UNIVERSITY *of* PENNSYLVANIA
LAW REVIEW

Founded 1852

Formerly
AMERICAN LAW REGISTER

VOL. 172 JANUARY 2024 NO. 2

ARTICLE

TERMS OF SERVICE AND FOURTH AMENDMENT RIGHTS

ORIN S. KERR†

Almost everything you do on the Internet is governed by Terms of Service. The language in Terms of Service typically gives Internet providers broad rights to address potential account misuse. But do these Terms alter Fourth Amendment rights, either diminishing or even eliminating constitutional rights in Internet accounts? In the last five years, many courts have ruled that they do. These courts treat Terms of Service like a rights contract: by agreeing to use an Internet account subject to broad Terms of Service, you give up your Fourth Amendment rights.

This Article argues that the courts are wrong. Terms of Service have little or no effect on Fourth Amendment rights. Fourth Amendment rights are rights against the

† William G. Simon Professor, University of California, Berkeley Law School. Thanks to Riana Pfefferkorn and Rebecca Wexler for comments on an earlier draft.

government, not private parties. Terms of Service can define relationships between private parties, but private contracts cannot define Fourth Amendment rights. This is true across the range of Fourth Amendment doctrines, including the "reasonable expectation of privacy" test, consent, abandonment, third-party consent, and the private search doctrine. Courts that have linked Terms of Service and Fourth Amendment rights are mistaken, and their reasoning should be rejected.

INTRODUCTION 288
I. TERMS OF SERVICE AND DIVIDED COURTS 291
A. *Introduction to Terms of Service* 292
B. *Cases Holding That Terms of Service Determine Fourth Amendment Rights* 294
C. *Cases Holding That Terms of Service Do Not Determine Fourth Amendment Rights* 300
II. TERMS OF SERVICE AND EXPECTATIONS OF PRIVACY 304
A. *Fourth Amendment Rights in Shared Space* 305
B. *Does Formalizing the Sharing Arrangement Matter?* 307
C. *The Effect of Owner–User Agreements on Car Rentals, Apartment Leases, and Hotel Rentals* 308
D. *The Special Case of Government Spaces and Government Policies* 313
III. TERMS OF SERVICE AND RIGHTS-LOSING DOCTRINES 317
A. *Four Ways to Lose Rights in Shared Space* 318
B. *Irrelevance to the Private Search Doctrine* 321
C. *Irrelevance to Third-Party Consent* 322
D. *Irrelevance to Direct Consent* 324
E. *Irrelevance to Abandonment* 326
CONCLUSION 327

INTRODUCTION

When you use the Internet, you are using computer networks that belong to others. You are visiting computers around the country, and sometimes around the world, that are typically owned by large companies.[1] Those companies have lawyers. And those lawyers want to make sure you can't sue those companies for how you use their services.[2] So they do what lawyers do

1 The top five most visited websites belong to large companies: Google, YouTube, Facebook, Amazon, and Yahoo. *Top Websites Ranking*, SIMILARWEB, https://www.similarweb.com/top-websites/united-states/ [https://perma.cc/8RS6-H58S] (last visited Jan. 25, 2023).

2 *See generally* Jessica R. Friedman & Gerry A. Fifer, *Website Development and Hosting Agreements for Terms of Service*, *in* REPRESENTING THE NEW MEDIA COMPANY 2000, at 469, 476-

best: they put it in writing. As a condition of use, the services require users to agree to contractual language giving the company broad rights over your use of their machines. Those contractual terms, usually called Terms of Service, appear to users like an endless CVS-receipt of legalese that they click through on the way to setting up an account.[3]

This essay considers the effect of Terms of Service on Fourth Amendment rights. In particular, it asks whether language in Terms of Service can limit or even eliminate user Fourth Amendment rights. If Terms of Service say you have no rights, or only limited or conditional rights, do those Terms control? In *Carpenter v. United States*[4] and *Riley v. California*,[5] the Supreme Court has suggested that the Fourth Amendment applies broadly to computers and the Internet. The Fourth Amendment requires a warrant if the government wants to obtain the contents of your messages, or even certain non-content records.[6] But Terms of Service threaten that conclusion. If such Terms can narrow or eliminate Fourth Amendment rights online, then those rights may be an illusion. What the Supreme Court has given, Terms of Service might take away.

This is a genuine and pressing problem. In the last five years, the effect of Terms of Service on Fourth Amendment rights has been frequently litigated in lower courts.[7] Judges have divided sharply. A few opinions say the Terms make little difference.[8] But a majority of courts have treated Terms of Service like a rights contract: by agreeing to use the service, they reason, you agree to whatever narrowing or elimination of rights that the contract implies.[9] Using the service becomes a waiver of Fourth Amendment rights that gives up a reasonable expectation of privacy or consents to any future search.[10] The case law is recent, and existing legal scholarship has not yet addressed, or even recognized, the problem.[11] But the decisions suggest a

81 (2000) (Practising Law Institute Intellectual Property Course Handbook Series No. G-587, 2000) (providing website owners with an overview of points to consider in drafting a Terms of Service agreement).

3 Terms of Service are also called "Terms of Use." The two phrases are widely used interchangeably, although I will use the former label in this article.

4 138 S. Ct. 2206 (2018).

5 134 S. Ct. 2473 (2014).

6 *See Carpenter,* 138 S. Ct. at 2221 (holding that the Fourth Amendment requires a warrant to compel historical cell site location records covering at least seven days of use).

7 *See* discussion *infra* Sections I.B–C.

8 *See* discussion *infra* Section I.C.

9 *See* discussion *infra* Section I.B.

