border*, 70 DUKE L.J. 1837 (2021); Jennifer D. Oliva, *Prescription-Drug Policing: The Right to Health-Information Privacy Pre- and Post-Carpenter*, 69 DUKE L.J. 775 (2020); Claire Abrahamson, Note, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 FORDHAM L. REV. 2539 (2019); Ryan Knox, *Fourth Amendment Protections of Health Information After Carpenter v. United States: The Devil's in the Database*, 45 AM. J.L. & MED. 331 (2019).

¹⁵ *Most Popular Email Providers in History*, STATISTICS & DATA (2022), <https://statisticsanddata.org/data/most-popular-email-providers-in-history/>.

¹⁶ See *Email Statistics Report, 2021-2025*, THE RADICATI GROUP, INC. 1, 2 (2021), https://www.radicati.com/wp/wp-content/uploads/2021/Email_Statistics_Report_2021-2025_Executive_Summary.pdf (last visited Oct. 25, 2023) ("Email is an integral part of the overall Internet experience as an email account (i.e. email address) is required to sign up to any kind online activity, including social networking sites, instant messaging and any other form of presence on the Internet. Online commerce also relies on email for confirmations, notifications and all pertinent communications."). See also Kate O'Flaherty, *How Private is Your Gmail, and Should You Switch?*, THE GUARDIAN (May 9, 2021, 4:00 AM), <https://www.theguardian.com/technology/2021/may/09/how-private-is-your-gmail-and-should-you-switch>.

This Comment argues that the *Carpenter* exception must apply to e-mail data, including e-mail content and related metadata, as e-mail is an inescapable Internet-based service that is effectively required for modern life. Part I will discuss the background of the Fourth Amendment in the age of electronic communications and how it developed through and including *Carpenter*. Part II will explain how the Court of Appeals for the Sixth Circuit in *United States v. Warshak* found a reasonable expectation of privacy regarding e-mail communications, despite the third-party doctrine. Part III will describe the take-it-or-leave-it clickwrap and browsewrap agreements commonly implemented in Internet terms of service and privacy policies. Part IV will show how these non-negotiable agreements, combined with society's dependence on e-mail, effectively require people to provide personal and revealing information to e-mail providers. Finally, Part V will argue that the *Carpenter* exception must apply to e-mail data because users maintain a reasonable expectation of privacy regarding their e-mail accounts.

BACKGROUND

I. THE FOURTH AMENDMENT IN THE TWENTIETH AND TWENTY-FIRST CENTURIES

Beginning in the late 1960s, the Supreme Court heard a series of cases that called into question the previous understanding of the Fourth Amendment as a protection against only physical trespass.¹⁷ The Fourth Amendment states that “[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.”¹⁸ As shown in early cases such as *Olmstead v. United States*, at one point the Court interpreted this protection to shield only physical property against physical searches and seizures.¹⁹ But starting with *Katz v. United States* in 1967, the Court discarded this restriction and found the Fourth Amendment to protect more than just physical property, such as telephonic communications.²⁰ Over the next five decades, the Court continued to outline the reasonable

¹⁷ See, e.g., *Katz v. United States*, 389 U.S. 347 (1967); *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).

¹⁸ U.S. CONST. amend. IV.

¹⁹ *Olmstead v. United States*, 277 U.S. 438, 464 (1928), *overruled by Katz*, 389 U.S. 347.

²⁰ *Katz*, 389 U.S. at 350–52.

expectation of privacy test and the third-party doctrine, most recently through its 2018 opinion in *Carpenter*.²¹

A. *Reasonable Expectation of Privacy*

The Supreme Court began the development of the modern understanding of the Fourth Amendment in *Katz v. United States*.²² In this case, the defendant Katz was convicted for transmitting gambling information via interstate telephone calls, an act that violated federal law.²³ FBI agents captured part of Katz's conversation by placing a listening device on the outside of the public phone booth that Katz was using and presented this conversation as evidence to try and convict Katz, over his objection.²⁴

In this seven-to-one decision, the Court overhauled the Fourth Amendment's protections by extending it beyond physical trespass, declaring that "the Fourth Amendment protects people, not places."²⁵ The Court distinguished between information that a person intentionally exposes to the public, and information that a person intends to keep private, with the former being unprotected by the Fourth Amendment and the latter within its scope.²⁶ It found that Katz reasonably relied on the privacy of the phone booth, and that the government violated this privacy when the FBI agents electronically listened to this conversation without a warrant.²⁷ Importantly, the Court placed special importance in the vital role of public telephones in society at the time.²⁸ The impact of this case would come to be summarized by the two-part reasonable expectation of privacy test outlined by Justice Harlan in his concurrence: that an individual is entitled to Fourth Amendment protections when (1) "that person ha[s] exhibited an actual (subjective) expectation of

²¹ *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

²² See Richard L. Aynes, Note, *Katz and the Fourth Amendment: A Reasonable Expectation of Privacy or, a Man's Home Is His Fort*, 23 CLEV. ST. L. REV. 63, 66 (1974) ("Katz not only extended fourth amendment protection to electronic surveillance situations, but also potentially altered all future application.").

²³ *Katz v. United States*, 389 U.S. 347–48 (1967).

²⁴ *Id.*

²⁵ *Id.* at 351.

²⁶ *Id.*

²⁷ *Id.* at 353.

²⁸ *Id.* at 352.

privacy,” and (2) “the expectation be one that society is prepared to recognize as ‘reasonable.’”²⁹

B. *Third-Party Doctrine*

The next major development in Fourth Amendment jurisprudence was the creation of the third-party doctrine, which represents a significant constraint on the protections granted by the Fourth Amendment. In *United States v. Miller*, Miller was convicted of violating federal law by possessing unregistered distilling equipment and untaxed whiskey.³⁰ As part of the investigation, federal agents subpoenaed two banks to obtain all checks, deposit slips, and financial statements corresponding to Miller for a period of three months.³¹ This accorded with the Bank Secrecy Act, which required banks to preserve such records for criminal investigative purposes.³² Miller objected to the use of this evidence as a violation of his Fourth Amendment rights.³³

The Court found no violation.³⁴ Its reasoning centered on the finding in *Katz* that “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”³⁵ The documents in question contained information that Miller voluntarily provided to the banks and that the banks used as part of their regular business transactions.³⁶ Thus, the Court found no reasonable expectation of privacy with regard to this information, because Miller objectively took the risk that his personal information would be shared with the government, even if he subjectively wished that information to remain private.³⁷

Importantly, this case applied the third-party doctrine specifically to the reasonable expectation of privacy test. As stated in *Miller*, the Court had previously found that individuals forfeit their Fourth Amendment protections for information voluntarily revealed to a

²⁹ *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

³⁰ *United States v. Miller*, 425 U.S. 435, 436 (1976).

³¹ *See id.* at 437–38.

³² *Id.* at 442–43; 12 U.S.C.A. § 1829b (West).

³³ *See Miller*, 425 U.S. at 436–37.

³⁴ *Id.* at 437.

³⁵ *Id.* at 442 (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)).

³⁶ *See United States v. Miller*, 425 U.S. 435, 442 (1976).

³⁷ *See id.* at 443.

third party.³⁸ Although the Court still had to “examine the nature of the particular documents sought,” because the documents obtained contained only information that Miller willingly provided to the bank and its employees, there could be no expectation of privacy.³⁹ This is the third-party doctrine, that individuals maintain no reasonable expectation of privacy concerning information voluntarily shared with others, even if the individual believes that the third party will or should keep that information confidential.⁴⁰

The Court further confirmed the third-party doctrine in *Smith v. Maryland* three years later.⁴¹ Here, the police had a phone company install a pen register to record the phone numbers dialed from Smith's home phone, and used that evidence in Smith's conviction for robbery.⁴² In upholding the conviction, the Court specifically cited and confirmed Justice Harlan's reasonable expectation of privacy test from *Katz*,⁴³ and further confirmed this to be separate from the trespass test for Fourth Amendment cases.⁴⁴ With that in mind, the Court analyzed the two elements of the test. First, it held that people in general, and Smith in particular, do not maintain a reasonable expectation of privacy for the phone numbers they dial.⁴⁵ Users must provide those numbers to their phone company, which stores and uses those numbers for a variety of business purposes.⁴⁶ The Court was not convinced that individuals maintain a subjective expectation that the phone numbers they call would remain secret, given the general awareness of the standard practice to store called numbers for purposes such as billing and spam detection.⁴⁷ Second, the Court reasoned that even if Smith had a

³⁸ *Id.* (citing *Hoffa v. United States*, 385 U.S. 293 (1966) (finding no Fourth Amendment protection for statements to a person who ended up being an informant because they were freely made); *Lopez v. United States*, 373 U.S. 427 (1963) (upholding the admissibility of a recorded conversation with the defendant because the defendant invited the federal agent into his office and willingly spoke to him); *United States v. White*, 401 U.S. 745 (1971) (finding no violation of the Fourth Amendment for listening to the defendant's conversations over a listening device carried by an informant because those conversations were voluntary)).

³⁹ *Miller*, 425 U.S. at 442.

⁴⁰ *Id.* at 443.

⁴¹ *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

⁴² *Id.* at 737–38.

⁴³ *Id.* at 740–41.

⁴⁴ *See id.* at 741–42.

⁴⁵ *Id.* at 742.

⁴⁶ *Id.*

⁴⁷ *Smith v. Maryland*, 442 U.S. 735, 742–43 (1979)

subjective expectation of privacy, it was not one that society was willing to accept as reasonable.⁴⁸ Like *Miller*, the Court found that Smith took the risk that the phone numbers he called would be shared with the government when he provided them to his phone company—a third party—and, therefore, any expectation of privacy with respect to that information would be unreasonable.⁴⁹

C. *The Path of Dissents to Carpenter*

Significantly, these cases defining the third-party doctrine were not unanimous decisions, and their dissenting opinions followed a pattern that culminated in *Carpenter*.⁵⁰ Dissenting in *Miller*, Justice Brennan argued that individuals do in fact maintain a reasonable expectation of privacy regarding the information they provide to banks.⁵¹ He largely quoted from Justice Mosk's opinion in the California Supreme Court case of *Burrows v. Superior Court*.⁵² In that case, dealing with practically the same factual background and an identical right under the California Constitution protecting against "unreasonable seizures and searches,"⁵³ the California Supreme Court came to a unanimous conclusion opposite that of the United States Supreme Court in *Miller*.⁵⁴ It held that the accused did maintain a reasonable expectation of privacy for his financial records and that he did not forfeit this expectation simply by providing that information to the bank.⁵⁵ Justice Brennan, through Justice Mosk's words, found that customers of banks reasonably believe that the information they provide to the banks will be used only by the bank for legitimate business purposes, and not shared without proper legal compulsion.⁵⁶ Moreover, he found that customers do not truly provide their information voluntarily as "it is impossible to participate in the economic life of contemporary society without maintaining a bank

⁴⁸ *Id.* at 743.

⁴⁹ *See id.* at 744.

⁵⁰ *See* *United States v. Miller*, 425 U.S. 435, 448 (1976) (7-2 decision) (Brennan, J., dissenting); *Smith*, 442 U.S. at 746 (5-3 decision) (Stewart, J., dissenting).

⁵¹ *Miller*, 425 U.S. at 448 (Brennan, J., dissenting).

⁵² *Id.* at 448-52 (quoting *Burrows v. Super. Ct.*, 529 P.2d 590, 593-96 (Cal. 1974)).

⁵³ CAL. CONST. art. I, § 13.

⁵⁴ *See Burrows*, 529 P.2d at 593-95.

⁵⁵ *Id.* at 593-94.

⁵⁶ *United States v. Miller*, 425 U.S. 435, 448-49 (1976) (Brennan, J., dissenting) (quoting *Burrows*, 529 P.2d at 593).

account.”⁵⁷ In the minds of both Justice Mosk and Justice Brennan, this effective social requirement overruled any appearance of a voluntary transfer of information. Further, because financial information can be incredibly revealing and is a “virtual current biography” of the customer, both dissenters feared that finding no reasonable expectation of privacy created limitless opportunities for abuses of police power.⁵⁸ Thus, Justice Brennan stated that this information should fall within the protection of the Fourth Amendment, despite Miller seeming to have provided it to the bank voluntarily.⁵⁹

The five-to-three case of *Smith* was significantly more split than *Miller*, although their respective dissenting opinions followed similar reasoning. Justice Stewart, joined by Justice Brennan, focused on the importance of private phone communications in society, and compared that to the clear vital role that the Court placed on public phones in *Katz*.⁶⁰ He argued that, if *Katz* was permitted to assume the privacy of his phone conversations despite transmitting them over telephone company equipment, then so too should *Smith* not have to forfeit the privacy of his called phone numbers simply because they are transmitted to the phone company.⁶¹ In both cases, the phone company could use equipment to record the numbers called and the conversations held. It was therefore inconsistent to protect the phone conversations in *Katz*, but refuse to protect the phone numbers in *Smith*, based on identical information sharing practices.⁶² In Justice Stewart’s opinion, the phone companies recording numbers is no more than a necessary part of telephone calls.⁶³ He concluded by stating that most of society would want a list of the phone numbers they call to remain private, as even that “easily could reveal the identities of the persons and the places called, and, thus, reveal the most intimate details of a person’s life.”⁶⁴

Justice Marshall, also joined by Justice Brennan, similarly dissented by arguing against applying the third-party doctrine in this case.⁶⁵ He reasoned that, even if customers understand that phone

⁵⁷ *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (quoting *Burrows*, 529 P.2d at 596).

⁵⁸ *See id.*

⁵⁹ *Miller*, 425 U.S. at 454 (Brennan, J., dissenting).

⁶⁰ *Smith v. Maryland*, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting).

⁶¹ *See id.* at 746–47.

⁶² *See id.*

⁶³ *See id.* at 746.

⁶⁴ *Id.* at 748.

⁶⁵ *See Smith*, 442 U.S. at 748 (Marshall, J., dissenting).

companies monitor their phone calls, they do not automatically expect that information to be made public or be shared with the government.⁶⁶ Importantly, he believed, “Privacy is not a discrete commodity, possessed absolutely or not at all.”⁶⁷ Further, he pointed out that the cases of *Lopez v. United States*,⁶⁸ *Hoffa v. United States*,⁶⁹ and *United States v. White*,⁷⁰ each of which the majority cited to defend applying the third-party doctrine in this case,⁷¹ involved conversations where the defendants actively chose whether and with whom to share their confidential information.⁷² Justice Marshall contrasted such a scenario with private telephone communications, arguing that a person cannot actively make such decisions regarding dialed phone numbers because individuals, such as Smith, have no realistic alternative other than abandoning private phone communications—“use of what for many has become a personal or professional necessity.”⁷³ Thus, Justice Marshall argued that using the third-party doctrine to remove all Fourth Amendment protections in this case ignored the important role that telephone communications play in society.⁷⁴ He concluded by defending Smith’s reasonable expectation of privacy regarding the numbers dialed from his personal phone, and, therefore, would have held that the warrantless installation of the pen register violated Smith’s Fourth Amendment rights.⁷⁵

D. *The Carpenter Exception*

Finally, in 2018 the Supreme Court published its decision in *Carpenter v. United States*, creating a powerful, if currently “narrow,”

⁶⁶ *Smith v. Maryland*, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

⁶⁷ *Id.*

⁶⁸ *See Lopez v. United States*, 373 U.S. 427 (1963) (upholding the admissibility of a recorded conversation with the defendant because the defendant invited the federal agent into his office and willingly spoke to him).