10 *See id.*

11 I commented in passing on this question in a 2010 article. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1031 & n.100 (2010) ("Terms of Service may have a role in defining Fourth Amendment rights as well, although I believe their role is in determining whether a user has consented or given the provider third-party consent

troubling reality: our Fourth Amendment rights online hinge on the effect of Terms of Service.[12]

This Article argues that Terms of Service have little or no impact on Fourth Amendment rights. With limited exceptions, Terms of Service cannot reduce or eliminate Fourth Amendment protections. The courts that have held to the contrary are wrong, and their reasoning should be rejected.[13] The explanation rests on the underappreciated role of private contracts in Fourth Amendment law. The Fourth Amendment provides rights against the government, and agreements between private parties and the government can relinquish Fourth Amendment rights. But Terms of Service play a different role. They define legal relationships between private parties, such as those between private network provider and private network user. Agreements among private parties do not relinquish rights. As private agreements, Terms of Service might help clarify relationships relevant to some Fourth Amendment doctrines.[14] But it is the relationships, not the language found in Terms of Service, that matter.

From a practical perspective, this Article has an important doctrinal payoff: it secures Fourth Amendment rights online against the threat of nullification by Terms of Service. It explains why courts should reject a dystopian future in which our Fourth Amendment rights are at the mercy of form contracts written by lawyers for multinational corporations. That result would not only be disturbing. It also turns out to be wrong.

The Article also makes a deeper point about the nature of Fourth Amendment rights. Rights against unreasonable searches and seizures are rights against the government that rest on a judicial judgment that spaces and information are *yours*. Rights in shared space are common, and formalizing expectations between private parties sharing space has little or no impact on those rights. As a result, the language of private contracts cannot define Fourth Amendment protections. This explains why violating an apartment

rights, not whether the provisions in a Terms of Service eliminate a reasonable expectation of privacy."). My views have evolved since that time, as this article shows. There has been little other comment on the issue. The most in-depth treatment is a student note that discusses some of the early case law, described below in Section I.B, that has viewed Terms of Service as controlling. *See* Eric Johnson, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 STAN. L. REV. 867, 898-909 (2017). The Note assumes that those cases are correct, and it focuses on how providers can draft Terms to maintain Fourth Amendment rights. *Id.* As explained in this Article, however, the cases that the Note relies on were wrongly decided and their reasoning should be rejected.

12 The arguments have now been briefed, and are currently awaiting decision, in appellate courts. *See, e.g.*, Brief of the United States as Appellee at 33, United States v. Bohannon, No. 21-10270 (9th Cir. Sept. 27, 2022) ("[B]y agreeing to Microsoft's Terms of Service, Bohannon expressly authorized Microsoft to consent to a government search of Bohannon's files.").

13 *See infra* Parts II–III.

14 *See id.*

lease or breaching a rental car contract does not narrow or eliminate search and seizure protections. When we apply the Fourth Amendment to the Internet, the same rule should apply to Terms of Service. Fortunately, search and seizure rights are made of sterner stuff—both offline and online.

The argument proceeds in three parts. Part I introduces the role of Terms of Service. It explains the different types of Terms, introducing the difference between rules-of-the-road provisions and breach provisions. It then summarizes the recent case law on the role of Terms of Service in Fourth Amendment law. It shows that courts are divided on whether Terms define Fourth Amendment rights, and that many courts recently have agreed that Terms eliminate those rights.

Part II explains why Terms of Service cannot reduce or eliminate reasonable expectations of privacy online. Private contracts have little effect in Fourth Amendment law because the nature of those rights is against the government rather than private parties. This is reflected in case law on other owner–user agreements, such as apartment leases and rental contracts, and Terms of Service should follow the same path. Courts that have erroneously held otherwise have mistakenly followed case law on Fourth Amendment rights for government employees. Policies control in that one context because the government is the property owner, but that case law cannot be extended to private Internet providers.

Part III then considers the Fourth Amendment doctrines that might lead to lost privacy because of Terms of Service even if a reasonable expectation of privacy exists. It considers four such doctrines: the private search doctrine, consent, third-party consent, and abandonment.[15] It explains why, in each case, Terms of Service are irrelevant to how these doctrines apply. Terms can in some cases clarify relationships that have Fourth Amendment relevance. But the actual relationships, not formal language, controls. And Terms of Service are particularly unlikely to clarify relationships because few people read them and even fewer understand what they say.

I. TERMS OF SERVICE AND DIVIDED COURTS

This part explains what Terms of Service are and why they have come to be relevant to Fourth Amendment rights online. It explores existing case law, most of it in the last few years, that has divided on the effect of Terms of Service on Fourth Amendment rights.

15 *See infra* Part III.

A. *Introduction to Terms of Service*

There are many Terms inside typical Terms of Service—they often run many pages long—but two categories of Terms are particularly important for Fourth Amendment rights. The first kind of term is what I will call *rules-of-the-road provisions*. These Terms set expectations about how a service will be run, such as what the company will do with your data in various circumstances. The second kind of term is what I will call *breach provisions*. The Terms define a contract, and these Terms explain what the company considers a breach that allows the company to limit or delete the user's account. Of course, the Terms can be related: a term of service can tell users the rules-of-the-road if they breach. But it is helpful to recognize the two types of Terms, even if they can blend in practice.

An example can help make this concrete. A majority of American adults have Facebook accounts, run by the company now known as Meta.[16] The account Terms of Service include the following:[17]

- "Meta may access, preserve, use and share any information it collects about you where it has a good faith belief it is required or permitted by law to do so."[18]
- If Meta learns of "misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community," they "may take appropriate action based on our assessment that may include - notifying you, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement."[19]
- "You may not upload viruses or malicious code, use the services to send spam, or do anything else that could disable, overburden, interfere with, or impair the proper working, integrity, operation, or appearance of our services, systems, or Products."[20]
- "[Y]ou cannot use Facebook if [any one of these are true]: You are under 13 years old . . . . You are a convicted sex offender . . . . We've previously

16 Pew Research Center, in a 2021 survey, estimated that about 69% of American adults at least occasionally use Facebook. Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RESEARCH CENTER (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/ [https://perma.cc/PWC2-YNGV].