⁶⁹ *See Hoffa v. United States*, 385 U.S. 293 (1966) (finding no Fourth Amendment protection for statements to a person who ended up being an informant because they were freely made).

⁷⁰ *See United States v. White*, 401 U.S. 745 (1971) (finding no violation of the Fourth Amendment for listening to the defendant’s conversations over a listening device carried by an informant because those conversations were voluntary).

⁷¹ *See Smith*, 442 U.S. at 743–44.

⁷² *Smith v. Maryland*, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting).

⁷³ *Id.* at 750.

⁷⁴ *See id.* at 751.

⁷⁵ *See id.* at 752.

exception to the third-party doctrine.⁷⁶ In this case, Carpenter was charged with federal crimes connected to a series of robberies.⁷⁷ As part of the investigation, federal agents compelled two different wireless carriers to disclose cell-site location information (“CSLI”) data connected to Carpenter’s phone for a period of several months.⁷⁸ This data was used to track Carpenter’s location with incredible precision for the entirety of that time period, including specifically at the moment of a robbery.⁷⁹ The government also presented this location information at trial, over Carpenter’s objections, to secure his conviction.⁸⁰ The Court of Appeals for the Sixth Circuit affirmed his conviction, finding no reasonable expectation of privacy for this CSLI data because of the third-party doctrine.⁸¹

The Supreme Court overturned this ruling.⁸² The Court focused on “what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted,”⁸³ and reasoned that this analysis is not a strict test, but an approach designed to guarantee the same level of privacy that Americans reasonably expected at the time of the amendment’s passage—even in the face of modern, ever-developing surveillance technology.⁸⁴ Further, the Court affirmed the distinction between Fourth Amendment issues involving physical trespass and those involving information that a person wishes to preserve as private.⁸⁵ The Court specifically cited *Smith* and *Miller* to outline the third-party doctrine, but refused to apply it in this situation.⁸⁶ Importantly, the Court found that the unique nature of CSLI placed it outside of the scope of the third-party doctrine.⁸⁷ The Court put special importance on the data’s ability to track a user’s location to incredible specificity, reasoning that society has long held the expectation that law enforcement would not be able to track individuals with such

⁷⁶ See *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

⁷⁷ *Id.* at 2212.

⁷⁸ *Id.*

⁷⁹ See *id.* at 2213.

⁸⁰ See *id.* at 2212–13.

⁸¹ *Id.* at 2213.

⁸² *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

⁸³ *Id.* at 2214 (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)).

⁸⁴ *Carpenter*, 138 S. Ct. at 2214 (citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

⁸⁵ *Carpenter*, 138 S. Ct. at 2215–16.

⁸⁶ See *id.* at 2216–17.

⁸⁷ See *id.* at 2217.

granularity over a significant amount of time.⁸⁸ In Carpenter’s case, the Court held that law enforcement’s ability to track his precise location for a continuous period of about four months directly violated this reasonable expectation.⁸⁹

The Court reached this conclusion for two main reasons. First, it found that the third-party doctrine does not completely remove Fourth Amendment protections, but creates a presumption that the person no longer maintains a reasonable expectation of privacy.⁹⁰ Under this presumption, “the nature of the particular documents sought” must still be considered to determine whether the expectation of privacy is reasonable.⁹¹ In this particular case, the Court found that not only did this CSLI data have the potential to reveal Carpenter’s individual movements, but also that this precise location data for an extended period of time could easily reveal much about a person’s “familial, political, professional, religious, and sexual associations” and many other “privacies of life.”⁹² This potential deep insight into a person’s private life was both unacceptably revealing and easily abused in the hands of law enforcement—two points that became the first two elements of the exception.

Additionally, the Court reasoned that the automatic nature of the data was unique compared to the previous third-party doctrine cases.⁹³ Providers continuously log this CSLI data for every user and, thus, law enforcement does not need to know ahead of time whether a person should be tracked.⁹⁴ Instead, investigators can effectively reach back in time and discover an individual’s pattern of life, and “[o]nly the few without cell phones could escape this tireless and absolute surveillance.”⁹⁵ Importantly, the Court held that having one’s CSLI data collected is effectively not voluntary, as “carrying [a cell phone] is indispensable to participation in modern society,” and users generate and share this data with their provider without an affirmative act of

⁸⁸ See *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

⁸⁹ *Id.* at 2219.

⁹⁰ See *id.*

⁹¹ See *id.* (quoting *United States v. Miller*, 425 U.S. 435, 442 (1976)).

⁹² *Carpenter*, 138 S. Ct. at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886))).

⁹³ See *id.* at 2220.

⁹⁴ See *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

⁹⁵ *Id.*

consent besides simply using their phone.⁹⁶ Thus, individuals such as Carpenter do not truly assume the risk of the third party sharing this information with the government in the same way that the Court found Smith and Miller did.⁹⁷

Importantly, the Court specifically held this to be a narrow exception, requiring a warrant only in the rare case where an individual maintains a reasonable expectation of privacy with information held by a third party.⁹⁸ The Court also made clear, however, that the Fourth Amendment must be carefully examined in light of new and emerging technologies, and that care must be taken to ensure such technological improvements do not undermine Fourth Amendment protections.⁹⁹ Thus, the Court created the *Carpenter* exception: in the rare case where the data sought is incredibly revealing, easily abused by law enforcement, and individually inescapable, the third-party doctrine will not apply.¹⁰⁰

E. *Post-Carpenter Analysis*

Despite it being purportedly a narrow exception, the *Carpenter* decision kickstarted a vigorous debate on its potential impacts and applications to numerous other fields of technology.¹⁰¹ Generally, the focus has been on the first two factors of the *Carpenter* exception, that the data sought is incredibly revealing and easily abused,¹⁰² prompting arguments to apply *Carpenter* to the likes of cloud storage data, facial recognition information, and some confidential communications.¹⁰³ In a time that we now call the Information Age,¹⁰⁴ it can be a simple thing

⁹⁶ *Id.* at 2220.

⁹⁷ *See id.*

⁹⁸ *See id.* at 2220, 2222.

⁹⁹ *See id.* at 2223.

¹⁰⁰ *See Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

¹⁰¹ *See, e.g.*, Steven Arango, *Cloudy with A Chance of Government Intrusion: The Third-Party Doctrine in the 21st Century*, 69 CATH. U. L. REV. 723 (2020); Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter?*, 26 B.U. J. SCI. & TECH. L. 286 (2020); Mihailis E. Diamantis, *Privileging Privacy: Confidentiality As A Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485 (2018).

¹⁰² *Cf., e.g.*, Arango, *supra* note 101, at 736; Jimenez, *supra* note 14, at 1877.

¹⁰³ *See, e.g.*, Arango, *supra* note 101; Gee, *supra* note 101. *Cf.* Diamantis, *supra* note 101.

¹⁰⁴ *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (“Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age.”).

to show that the sheer volume of information generated and collected is just as revealing and abusable as CSLI data.¹⁰⁵

Yet, whether because of the newness of the decision, or because of a hesitance to expand *Carpenter* beyond CSLI, a significant number of cases relying on *Carpenter* have not found a similar protection.¹⁰⁶ The reasons for this may be wrapped up in a lack of understanding of the logic behind the decision, or other reasons related to the function of the criminal justice system.¹⁰⁷ But it could be based in part on the third element of the *Carpenter* exception, the automatic and inescapable nature of the information sought.¹⁰⁸ Health information, location data, and e-mail communications generally have the appearance of being intentionally shared with a third party, and, thus, until this third element can be met, the *Carpenter* exception will not apply.

II. THE STORED COMMUNICATIONS ACT AND *WARSHAK*'S REASONABLE EXPECTATION OF PRIVACY FOR E-MAIL

E-mail communications are covered by the Stored Communications Act (“SCA”),¹⁰⁹ a federal law that permits the government to compel an electronic communications service provider to disclose the contents of communications, such as e-mail, subject to certain conditions.¹¹⁰ Specifically, how long the electronic communication has been in electronic storage determines the level of protection it receives.¹¹¹ The government requires a warrant to compel disclosure of communications in storage for under 180 days,¹¹² but for any data stored longer, the government can compel disclosure through a warrant, an administrative subpoena, or a court order.¹¹³ Notably, these additional options for communications stored for longer than 180 days create a significantly

¹⁰⁵ See *Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2020, with Forecasts from 2021 to 2025*, STATISTA (2023), <https://www.statista.com/statistics/871513/worldwide-data-created/> (last visited Sept. 3, 2023).

¹⁰⁶ Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1809 (2022).

¹⁰⁷ See *id.* at 1809–11.

¹⁰⁸ See *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018).

¹⁰⁹ 18 U.S.C. § 2701(a).

¹¹⁰ § 2703(a).

¹¹¹ See § 2703(a)-(b)(1).

¹¹² § 2703(a).

¹¹³ § 2703(b)(1).

lower bar than a warrant: the government does not need to establish probable cause, only “reasonable grounds” that the communications sought contain “information relevant and material to an ongoing criminal investigation.”¹¹⁴

The Sixth Circuit analyzed the overlap of the SCA and a reasonable expectation of privacy regarding e-mail in *United States v. Warshak*.¹¹⁵ In this case, the government obtained a court order requesting NuVox Communications to preserve the e-mail communications of Steven Warshak, who was under investigation for various federal financial crimes.¹¹⁶ The government used those e-mail communications to convict Warshak, who then appealed, claiming a violation of his Fourth Amendment rights.¹¹⁷

The Sixth Circuit agreed.¹¹⁸ In applying the reasonable expectation of privacy test, the court found that Warshak easily satisfied the first part of the test because he manifested a subjective intent to protect the contents of his e-mails from the public, which often contained sensitive and damning information—“for people seldom unfurl their dirty laundry in plain view.”¹¹⁹ The second part of the test, that society is prepared to recognize that expectation as reasonable, involved a more complex analysis. The Sixth Circuit noted the importance of this discussion, analogizing the prominent role of e-mail in modern society to that of public telephones at the time of the *Katz* decision.¹²⁰ The court found that e-mail communications now play a central role in a wide range of public uses, including personal and sensitive exchanges, business communications, and commerce.¹²¹ The court considered access to one’s e-mail account to grant more than just access to communications: “In short, ‘account’ is an apt word for the conglomeration of stored messages that comprises an e-mail account, as it provides an account of its owner’s life. By obtaining access to

¹¹⁴ § 2703(d). See also Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 382 (2009).

¹¹⁵ See *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

¹¹⁶ *Id.* at 283.

¹¹⁷ *Id.* at 281–82.

¹¹⁸ *Id.* at 288.

¹¹⁹ *Id.* at 284.

¹²⁰ *Id.*

¹²¹ See *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

someone's e-mail, government agents gain the ability to peer deeply into his activities."¹²²

The court further analogized e-mail communications to phone conversations and letters, both of which maintain a level of Fourth Amendment protections despite the ability of a third party to view the contents of those communications.¹²³ The court reasoned that e-mails are simply the digital version of those communications, and, thus, they must be granted the same level of protection.¹²⁴ Specifically, the court ruled that the ability or right of a third party to access the contents of a communication does not defeat an individual's reasonable expectation of privacy.¹²⁵ Importantly, the court distinguished this from the case of *Miller* and refused to apply the third-party doctrine.¹²⁶ It did so not only because the potentially limitless access to confidential communications differed from the ordinary business records of *Miller*, but also because NuVox Communications was simply the intermediary of Warshak's e-mails, versus the bank in *Miller* being the intended recipient of Miller's bank records.¹²⁷ Thus, the third-party doctrine did not apply in this case, because NuVox Communications's ability to read the contents of Warshak's e-mails as an intermediary did not defeat Warshak's reasonable expectation of privacy.

Significantly, the *Warshak* court distinguished this case—concerning an Internet service provider that did not expressly intend to audit or monitor the contents of e-mail—from the situation where the provider contractually requires that it can inspect the contents of e-mail communications.¹²⁸ In such a case, the court found that such an express intention or contract “might” be sufficient to defeat any expectation of privacy.¹²⁹ What would tip the scale from preserving such an expectation to defeating it remains undetermined.

¹²² *Id.*

¹²³ *Id.* at 285 (citing *United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Katz v. United States*, 389 U.S. 347, 348 (1967)).

¹²⁴ *See Warshak*, 631 F.3d at 285–86.

¹²⁵ *See id.* at 286–87.

¹²⁶ *Id.* at 288.

¹²⁷ *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

¹²⁸ *See id.* at 287.

¹²⁹ *Id.*

III. PRIVACY POLICIES AND TERMS OF SERVICE: INTERNET CONTRACTS WITH NO REASONABLE OPPORTUNITY TO NEGOTIATE

Privacy policies and terms of service are contracts at their core, and, under general contract law, an enforceable contract requires a manifestation of mutual assent, either through affirmative action or indirect inaction.¹³⁰ This has not changed in the age of the Internet and online terms of service and privacy policies.¹³¹ In *ProCD, Inc. v. Zeidenberg*, the Seventh Circuit ruled that the individual who purchased software was bound to the license terms of that software because they were displayed on the computer screen before every use, which provided the actual notice of the terms required for a manifestation of assent.¹³² This “shrinkwrap” agreement, where notice of further terms could only be read after purchasing and opening the product,¹³³ is the precursor for the “clickwrap” and “browsewrap” agreements found on the Internet today.¹³⁴

In determining whether the user manifested assent to terms of service for online contracts, courts distinguish between two types of agreements: clickwrap and browsewrap.¹³⁵ Clickwrap agreements are those that require the user to affirmatively agree to the terms, generally by clicking on a button that says “I Agree,” or something similar.¹³⁶ Courts usually uphold contracts through clickwrap agreements because the required affirmative agreement to abide by the terms of service provides the user with actual knowledge of the terms, and this knowledge

¹³⁰ RESTATEMENT (SECOND) OF CONTRS. §§ 17, 19 (AM. L. INST. 1981).

¹³¹ See *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1450 (7th Cir. 1996) (“[W]e treat the licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts.”); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007) (“To determine whether a clickwrap agreement is enforceable, courts presented with the issue apply traditional principles of contract law and focus on whether the plaintiffs had reasonable notice of and manifested assent to the clickwrap agreement.”); *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 231–32 (2d Cir. 2016) (citing *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 403 (2d Cir. 2004)) (“Indeed, as we have explained on multiple occasions, ‘new commerce on the Internet . . . has not fundamentally changed the principles of contract.’”).