17 *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/SC9E-4U76] (last modified July 26, 2022).

18 *Id.*

19 *Id.*

20 *Id.*

> disabled your account for violations of our Terms or the Community Standards . . . ."[21]

Note how the various Terms match the two categories. The first two are rules-of-the-road provisions. They set expectations for what Meta can do. Facebook is a product, after all, and these Terms tell you about the product and what Meta does as it provides the product. The last two are breach provisions. They tell users what the users cannot do with their Facebook accounts. Meta hosts several billion Facebook accounts,[22] and one of its jobs in providing Facebook is moderating and suspending problematic accounts.[23] The breach provisions tell the user what Facebook will treat as a breach that can, if Facebook so chooses, lead to some action such as moderation or suspension.

It should be no surprise that these Terms are broad. Companies such as Meta make money from serving advertising, and the more targeted the advertising, the higher the rates.[24] Terms of Service typically give companies broad authority to do what they want with your data.[25] Similarly, Terms will prohibit a range of potentially harmful acts that you might do with the account.[26] Again, that is to be expected. You may be one of potentially billions of users, and businesses want maximum flexibility to do what they want with your account.

What does this have to do with the Fourth Amendment? As Part II explains, my view is that the correct answer is, well, not much. But for now I want to ask a different question: why *might* Terms of Service be relevant? Put another way, why might someone think that Terms of Service have an important influence on Fourth Amendment rights?

The answer is that Terms of Service purport to define rights in data, which is exactly what Fourth Amendment protection rests upon. To have Fourth Amendment rights in information, a person ordinarily must have a

---

21 *Id.*

22 According to Meta, 3.03 billion Facebook accounts were used on at least a monthly basis during the quarter that ended June 30, 2023. *See* Press Release, Meta Platforms, Inc., Meta Reports Second Quarter 2023 Results (July 26, 2023), https://s21.q4cdn.com/399680738/files/doc_financials/2023/q2/Meta-06-30-2023-Exhibit-99-1-FINAL.pdf [https://perma.cc/DP3G-SFNQ].

23 *See, e.g.*, Republic of the Gambia v. Facebook, Inc., 575 F. Supp. 3d 8 (D.D.C. 2021) (considering rights in suspended accounts following content moderation).

24 *See* YAN LAU, FED. TRADE COMM'N, A BRIEF PRIMER ON THE ECONOMICS OF TARGETED ADVERTISING 7 (2020) (discussing charges for targeted and untargeted ads).

25 *Cf.* Stuart A. Thompson, *These Ads Think They Know You*, N.Y. TIMES (Apr. 30, 2019), https://www.nytimes.com/interactive/2019/04/30/opinion/privacy-targeted-advertising.html [https://perma.cc/GME2-V6JV] (describing the sale of customer data collected on the Internet to marketing companies).

26 *See, e.g.*, *supra* note 20 and accompanying text.

reasonable expectation of privacy in that information.[27] And after a person has a reasonable expectation of privacy in data, their rights are often subject to what other people might do with their data, such as granting third party consent to search.[28] On their face, then, Terms of Service seem to define exactly what the Fourth Amendment law cares most about. We can express the argument as a syllogism: Fourth Amendment protection requires rights; Terms of Service define rights in online accounts; and therefore Terms of Service define Fourth Amendment protection in online accounts.

In the last five years, lower courts have handed down a string of cases on whether this syllogism is valid. When rules-of-the-road provisions give providers broad rights, courts have asked, does that empowering of the provider eliminate the user's reasonable expectation of privacy or constitute consent to any searches? When a user violates a breach provision, courts ask, does the fact of the breach make the user an unauthorized person who cannot claim rights in the account? Courts have divided. A quick overview of the recent case law, presented below, frames how far the syllogism might run and how far the stakes of the subject extend.

B. *Cases Holding That Terms of Service Determine Fourth Amendment Rights*

We begin with the cases adopting the syllogism about the role of Terms of Service. These cases look to Terms of Service to define Fourth Amendment rights, finding that such Terms often reduce or entirely eliminate otherwise-existing constitutional protections.

The Pennsylvania Supreme Court's 2021 ruling in *Commonwealth v. Dunkins* is a useful starting point.[29] Police at a private college identified a robber who had entered a college dorm room by asking the college system administrators to tell them what student accounts were logged into the campus wifi in that dorm at the time the robbery occurred.[30] The list was compiled and disclosed to the police. It revealed that there was only one account associated with a male student who did not live in the dorm on the list—Dunkins, the defendant.[31] That tip led to further evidence and the defendant's arrest, and he later moved to suppress the evidence on the ground that it was a fruit of the unlawful surveillance of his account in violation of his Fourth Amendment rights. The trial court rejected the claim because the

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

28 *See* United States v. Miller, 425 U.S. 435, 443 (1976).

29 263 A.3d 247, 249 (Pa. 2021).

30 *See id.* at 249.

31 *See id.* at 249-50.

records were not protected by the Fourth Amendment under *Carpenter v. United States*.[32]

The Pennsylvania Supreme Court agreed with the Superior Court's result but adopted a different rationale. Instead of addressing whether *Carpenter* applied, the Supreme Court held that the college network's Terms of Service had defeated any Fourth Amendment rights Dunkins might have had.[33] Students at the college were required to accept the college's Computing Resources Policy as a condition of having an account. That policy included broad waivers. One term stated that a user "cannot and should not have any expectation of privacy with regard to any data . . . created or stored on computers within or connected to the institution's network."[34] Another term stated that "[a]ll Internet data composed, transmitted, or received through the institution's computer system is considered part of the institution's records and, as such, subject at any time to disclosure to institutional officials, law enforcement, or third parties[.]"[35]

According to the Pennsylvania Supreme Court, Dunkins had abandoned any Fourth Amendment rights in the data because of the Terms of Service. Agreeing to the Terms, and then logging on to the network, "provid[ed] clear intent to relinquish any purported expectation of privacy in the WiFi connection records."[36] In the language suggested earlier, the college's Computing Resource Policy imposed rules-of-the-road provisions. By agreeing to use the Internet service, users agreed to whatever happened to their data. According to *Dunkins*, agreeing to those rules-of-the-road amounted to a waiver of all Fourth Amendment rights.