¹³² See *ProCD, Inc.*, 86 F.3d at 1452.

¹³³ See *id.* at 1449.

¹³⁴ See, e.g., *Specht v. Netscape Commun. Corp.*, 306 F.3d 17, 32 (2d Cir. 2002); *Nicosia*, 834 F.3d at 232; *Meyer v. Uber Techs., Inc.*, 868 F.3d 66, 72 (2d Cir. 2017).

¹³⁵ *Meyer*, 868 F.3d at 72. See also *Nicosia*, 834 F.3d at 233; *Specht*, 306 F.3d at 32; *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1175–76 (9th Cir. 2014).

¹³⁶ *Meyer*, 868 F.3d at 75.

is enough to assume assent.¹³⁷ In contrast, browsewrap agreements do not require express assent, and so courts use a fact-dependent inquiry to determine whether the user has actual or constructive knowledge of the terms of the agreement.¹³⁸ As this inquiry is context-dependent, courts have sometimes decided that a reasonable computer user would not have had actual or constructive knowledge of the existence of the terms, and, therefore, are not bound because there was no assent.¹³⁹

Although service providers can use either clickwrap, browsewrap, or some hybrid approach,¹⁴⁰ this Comment does not focus on the distinction between the two types. Rather, it assumes for the purposes of this discussion that service providers such as Google and Microsoft either implement a clickwrap or browsewrap agreement that provides sufficient notice, or they could easily do so. In fact, a cursory investigation into the process of registering for a Google Gmail or Microsoft Outlook e-mail account shows that this assumption is likely true.¹⁴¹ Further, this Comment does not explore whether or to what extent the terms of most privacy policies and terms of service are objectionable or otherwise substantively unconscionable, which could render them unenforceable.¹⁴² These are interesting and important topics of discussion, best suited for another paper.

Thus, regardless of whether the service provider uses a clickwrap or browsewrap agreement, so long as it provides the required constructive notice, registering for or using the service creates an enforceable

¹³⁷ See *id.* at 75; *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 238 (2d Cir. 2016); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007); *Specht*, 306 F.3d at 22 n.4.

¹³⁸ See *Meyer*, 868 F.3d at 67; *Nguyen*, 763 F.3d at 1177–78; *Nicosia*, 834 F.3d at 233. See also *Schnabel v. Trilegiant Corp.*, 697 F.3d 110, 129 n.18 (2d Cir. 2012) (citing *Specht*, 306 F.3d at 30–32).

¹³⁹ See, e.g., *Nicosia*, 834 F.3d at 236–37 (“Nothing about the ‘Place your order’ button alone suggests that additional terms apply, and the presentation of terms is not directly adjacent to the ‘Place your order’ button so as to indicate that a user should construe clicking as acceptance.”); *Specht*, 306 F.3d at 31–32 (“Moreover, the fact that, given the position of the scroll bar on their computer screens, plaintiffs may have been aware that an unexplored portion of the Netscape webpage remained below the download button does not mean that they reasonably should have concluded that this portion contained a notice of license terms.”). *Contra Meyer*, 868 F.3d at 79–80 (“A reasonable user would know that by clicking the registration button, he was agreeing to the terms and conditions accessible via the hyperlink, whether he clicked on the hyperlink or not.”).

¹⁴⁰ See *Nicosia*, 834 F.3d at 236.

¹⁴¹ See *Create Account*, MICROSOFT, <https://signup.live.com/signup> (last visited Dec. 22, 2022); *Create Your Google Account*, GOOGLE, <https://accounts.google.com/signup/v2/webcreateaccount?flowName=GlifWebSignIn&flowEntry=SignUp> (last visited Dec. 22, 2022).

¹⁴² See *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996) (“Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general.”).

contract, binding the user to the associated terms of service and privacy policies. Refusal to assent to the terms can only be accomplished by refusing to use the service altogether. This effective procedural unconscionability creates a take-it-or-leave-it barrier to use services on the Internet, many of which are practically essential.

ANALYSIS

I. IN MODERN SOCIETY DEPENDENT ON THE INTERNET, USERS HAVE NO CHOICE BUT TO AGREE TO PRIVACY POLICIES AND PROVIDE PERSONAL INFORMATION TO THIRD PARTIES

Modern society is rife with technology. The Internet of Things and smart home devices have brought the Internet into contact with everyday life, and the COVID-19 pandemic only exacerbated this development, shifting entire fields of services and employment to the Internet.¹⁴³ Importantly, there are a handful of fundamental technologies that are essential to access Internet resources and to use basic Internet services.¹⁴⁴ The use of these technologies is therefore inevitable for any who wishes to participate in modern society.¹⁴⁵ One prime example is e-mail: as a foundational piece to the modern Internet ecosystem of instant communication, using an e-mail service—and providing personal information to the e-mail provider—is just as inescapable as sharing CSLI with cell providers in *Carpenter*.¹⁴⁶

¹⁴³ Anja Feldmann et al., *A Year in Lockdown: How the Waves of COVID-19 Impact Internet Traffic*, 64, 7 COMM'NS OF THE ACM 101, 107 (2021).

¹⁴⁴ See Cynthia K. Sanders and Edward Scanlon, *The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion Through Social Work Advocacy*, NATIONAL LIBRARY OF MEDICINE (March 19, 2021), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7973804/>; Catherine Howell and Darrell West, *The Internet as a Human Right*, BROOKINGS (Nov. 7, 2016), <https://www.brookings.edu/articles/the-internet-as-a-human-right/>.

¹⁴⁵ See *Importance of Internet in Daily Life*, ASIANET BLOGS, <https://asianetbroadband.in/importance-internet-daily-life/> (2023).

¹⁴⁶ Compare *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (quoting *Riley v. California*, 573 U.S. 373 (2014)) (“In the first place, cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.”) with Morey Haber, *Why Every Person Needs At Least Four Email Accounts*, FORBES (Feb. 13, 2020, 7:40 AM), <https://www.forbes.com/sites/forbestechcouncil/2020/02/13/why-every-person-needs-at-least-four-email-accounts/?sh=2e1d57267006>, and *Internet Basics: What Can You Do Online?*, GCFGLOBAL, <https://edu.gcfglobal.org/en/internetbasics/what-can-you-do-online/1/> and *What is Email? How to Trace an Email Address?*, WHATIS MYIPADDRESS, <https://whatismyipaddress.com/email-basics#:~:text=One%20thing%20you%20may%20>

A. *E-mail is an Inescapable Technology Essential to Modern Society*

Participation in modern society effectively requires individuals to use certain technologies. For example, Supreme Court Justice Brennan and California Justice Mosk believed individuals must maintain an active bank to participate in regular economic life.¹⁴⁷ Similarly, Justice Marshall in his dissent in *Smith* called telephonic communications a personal or professional necessity.¹⁴⁸ Most recently, the Court in *Carpenter* found cell phones to be “such a pervasive and insistent part of daily life” that individuals cannot escape using them.¹⁴⁹ Especially in the age of the Internet, certain technologies are simply foundational and effectively required for participation in modern society—meaning individuals realistically cannot escape using them.

E-mail is one of these inescapable technologies. Opening one’s work e-mail is a common ritual to start a day in the office, assuming the employer does not require employees to be responsive and tied to their e-mail accounts at all hours of the day.¹⁵⁰ Moreover, the shift to work-from-home employment necessitates the use of such a work e-mail for everything from scheduling meetings to basic collaboration.¹⁵¹ Before even being able to work such a job, one would have to submit a job application, which if not done via e-mail, would probably require an active e-mail account to communicate the results anyway. Likewise, colleges and universities often provide school e-mail accounts to every incoming student to provide class updates, school notifications,

20be,our%20IP%20address%20and%20email (“Email is as common as having a telephone for just about all of us. There are about two billion email users around the world. In 2012, Google said it had 425 million email users worldwide, and Microsoft said it had more than 360 million Windows Live Hotmail customers. And most of us have more than one email account—one at work and a few for our personal use at home.”).