The Seventh Circuit's 2019 ruling in *United States v. Adkinson*,[37] favorably cited in *Dunkins*,[38] runs along similar lines. Following robberies at T-Mobile stores, T-Mobile investigated the cell phone location records of its T-Mobile cell service customers and found that only one customer, Adkinson, had been in the area of both robberies.[39] T-Mobile then gave the records to the FBI, although it was unclear whether the FBI had first requested the records. When Adkinson later challenged government access to his records, the Seventh Circuit rejected his claim on four independent grounds, including

---

32 Commonwealth v. Dunkins, 229 A.3d 622, 629 (Pa. Super. 2020), *allocatur granted*, 237 A.3d 415 (2020) (per curiam) (citing Carpenter v. United States, 138 S. Ct. 2206 (2018)).

33 *See Dunkins*, 263 A.3d at 255 (concluding that the appellant did not have any purported expectation of privacy, given that he accepted the Terms of Service when he voluntarily connected to the WiFi network).

34 *Id.*

35 *Id.*

36 *Id.*

37 916 F.3d 605 (7th Cir. 2019).

38 *Dunkins*, 229 A.3d at 630.

39 *Adkinson*, 916 F.3d at 608.

that T-Mobile was a private actor, that Adkinson had no Fourth Amendment rights in the records, and that the good-faith exception applied.[40]

But the Seventh Circuit added a fourth argument, that "Adkinson consented to T-Mobile collecting and sharing his cell-site information"[41] by agreeing to T-Mobile's Terms of Service. Those Terms allowed T-Mobile to disclose private information about user accounts "[t]o protect [T-Mobile's] rights or interests, property or safety or that of others."[42] As a matter of law, the court reasoned, "A defendant can voluntarily consent in advance to a search as a condition of receiving contracted services."[43] Signing up for a T-Mobile account had created "consent in advance" to conduct that complied with the Terms. Much like in *Dunkins*, the Terms in *Adkinson* were rules-of-the-road provisions that were deemed to control Fourth Amendment rights. A user could not object to the provider following the rules-of-the-road that the user had agreed to in advance.

Many of the additional cases treating Terms of Service as controlling involve providers scanning for Child Sexual Abuse Material (CSAM), sometimes called "child pornography." Some background may be helpful. The major Internet providers, and the major cloud providers, have programs in place in which they scan the contents of user account files looking for known images of CSAM.[44] The scans rely on "hashes," cryptographic numbers that enable images to be identified without a person actually seeing them based on a match with known files.[45] When a hash match is found, providers report the images to the National Center for Missing and Exploited Children (NCMEC).[46] NCMEC then opens the file, and if it contains the suspected CSAM file, they report the finding to law enforcement.[47]

Many cases challenging this process have been resolved on state action grounds. Because the providers scan voluntarily, courts have reasoned, they are private actors rather than state actors and the Fourth Amendment does

---

40 *Id.* at 610-11.

41 *Id.* at 610.

42 *Id.* at 608 (quoting T-Mobile's Terms of Service).

43 *Id.* at 610 (citing Medlock v. Trustees of Indiana Univ., 738 F.3d 867, 872 (7th Cir. 2013)).

44 *See* Michael H. Keller & Gabriel J.X. Dance, *Child Abusers Run Rampant as Tech Companies Look the Other Way*, N.Y. TIMES (Nov. 9, 2019), https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html [https://perma.cc/3CYG-BBFK] (detailing such scanning programs).

45 *See NCMEC, Google and Image Hashing Technology*, GOOGLE: GOOGLE SAFETY CTR., https://safety.google/stories/hash-matching-to-help-ncmec/ [https://perma.cc/5SZ6-3FPP] (explaining how hashes help facilitate the detection of CSAM).

46 *See id.*

47 *See id.* ("[NCMEC has] a really important job, which is to take [information about potential CSAM] and turn it around as quickly as possible to law enforcement.").

not apply to their conduct.[48] But some cases have taken a different path, ruling that the Fourth Amendment was not violated because of language in the providers' Terms of Service.

The Minnesota Court of Appeals' ruling in *State v. Pauli*[49] is a helpful example. Pauli used a Dropbox account to remotely store files, including, as it turned out, a significant collection of CSAM images.[50] Dropbox scanned the files, reported 63 suspected files to NCMEC, and then NCMEC opened two of the files and confirmed they were CSAM.[51] NCMEC then forwarded the images to state investigators, who obtained a warrant to search his home and the rest of his Dropbox account. More CSAM was found, and Pauli admitted he used his Dropbox account to store CSAM.[52]

The state court of appeals ruled that Pauli had no Fourth Amendment rights in his files because Dropbox's "clear and unambiguous terms of service . . . undermined"[53] his reasonable expectation of privacy. "As a precondition to creating an account," the court noted, "Dropbox required Pauli to agree to its terms of service."[54] Dropbox's Terms of Service stated that its users "must not even try to . . . publish or share materials that are unlawfully pornographic or indecent," "violate the law in any way," or "violate the privacy or infringe the rights of others."[55] Further, the Terms "provided that users granted Dropbox permission to access, store, and scan files; that Dropbox could review user conduct for compliance with the terms of service; and that Dropbox could disclose user information to third parties if necessary to comply with its own legal obligations and prevent abuse of its services."[56] By using Dropbox to store CSAM, Pauli had given up his Fourth Amendment rights:

> In this case, the undisputed evidence reflects that Pauli voluntarily stored his child-pornography content with Dropbox despite clear and unambiguous warnings that such content violated Dropbox's policies; that Dropbox could review Pauli's conduct and content for compliance; and that Dropbox could

48 *See, e.g.*, United States v. Miller, 982 F.3d 412, 424 (6th Cir. 2020) ("Google's decision to scan its customers' files is instead like the utility's decision to disconnect its customers' electricity: The 'initiative' to take both actions 'comes from' the private party, not the government."). *See generally* ORIN S. KERR, COMPUTER CRIME LAW 410 (5th ed. 2022) ("Circuit courts have held that the Internet providers [that scan for CSAM images] are private actors.").

49 No. 69DU-CR-17-3210, 2020 WL 7019328 (Minn. Ct. App. Feb. 24, 2021), *aff'd on other grounds*, 979 N.W.2d 39 (Minn. 2022).

50 *Id.* at *1.

51 *Id.*

52 *Id.*

53 *Id.* at *3.

54 *Id.* at *1.

55 *Id.* (quoting Dropbox's Terms of Service).

56 *Id.*

> report his content to law enforcement. Pauli voluntarily turned his information over to a third party subject to clear and unambiguous terms of service that undermined any objectively reasonable expectation of privacy in his Dropbox account content.[57]

According to this reasoning, Pauli violated the breach provisions that then triggered the rules-of-the-road provision, eliminating his reasonable expectation of privacy and extinguishing his Fourth Amendment rights. Granted, the Minnesota Supreme Court ended up affirming on a different ground: it held that Dropbox was a private actor outside the Fourth Amendment without considering the effect of Terms of Service if the Fourth Amendment had applied.[58] But several federal district court cases have adopted similar reasoning as the court of appeals in *Pauli*, taking this approach across a range of providers with various breach and rules-of-the-road provisions.

A quick review is instructive. In *United States v. Sporn*,[59] in 2022, Twitter investigated a Twitter user suspected of using his account to distribute CSAM. Twitter's investigation led to discovery of CSAM and subsequent criminal charges.[60] The court, in denying the motion to suppress, ruled that Sporn "lacked a reasonable expectation of privacy in [his] Twitter account" because Twitter's Terms of Service announced a "zero tolerance policy for child sexual exploitation," informing users that Twitter "reserve[s] the right to access [and] read" account files to detect "abuse and prohibited images."[61]

A similar result was reached in *United States v. Bohannon*,[62] in 2020, involving scanning by Microsoft of folders on OneDrive cloud service using a tool called PhotoDNA. The Terms of Service gave Microsoft the right to access folders if Microsoft believed it was necessary to enforce its Terms of Service, including its prohibition on using OneDrive in a way that "exploits, harms, or threatens to harm children."[63] "That is precisely what happened here," the court reasoned; if Microsoft was a government actor, "its PhotoDNA search was reasonable under the Fourth Amendment."[64]

There are several more similar cases, with essentially identical facts, involving scanning by different providers. They include: Sony and its PlayStation Network, which has broad breach provisions prohibiting using

---

57 *Id.* at *3.

58 *See* State v. Pauli, 979 N.W.2d 39, 52 (Minn. 2022) ("Pauli . . . failed to meet his burden to demonstrate Dropbox was acting as a government agent in searching his files.").

59 No. 21-10016, 2022 WL 656165 (D. Kan. Mar. 4, 2022).

60 *Id.* at *1.

61 *Id.* at *10.

62 506 F. Supp. 3d 907 (N.D. Cal. 2020).

63 *Id.* at 910.

64 *Id.* at 915.

PlayStation for unlawful or harmful acts;[65] America Online (AOL) email messages, which are governed by broad breach and rules-of-the-road provisions prohibiting unlawful acts and granting it discretion to take appropriate action;[66] Yahoo and its instant messenger service, governed by broad breach and rules-of-the-road provisions prohibiting using Yahoo's services for unlawful purposes and authorizing Yahoo to enforce its Terms of Service.[67]

I don't want to overstate the force of these decisions. In each context, reliance on Terms of Service was only one of several ways the court could have resolved the case against the defendant.[68] Courts could have also ruled (and sometimes did rule, as alternative arguments) that the providers were not state actors or that the particular records were not protected.[69] And in some cases, initial decisions based on Terms of Service were later revised, either on rehearing, or else affirmed on a different ground on appeal.[70] So there is a tentativeness to the case law—a sense of courts looking for the best ground to justify a result they would reach another way otherwise. But these caveats aside, there is currently a substantial body of case law accepting the syllogism that Terms of Service control Fourth Amendment rights.

---

65 *See* United States v. Stratton, 229 F. Supp. 3d 1230, 1233 (D. Kan. 2017) (including restrictions on user action that Sony "finds offensive, hateful or vulgar" or that "violate any local, state or federal laws").

66 *See* United States v. Ackerman, 296 F. Supp. 3d 1267, 1269 (D. Kan. 2017) (highlighting AOL Mail's Terms of Service); VanDyck v. United States, 2022 WL 17689168, at *7 (D. Ariz. Dec. 15, 2022) ("In summary, the terms of service expressly precluded use of AOL email to send illegal attachments, which includes child pornography. Petitioner was expressly warned that AOL could 'take any technical, legal, and other actions' that it deemed necessary and appropriate.").

67 *See* United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *25 (W.D.Ky. Aug. 17, 2009) ("Given the Yahoo! Terms of Service, [defendant] cannot meet [his] burden [of establishing a legitimate expectation of privacy]."); *see also* United States v. Bode, No. ELH-12-158, 2013 WL 4501303, at *20 (D. Md. Aug. 21, 2013) (holding that display of Terms of Service on a website's warning banner eliminated Fourth Amendment rights).

68 *See, e.g.*, Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 183 (D. Conn. 2005) (holding that there is no Fourth Amendment protection of basic subscriber information under the third-party doctrine, and further that Terms of Service contemplated disclosure and thus no Fourth Amendment rights were violated even if the records were protected).