¹⁴⁷ *United States v. Miller*, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting); *Burrows v. Super. Ct.*, 529 P.2d 590, 596 (Cal. 1974).

¹⁴⁸ See *Smith v. Maryland*, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

¹⁴⁹ *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 387).

¹⁵⁰ See Nicole Lyn Pesce, *The Average Worker Checks Their Email Before They Even Get Out of Bed in the Morning*, MARKETWATCH (Feb. 9, 2019, 6:15 AM), <https://www.marketwatch.com/story/the-average-worker-checks-their-email-before-they-even-get-out-of-bed-in-the-morning-2019-02-06>.

¹⁵¹ See Alex Hern, *Covid-19 Could Cause Permanent Shift Towards Home Working*, THE GUARDIAN (Mar. 13, 2020, 1:11 PM), <https://www.theguardian.com/technology/2020/mar/13/covid-19-could-cause-permanent-shift-towards-home-working>.

and other similar messaging.¹⁵² Furthermore, banks,¹⁵³ health care providers,¹⁵⁴ and countless other services all depend on active e-mail accounts to communicate with their users.¹⁵⁵ Unless a person is willing to forfeit access to such services, complicate their college education, limit themselves to only disconnected jobs, and otherwise separate themselves from the modern version of the postal system, that person will inevitably find themselves with an e-mail account.

This parallels the inescapability of generating and sharing CSLI data in *Carpenter*. The Court specifically found that cell phones are “indispensable to participation in modern society.”¹⁵⁶ As a result, the Court found individuals do not have a realistic choice whether to use these devices, and by extension whether to generate and share the corresponding CSLI data.¹⁵⁷ In the Court’s opinion, the practical requirement of cell phones combined with the automatic sharing of CSLI data to create no meaningful choice for users regarding sharing this revealing data with third parties.¹⁵⁸ Similarly, individuals have no realistic alternative but to have an active e-mail account. As the Sixth Circuit argued in *Warshak*, “E-mail . . . plays an indispensable part in the Information Age.”¹⁵⁹ E-mail has become a standard means of communication in the modern world, being used for both business and personal correspondence, and otherwise effectively being an “essential means or necessary instrument[] for self-expression, even

¹⁵² See Elkafi Hassini, *Student–Instructor Communication: The Role of Email*, 47, 1 *COMPUTS. & EDUC.* 29, 30 (2004).

¹⁵³ See David Fouse, *Do Banks Rely Too Heavily On Email For Customer Communication?*, *FORBES* (Jul. 20, 2021), <https://www.forbes.com/sites/forbesagencycouncil/2021/07/20/do-banks-rely-too-heavily-on-email-for-customer-communication/?sh=4c70ae175031>.

¹⁵⁴ See Beverly Kane and Daniel Z. Sands, *Guidelines for the Clinical Use of Electronic Mail with Patients*, 5 *J. AM. MED. INFORM. ASSOC.* 104, 104–11 (1998) (discussing guidelines for the clinical use of email with patients).

¹⁵⁵ See *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (“Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments.”).

¹⁵⁶ *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

¹⁵⁷ See *Carpenter*, 138 S. Ct. at 2220.

¹⁵⁸ *Id.*

¹⁵⁹ *Warshak*, 631 F.3d at 286.

self-identification.”¹⁶⁰ Thus, regular participating members of society do not have any meaningful alternative besides providing personal information to an often limited selection of third-party providers of e-mail services. As the *Warshak* court argues, to find otherwise is to ignore the importance that e-mail plays in regular communication¹⁶¹—much like the importance of telephonic communications argued in the *Katz* and *Smith* decisions.¹⁶² In none of these situations do individuals truly share information with their providers “voluntarily,” as the alternative is to remove themselves from modern society altogether. Like the users of phones in *Carpenter*, only the few who manage to live their lives without e-mail would escape providing companies like Google and Microsoft with seemingly limitless personal information.¹⁶³ Thus, sharing this personal information via e-mail is just as inescapable as the CSLI data in *Carpenter*.

B. *Non-Negotiable Terms of Service and Privacy Policies Exacerbate this Inescapability*

Not only are e-mail services inescapable, but users are forced to comply with complex terms of service and privacy policies when using or registering for these services in the first place. Whether through an affirmative clickwrap agreement, like Google requires when registering for an account,¹⁶⁴ or through implied assent via a browsewrap agreement, like Microsoft implements for its account registration,¹⁶⁵ users must agree to whatever the terms of service and privacy policies require. These requirements involve agreements to share personal information with the service provider and sometimes other third parties, and generally include both user-provided information and automatically generated data.¹⁶⁶ Not only is there no opportunity to negotiate these

¹⁶⁰ *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (quoting *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010)).

¹⁶¹ *Warshak*, 631 F.3d at 286.

¹⁶² See *Katz v. United States*, 389 U.S. 347, 352 (1967) (“To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”); *Smith v. Maryland*, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting) (“The use of pen registers, I believe, constitutes such an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships . . .”).

¹⁶³ See *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

¹⁶⁴ *Create Your Google Account*, *supra* note 141.

¹⁶⁵ *Create Account*, *supra* note 141.

¹⁶⁶ See, e.g., *Google Privacy & Terms*, *supra* note 4; *Microsoft Privacy Statement*, *supra* note 4.

agreements, but they usually consist of dozens of pages of complex legal and technical language, making it difficult for any user to fully understand what data is being shared and with whom.¹⁶⁷ Thus, for an essential service such as e-mail, users effectively take no affirmative action to share personal information with third parties beyond simply using their required service and thereby agreeing to any related terms of service and privacy policies.

While the clickwrap and browsewrap agreements found in Internet terms of service have the appearance of an affirmative action, by either legally assuming users' acceptance or requiring it, in reality users have no reasonable alternative other than to accept the terms as is, because they have no reasonable opportunity to negotiate. When registering for a Gmail account, for example, there is no option to dispute the terms of service.¹⁶⁸ Users cannot simply call Google and argue for more favorable terms—if an individual wishes to have a Gmail account, they must agree to the terms as is. This take-it-or-leave-it approach for effectively essential services means users are forced to accept whatever the terms of service and privacy policies require concerning generating and sharing personal information.

Further, those privacy policies often demand extensive forfeiture of privacy from users. For example, Google's privacy policy states that the company collects information created or provided by the user, such as e-mail content and search terms, and information generated by using Google's services, such as activity history and location data.¹⁶⁹ Thus, users must consent to allow Google to collect this information if they wish to use a service such as Gmail. Similarly, Microsoft's Privacy Statement states that the company collects information from data both provided by the user and generated by their activity.¹⁷⁰ This also includes e-mail content, device identifiers, contacts and relationships, location data, and other similar types of information.¹⁷¹ Users must consent to this collection to use any of Microsoft's services, including Outlook e-mail.

Even the personalization options that allow users to opt out of some data sharing are generally limited. For example, Microsoft provides

¹⁶⁷ *Id.*

¹⁶⁸ See *Create Your Google Account*, *supra* note 141.

¹⁶⁹ *Google Privacy & Terms*, *supra* note 4.

¹⁷⁰ *Microsoft Privacy Statement*, *supra* note 4.

¹⁷¹ *Id.*

an opt-out page that allows users to control some aspects of personal data collection, but caveats this with this statement: “Not all personal data processed by Microsoft can be accessed or controlled via the tools above.”¹⁷² Similarly, service providers often allow users to delete some parts of their data, but even that is limited short of deleting the user’s account altogether.¹⁷³ Moreover, even though an opt-in model would be more apt for affirmatively agreeing to share this data,¹⁷⁴ these opt-out options often restrict the functionality of the service. For example, Microsoft’s privacy statement says:

When we ask you to provide personal data, you can decline. Many of our products require some personal data to provide you with a service. If you choose not to provide data required to provide you with a product or feature, you cannot use that product or feature. . . . Where providing the data is optional, and you choose not to share personal data, features like personalization that use such data will not work for you.¹⁷⁵

This means that there is a certain amount of personal data required to use Microsoft’s services.¹⁷⁶ Granted, service providers like Microsoft and Google should not be mandated to make features available regardless of privacy personalization options, as, for example, it is impossible to provide an e-mail service without asking for the recipient’s e-mail address. Rather, it is because of this impossibility that users are required to provide personal information to these third parties or otherwise forgo the ability to use these services, because that is the only way for them to perform their essential functions. A user cannot opt out of the essential functions of an e-mail service any more than they could opt out of an e-mail service entirely.

Moreover, terms of service and privacy policies often contain dozens or even hundreds of pages of complex legal jargon, meaning

¹⁷² *Id.*

¹⁷³ See, e.g., *Google Privacy & Terms*, *supra* note 4 (“We keep some data until you delete your Google Account, such as information about how often you use our services. . . . And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.”).

¹⁷⁴ See Fara Soubouti, Note, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 540–41 (2020) (“Opt-in consent is a stronger method of consumer control and requires affirmative action by a user to explicitly grant a company permission to use the consumer’s information.”).

¹⁷⁵ *Microsoft Privacy Statement*, *supra* note 4.

¹⁷⁶ See *id.*

most users are not even aware of what personal information service providers generate or store.¹⁷⁷ Certainly, they can take the time and effort to read any agreements before using the service, but it is not always clear what the agreement entails. For example, Google's Privacy Policy contains several sections of important information regarding how Google handles users' information.¹⁷⁸ Buried in these sections are dozens of footnotes and hyperlinks that contain yet more pertinent information for the privacy-conscious user.¹⁷⁹ Although there are some helpful videos available,¹⁸⁰ a user must pour through all of these legal and technical explanations to fully understand how the service provider generates, shares, or stores personal information—a significant effort to simply ask Google to send and receive e-mails. The vast majority of users do not have the time, patience, or training to understand a legal document concerning technical privacy.¹⁸¹ These constraints on users' ability to actively choose whether to share personal information with third parties—and whether to agree to the privacy policies at all—only exacerbate the inherent inescapability of doing so for an essential technology such as e-mail.

II. THE *CARPENTER* EXCEPTION CAN, AND MUST, APPLY TO E-MAIL AS AN ESSENTIAL INTERNET-BASED SERVICE

The Fourth Amendment must protect e-mail data as an essential Internet-based service, because individuals maintain a reasonable expectation of privacy regarding their e-mail accounts, and the *Carpenter* exception can and must prevent the third-party doctrine from defeating it. The reasonable expectation of privacy test has two parts, (1) “that person ha[s] exhibited an actual (subjective) expectation of privacy,” and (2) “that the expectation be one that society is prepared to recognize as ‘reasonable.’”¹⁸² As the Sixth Circuit showed in *Warshak*, the first element is simple to satisfy regarding e-mail communications.¹⁸³ Thus, whether such information satisfies this test turns on the second element, whether society recognizes expecting

¹⁷⁷ See Berreby, *supra* note 5.

¹⁷⁸ See *Google Privacy & Terms*, *supra* note 4.

¹⁷⁹ See *id.*

¹⁸⁰ See *id.*

¹⁸¹ See Berreby, *supra* note 5.

¹⁸² See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

¹⁸³ See *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

privacy in email communications as reasonable, which implicates the third-party doctrine and the *Carpenter* exception.¹⁸⁴

That exception must apply, because personal information generated and shared with the service providers of e-mail accounts is just as inescapable and automatic as the CSLI data in *Carpenter*. There are three parts to the *Carpenter* exception: (1) the particularly revealing nature of the data sought, (2) the abusable character of that data, and (3) the inescapable and automatic nature of the data collection.¹⁸⁵ Concerning e-mail contents and metadata, service providers such as Google and Microsoft store and analyze this data because the information is deeply revealing and they can use it for enormous financial gain.¹⁸⁶ In other words, this data is stored precisely because this information satisfies the first two elements of *Carpenter*. Google's Privacy Policy states two general types of information it collects on users of its services: (1) "Things you create or provide to us," and (2) "Information we collect as you use our services."¹⁸⁷ This second category comes in a few different forms: app, browser, and device information; activity data; and location information.¹⁸⁸ This data is not only used for directly providing the service, but also for many other uses including improving Google's services, personalization, and legal protection for the company.¹⁸⁹ This usage highlights both the revealing nature of this data and the financial benefits gained by the provider.

Similarly, Microsoft's Privacy Statement outlines the same types of information that it collects: some provided by the user and some generated by the user's use of its services.¹⁹⁰ This can include device data, usage information, location data, personal interests, social data, and so on.¹⁹¹ Microsoft collects this information for a similar purpose as Google, to operate their business and also to improve their products and personalize the service.¹⁹² In other words, e-mail providers such

¹⁸⁴ See *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018).

¹⁸⁵ See *id.* at 2223.

¹⁸⁶ See Megan Case, *Google, Big Data, & Antitrust*, 46 DEL. J. CORP. L. 189, 199–200 (2022) ("The more data Google is able to collect, the more it is able to solidify its economic dominance . . .").

¹⁸⁷ *Google Privacy & Terms*, *supra* note 4.

¹⁸⁸ *Id.*

¹⁸⁹ See *id.*

¹⁹⁰ *Microsoft Privacy Statement*, *supra* note 4.

¹⁹¹ *Id.*

¹⁹² See *id.*

as Google and Microsoft collect particularly revealing information on their users generated by their e-mail accounts to expose and effectively monetize their personal data.

Moreover, the revealing and abusable nature of the CSLI data is analogous to that of an e-mail address. The Court in *Carpenter* argued that the ability of the CSLI data to reveal the “familial, political, professional, religious, and sexual associations” and many other “privacies of life” created the need for an exception to the third-party doctrine.¹⁹³ In addition, the ability of law enforcement to effectively obtain a precise chronology of a person’s movements was too easily abused to permit.¹⁹⁴ The Sixth Circuit in *Warshak* makes a similar argument for e-mail data.¹⁹⁵ It found that an e-mail account was effectively an account of the user’s life¹⁹⁶—in stark contrast to the strictly business records sought in *Miller*.¹⁹⁷ Thus, access to an e-mail account would grant law enforcement incredible insight into an individual’s activities over an expansive amount of time,¹⁹⁸ access that would be deeply revealing and easily abused.

The third *Carpenter* requirement, however, that the information be inescapable and automatic in nature, is equally as important as the first two. As e-mail is essential to a society dependent on the Internet,¹⁹⁹ sharing personal information with e-mail providers is inescapable and effectively automatic. The Supreme Court has previously highlighted the personal and business necessity of telephonic communications and cell phone services, and used that to justify greater Fourth Amendment protections because individuals have no realistic alternative but to use those services.²⁰⁰ Further, the Sixth Circuit has also identified the increasing importance of e-mail communications in modern society.²⁰¹ Just as the Court found that the indispensability of cell phones

¹⁹³ *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *Riley v. California*, 573 U.S. 373, 403 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

¹⁹⁴ See *Carpenter*, 138 S. Ct. at 2218.