69 *See supra* note 48.

70 *See, e.g.*, United States v. Wolfenbarger, No. 16-CR-00519-LHK-1, 2019 WL 4085260, at *12 (N.D. Cal. Aug. 29, 2019) (initially holding that Terms of Service eliminate Fourth Amendment rights), *vacated and superseded by* United States v. Wolfenbarger, No. 16-CR-00519-LHK-1, 2019 WL 6716357, at *11 (N.D. Cal. Dec. 10, 2019) (taking no view on defendant's reasonable expectation of privacy).

C. *Cases Holding That Terms of Service Do Not Determine Fourth Amendment Rights*

Now to the flip side. There is also case law adopting the opposite view, holding that Terms of Service either have little effect on Fourth Amendment rights—or else no effect at all. To these courts, Terms of Service do not control: their language about user rights does not ordinarily alter Fourth Amendment protections. Courts on this side of the divide have often drawn physical analogies, noting that individuals often have Fourth Amendment rights in physical spaces despite having granted rights of access to third parties.

The leading case is the Sixth Circuit's ruling in *United States v. Warshak* ("*Warshak III*").[71] *Warshak III* has been widely cited for holding that the Fourth Amendment requires a warrant to compel the contents of e-mail from an e-mail provider.[72] A lesser-known part of that holding is that the Terms of Service of the Internet provider, NuVox, did not diminish defendants' expectations of privacy.[73] NuVox's Terms of Service stated that "NuVox *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service."[74] According to Judge Boggs, the provider's retention of the right of access "does not diminish the reasonableness of Warshak's trust in the privacy of his emails."[75]

This was so, Judge Boggs reasoned, because providers of previous technologies retained similar rights without apparently eliminating any Fourth Amendment rights. For example, the phone company in *Katz* had a similar right to tap phone calls to protect its service.[76] Yet, that authority had not interfered with Katz's reasonable expectation of privacy.[77] More broadly, it was common for rights holders to retain rights despite the reality of third-party access: a person who rented an apartment or a hotel room did not lose

---

71 631 F.3d 266 (6th Cir. 2010) ("*Warshak III*").

72 *Id.* at 288. For example, the majority opinion and two dissents in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), favorably cited *Warshak III*. *See id.* at 2222 (describing *Warshak III*'s warrant holding as "sensible . . . because it would prevent the subpoena doctrine from overcoming any reasonable expectation of privacy"); *id.* at 2269 (Gorsuch, J., dissenting) (citing *Warshak III* in support of the claim that an e-mail owner "retains a vital and protected legal interest" akin to that of an owner of traditional mail); *see also id.* at 2230 (Kennedy, J., dissenting) (citing *Warshak III* for the proposition that leading precedents "may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party.").

73 *Warshak III* at 286.

74 *Id.* at 287 (quoting NuVox's subscriber agreement).

75 *Id.*

76 *See id.* (citing Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967)) (noting the general access rights telephone companies had at the time *Katz* was decided).

77 *See id.* at 285 (noting that telephone users retained Fourth Amendment rights under *Katz* despite the apparent phone company access to the call).

their rights because the superintendent or a maid might enter.[78] The same was true, Judge Boggs reasoned, for privacy in Internet accounts.

Notably, *Warshak III* did not foreclose the claim that Terms of Service might be relevant in some cases. In an earlier round of the *Warshak* litigation, *Warshak II*, the *en banc* Sixth Circuit had rejected a facial Fourth Amendment challenge to accessing e-mails without a warrant in part on the grounds that Terms of Service might alter Fourth Amendment rights.[79] Such Terms were "moving parts," Judge Sutton speculated, that "could cast doubt on the validity of" compelling the contents of e-mails without a warrant "in a given case; others might not."[80] Given that uncertainty, it was "[b]etter . . . to decide the validity of" compelling the contents of e-mails without a warrant "in the context of a specific internet-service agreement and a specific search and seizure"[81] rather than in a facial challenge.

In *Warshak III,* citing the en banc court's discussion in *Warshak II*, Judge Boggs left open the possibility that some Terms of Service might alter Fourth Amendment rights: "[A] subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account."[82] In the ordinary case, however, such as in *Warshak III*, the Terms of Service did not affect Fourth Amendment rights. "[W]e doubt that will be the case in most situations," Judge Boggs cautioned, "and it is certainly not the case here."[83]

A few federal district courts have agreed with *Warshak III* that Terms of Service have modest or even no effect on Fourth Amendment rights. In *United States v. Irving*,[84] a warrant was obtained to search Irving's Facebook account for evidence that he had violated a state sex offender registry statute. Executing the warrant revealed CSAM in the account, and criminal charges followed.[85] When Irving filed a motion to suppress, the government contended that Irving had no standing to challenge the search of his account—that is, he lacked a reasonable expectation of privacy in its contents[86]—because of Facebook's Terms of Service.

---

78 *Id.* (citing United States v. Allen, 106 F.3d 695, 699 (6th Cir.1997) (hotel guests) and United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009) (tenants)).

79 Warshak v. United States, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) (Sutton, J.) ("*Warshak II*").

80 *Id.*

81 *Id.*

82 *Warshak III*, 631 F.3d at 286.

83 *Id.*

84 347 F. Supp. 3d 615 (D. Kan. 2018).

85 *Id.* 619.

86 *Id.* at 619-20. Under *Rakas v. Illinois*, 439 U.S. 128, 139 (1978), a Fourth Amendment "standing" inquiry merely asks whether the search implicated the movant's reasonable expectation of privacy.