¹⁹⁵ *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

¹⁹⁶ See *id.* at 284.

¹⁹⁷ See *United States v. Miller*, 425 U.S. 435, 442–43 (1976).

¹⁹⁸ See *Warshak*, 631 F.3d at 284.

¹⁹⁹ See *id.* at 284–86.

²⁰⁰ See *Katz v. United States*, 389 U.S. 347, 352 (1967). See also *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (“[C]ell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society.”).

²⁰¹ See *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

created the need for greater privacy protections,²⁰² so too should the necessity of the service upon which society depends for modern communication—e-mail.

Additionally, the Court in *Carpenter* specifically pointed out that users take no affirmative action to share their CSLI data with their cell provider beyond turning their phone on.²⁰³ Similarly, the type of information collected by email providers is not limited to actively created data, but also includes location information, device identifiers, activity history, and other similarly generated metadata.²⁰⁴ More significantly, even if the e-mail provider implements a clickwrap agreement requiring the user to click an “I Agree” button, the user has no realistic choice but to consent without negotiating the terms involved.²⁰⁵ For example, when registering for a Gmail account, users are presented with a choice between two options: consent to the terms of service and privacy policy, or not use the service.²⁰⁶ But effectively there is no choice at all, because users cannot realistically refuse to have an e-mail account.²⁰⁷ The user could opt for a different service provider, but that provider will have similar terms of service and privacy policies and so present the same choice.²⁰⁸ Thus, in reality, users do not make the affirmative choice to agree to share personal information with e-mail providers because there is no realistic alternate option. Therefore, the data collected is effectively just as inescapable and automatic as the CSLI information in *Carpenter*. As such, personal data generated and shared by using e-mail services must be subject to the *Carpenter* exception.

Furthermore, users intending to share some of this information with a specific recipient, for example e-mail content, does not justify applying the third-party doctrine over the *Carpenter* exception with respect to the e-mail provider. The Sixth Circuit in *Warshak* found a reasonable expectation of privacy regarding e-mail communications because the user intended to share that information only with a specific recipient, not the public in general or even the service provider in particular.²⁰⁹ The service provider’s status as an intermediary and not

²⁰² See *Carpenter*, 138 S. Ct. at 2220.

²⁰³ *Id.*

²⁰⁴ See *Google Privacy & Terms*, *supra* note 4; *Microsoft Privacy Statement*, *supra* note 4.

²⁰⁵ See *Carpenter*, 138 S. Ct. at 2220.

²⁰⁶ See *Create Your Google Account*, *supra* note 141.

²⁰⁷ See *United States v. Warshak*, 631 F.3d 266, 284–86 (6th Cir. 2010).

²⁰⁸ See, e.g., *Microsoft Privacy Statement*, *supra* note 4.

²⁰⁹ See *Warshak*, 631 F.3d. at 288.

the intended recipient was crucial to the court's decision.²¹⁰ The Sixth Circuit specifically contrasted this with the facts in *Miller*, where the bank was the intended recipient of Miller's bank records in the course of ordinary business.²¹¹ In comparison, Warshak's e-mail provider was not the intended recipient of his vast collection of personal information. Instead, the provider just operated as the intermediary and, therefore, the court did not apply the third-party doctrine.²¹² Similarly, e-mail providers are not the intended recipients of e-mail information: companies like Google and Microsoft are only the intermediaries. As the Sixth Circuit stated, the ability of these companies to access the information does not automatically defeat a reasonable expectation of privacy²¹³ and, therefore, the *Carpenter* exception to the third-party doctrine must apply.

While the court in *Warshak* did not decide whether a reasonable expectation of privacy would survive when the provider expressly intended to inspect the contents of e-mail communications,²¹⁴ it did so before the Supreme Court created the *Carpenter* exception for inescapable, automatic personal data collection. Because the take-it-or-leave-it privacy policies allow e-mail providers to demand access to deeply revealing personal e-mail accounts and serve as gatekeepers to essential e-mail services, this requirement is satisfied. Significantly, the Court in *Carpenter* found a notable difference between using a phone to obtain location data for a particular time and compiling a detailed collection of physical movements over several years.²¹⁵ Likewise, there is a compelling difference between obtaining a single e-mail sent to a third party, compared to accessing an entire e-mail account simply because the account is provided by a third party. Thus, e-mail providers such as Microsoft and Google requiring access to the accounts they provide does not prevent applying the *Carpenter* exception to the third-party doctrine regarding e-mail information.

Finally, the existence of niche providers such as Proton Mail—that claim to deliver greater privacy protections for their users²¹⁶—does not

²¹⁰ *See id.*

²¹¹ *Id.* at 288.

²¹² *Id.*

²¹³ *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010).

²¹⁴ *See id.* at 287.

²¹⁵ *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

²¹⁶ PROTON, <https://proton.me/about> (last visited Dec. 22, 2022).

defeat the inescapability of sharing personal data simply to use e-mail services. First and foremost, Proton Mail and others like it are still created by a third party, meaning users are still dependent on them for access to essential services. Moreover, this proposed workaround simply creates yet another barrier for users seeking to protect their Fourth Amendment rights. If Fourth Amendment protections are dependent on exclusively using services such as Proton Mail, then ordinary users must not only be legally knowledgeable enough to parse through complex privacy policies, but also technologically savvy enough to research niche solutions to privacy issues. Importantly, the Court has affirmed its intention to protect “that degree of privacy against government that existed when the Fourth Amendment was adopted.”²¹⁷ In *Carpenter*, the Court understood this to create an approach designed to guarantee the same level of privacy that Americans reasonably expected at the time of the Fourth Amendment’s passage.²¹⁸ Specifically, the Court must use this approach to ensure that modern, developing technology does not erode and undermine Fourth Amendment rights.²¹⁹ It is doubtful that the Founders at the time of ratification expected ordinary Americans to endure such great lengths to protect the intimate details of their personal lives from exposure.²²⁰ Thus, it is unreasonable to limit the right to privacy to only those users who are both technically and legally knowledgeable enough to understand the consequences of their actions.

CONCLUSION

The Supreme Court’s opinion in *Carpenter* stands to revolutionize modern Fourth Amendment doctrine. Although the extent of its impact is far from known, as technology continues to evolve and become more pervasive in everyday life, it is almost certain that cell-site location information will not be the only third-party-held data that society wishes to preserve as secret. E-mail communication is only a single example of an Internet-based service that individuals realistically have no choice

²¹⁷ See *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

²¹⁸ See *Carpenter*, 138 S. Ct. at 2213–14.

²¹⁹ See *id.* at 2223.

²²⁰ See *id.* at 2214 (quoting *Kyllo*, 533 U.S. at 34) (“We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to ‘assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’”)

but to use. Thus, though the *Carpenter* exception must apply to e-mail communications specifically, it will likely not end there. Web browsers, search engines, and operating systems are a few other arguably essential technologies that may be analogous to e-mail under *Carpenter*. Perhaps other services such as messaging apps or social media are approaching the point of being “inescapable,” if they have not reached it already. As Justice Sotomayor accurately predicted in her concurring opinion in *United States v. Jones*: “[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age.”²²¹ The Supreme Court began reconsidering that premise in *Carpenter*, but the American judicial system must continue to do so as technology promises to advance even more rapidly, and further conflict with the understandings of those who ratified the Fourth Amendment.

²²¹ *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