The government's argument in *Irving* relied on two different types of Terms. First, Irving had violated a breach provision: because Irving was a convicted sex offender, his use violated Facebook's Terms of Service rule that convicted sex offenders could not use Facebook.[87] Second, Facebook's Terms of Service contained broad Terms giving Facebook the right to handle data. In the government's view, these rules-of-the-road provisions collectively meant that one who used Facebook did so "at one's peril."[88]

The *Irving* court disagreed, holding that the defendant had established a reasonable expectation of privacy in his account and therefore had standing to challenge the search.[89] Part of the reasoning was based on the details of how Facebook's Terms were written. The Terms did not explicitly eliminate user rights and gave users certain rights to their data.[90]

Part of the reasoning was broader, however. Although Facebook could have terminated Irving's account for violating the breach provision, it had not actually done so: "Facebook . . . allowed Defendant to have an account on Facebook and he remained on Facebook at the time of the search (and after the search)."[91] Indeed, Facebook had not known that Irving had violated the Terms.[92] Accordingly, Irving remained an authorized user. The court offered a physical analogy: "In the same way that an individual who is a smoker may falsely represent to a landlord that he is not a smoker to obtain an apartment lease, that individual does not lose all expectation of privacy in the rented apartment."[93]

The district court's ruling in *United States v. DiTomasso*[94] takes a more mixed approach. *DiTomasso* was a CSAM scanning case in which AOL and a chat messaging provider called Omegle scanned messages sent to DiTomasso's account and found CSAM.[95] The government argued that the

---

87 *Irving*, 347 F. Supp. 3d at 620.

88 *Id.* at 621.

89 *Id.* at 623.

90 *Id.* at 623. The *Irving* court explained that

> Facebook's TOS does not have explicit terms about monitoring user's accounts for illegal activities and reporting those activities to law enforcement. Instead, Facebook's TOS generally states that Facebook can collect data and information. It also states, however, that the user owns all of the content and information and can control how to share it. Although Facebook's TOS does state that a user should not post content that is pornographic or unlawful, it makes these statements in the context of safety and in asking for the user's help "to keep Facebook safe."

Id. at 623.

91 *Id.* at 620.

92 *See id.* at 623 ("Indeed, at the time the government sought the search warrant, there was no indication that Defendant had violated Facebook's TOS.")

93 *Id.* at 620-21.

94 56 F. Supp. 3d 584 (S.D.N.Y. 2014), *aff'd on different grounds*, 932 F.3d 58 (2d Cir. 2019).

95 *Id.* at 586.

Terms of Service of both AOL and Omegle gave users notice of monitoring. AOL "reserved the right to . . . disclose[] the content of [user] communications to law enforcement"[96] if they used accounts "for illegal activities,"[97] and Omegle informed users that it had a scanning program and could "share [the results] with third parties, including law enforcement."[98] According to the government, DiTomasso could have no reasonable expectation of privacy against the monitoring that occurred, and even if he did, he consented to the searches.[99]

The district judge, Judge Shira Scheindlin, handed down a mixed ruling. On one hand, the Terms of Service did not eliminate DiTomasso's reasonable expectation of privacy. According to Judge Scheindlin, the government's argument failed because "it would subvert the purpose of the Fourth Amendment to understand its privacy guarantee as 'waivable'" in a world in which "the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms."[100]

Echoing both *Warshak III* and the reasoning of *Irving*, Judge Scheindlin based this intuition on analogies to physical space: "[W]hen employees constructively consent to searches by their supervisors, it does not automatically follow that they also consent to searches by law enforcement."[101] The same was true for hotel guests: "[I]t is well-established that granting hotel management access to one's room for limited purposes—for example, in case of emergency, or for housekeeping—neither vitiates one's expectation of privacy in the room nor authorizes hotel employees to consent to a search by the government on behalf of the guest."[102] The same should be true, Judge Scheindlin reasoned, with Internet accounts.[103]

But this victory was short-lived. After holding that violations of the Terms of Service did not eliminate a reasonable expectation of privacy, Judge Scheindlin ruled that using an Internet service amounted to consent to a law enforcement search if the Terms sufficiently put a user on notice that the provider might cooperate with law enforcement.[104] According to Judge Scheindlin, AOL's Terms were sufficiently clear about this possibility while Omegle's Terms were not: "In contrast to Omegle's policy, which includes only a passing reference to law enforcement—and which gives no indication

96 *Id.* at 592.
97 *Id.*
98 *Id.*
99 *Id.*
100 *Id.*
101 *Id.* at 593.
102 *Id.*
103 *Id.*
104 *Id.* at 597.

of the role Omegle intends to play in criminal investigations—AOL's policy makes clear that AOL intends to actively assist law enforcement"[105] in the event a user commits a crime using an account. Thus, using AOL amounted to consent to government monitoring, while using Omegle did not.[106]

There are other cases in the *Warshak III* vein.[107] While the first set of cases links Terms of Service and Fourth Amendment rights, the latter set of cases delinks them. Neither set offers a particular grounding in its conclusion. Both seem to proceed more by instinct than extended reasoning. But the lower court case law on the relationship between Fourth Amendment rights and Terms of Service is, in short, a mess. Courts cannot agree on the relationship, with different courts offering different answers.

II. TERMS OF SERVICE AND EXPECTATIONS OF PRIVACY

This part explains how courts should resolve the disagreement. It focuses on the basic question of whether Terms of Service can eliminate a reasonable expectation of privacy, making conduct that would be a Fourth Amendment search in the absence of Terms into an act that does not trigger the Fourth Amendment at all. The answer, it argues, is a resounding "no." Terms of Service have little or no effect on expectations of privacy because they are private contracts rather than agreements with the government. Private contracts over shared spaces cannot eliminate Fourth Amendment expectations of privacy.

From this perspective, Terms of Service are the latest in a long line of owner–user agreements: arrangements in which a property owner gives a person rights to use property subject to contractual limits imposed by the owner to protect the owner's interests. Case law on rental car contracts, apartment leases, and hotel rooms have held that violating analogous contractual Terms in owner–user agreements do not eliminate expectations of privacy. The same principle should be applied to Terms of Service.

How did so many courts get this wrong? The courts that have wrongly followed the syllogism and given Terms significant effect have made a basic category mistake. They looked to case law on the rights of government employees in government workplaces, where employer-imposed policies purporting to eliminate privacy rights have that effect. That line of cases

105 *Id.*

106 *Id.*, *see also* United States v. DiTomasso, 932 F.3d 58, 68 (2d Cir. 2019) (resolving the question on appeal on the ground that Omegle's status as a private actor rendered any monitoring it did "beyond the reach of the Fourth Amendment.").

107 *See, e.g.*, People v. Pierre, 51 Misc. 3d 1035 (N.Y. Sup. Ct. 2016) (concluding that Terms of Service did not alter Fourth Amendment rights).

should not apply to Terms of Service imposed by private companies, which are contracts with private companies and not the government.

This part makes that argument in four steps. It begins with Fourth Amendment rights in shared spaces, and it next considers the role of formalizing relationships through contract. It then turns to case law on owner–user agreements such as rental cars contracts, apartment leases, and hotel rental agreements. It concludes by explaining why cases giving effect to government workplace policies are inapplicable.

A. *Fourth Amendment Rights in Shared Space*

At the most fundamental level, Fourth Amendment law divides the world into government actors and private actors. Fourth Amendment rights are rights that private actors have against the government.[108] When a government actor wants to search a private space of a private actor, the government first needs a warrant or an exception to the warrant requirement to make the search reasonable and therefore legal.[109]

Now add a wrinkle: other people. In theory, a person might live alone, in a house owned in fee simple, where they let no one else inside. But it's more common for us to share our spaces with other people. We might live with family members. We might have a roommate. Even those who live alone usually let occasional guests enter. And it's common for people to have private spaces they don't actually own, in which their relationships are governed by contracts between the owner and themselves as renters. For example, many people lease their apartments. They might also rent temporary storage spaces. On a trip, they might rent out an Airbnb or a hotel room. In all of these cases, a person has rights in protected spaces that are shared with other private parties.

How does the Fourth Amendment treat this shared space? Sharing space ordinarily does not alter Fourth Amendment protection. The government needs a warrant to search your home if you have roommates, just like it needs a warrant to search your home if you live alone.[110] The government needs a warrant to search your house if you are renter, just like it does if you are an owner.[111] Sharing space with someone does not alter the basic dynamic of a

---

108 *See* Hiibel v. Sixth Jud. Dist. Court of Nev., 542 U.S. 177, 187 (2004) ("[T]he Fourth Amendment does not impose obligations on the citizen but instead provides rights against the government.").

109 *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

110 See *infra* notes 112–24 and accompanying text for a discussion of searches in shared spaces.

111 Even just being an overnight guest is sufficient to have standing that establishes Fourth Amendment protections. *See* Minnesota v. Olson, 495 U.S. 91, 96-97 (1990) ("Olson's status as an

search. The government is still entering a private space. The government still needs a warrant or an exception to the warrant requirement.

The Supreme Court's decision in *Mancusi v. DeForte*[112] is the leading case on this question. State officials searched a local union office looking for evidence that a union employee, DeForte, was engaged in corruption. The officials lacked a warrant, but they claimed it was not necessary to have one.[113] This was so, the police argued, because DeForte's office consisted of "one large room, which he shared with several other union officials."[114] When DeForte later challenged the search, the Supreme Court concluded that DeForte's Fourth Amendment rights were "not fundamentally changed because" he had "shared an office with other union officers"[115]:

> DeForte still could reasonably have expected that only those persons and their personal or business guests would enter the office, and that records would not be touched except with their permission or that of union higher-ups. This expectation was inevitably defeated by the entrance of state officials, their conduct of a general search, and their removal of records which were in DeForte's custody.[116]

Under *Mancusi v. DeForte*, sharing space has no direct relevance to Fourth Amendment rights.

Why is that? The Supreme Court has not explained the point in detail. But the reason is fundamental: Fourth Amendment rights are against the government.[117] To establish Fourth Amendment rights against searches, a person must have a reasonable expectation of privacy or some kind of property right in the place or thing searched.[118] A reasonable expectation of

---

overnight guest is alone enough to show that he had an expectation of privacy in the home that society is prepared to recognize as reasonable.").

112 392 U.S. 364 (1968).

113 *See id.* at 368.

114 *Id.*

115 *Id.* at 369.

116 *Id.*

117 *See* United States v. Irving, 347 F. Supp. 3d 615 (D. Kan. 2018).

118 Under *United States v. Jones*, 565 U.S. 400 (2012), the Court has recognized a physical property theory of Fourth Amendment searches that provides an alternate means of identifying a search. Its scope remains unclear, however. *Jones* described the test in two ways, as being based on trespass and physical intrusion. *Compare id.* at 406 (trespass), *with id.* at 404-05 (physical intrusion). A year later, the majority in *Florida v. Jardines*, 569 U.S. 1 (2013) applied *Jones* but referred only to "physical intrusion" and never mentioned trespass. *Id.* at 5. If the test is physical intrusion, then access to protected Internet records will be evaluated only under *Katz* and not under *Jones* because there is no physical intrusion. On the other hand, Justice Gorsuch has suggested that the *Jones*/*Jardines* approach could be applied more broadly to access to Internet records despite the absence of physical intrusion. *See* Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting) ("Under this more traditional [property-based] approach, Fourth Amendment

privacy is an expectation of privacy against government intrusion, not against private party observation.[119] The fundamental question is whether a person has a sufficient relationship with a protected space or information that the space or information is *theirs*,[120] and thus, when concealed from outside view, is protected against government intrusion.

It is true, of course, that sharing space creates risks that a co-occupant will share that information with the government.[121] Your roommate can consent to a search of areas of common authority.[122] And if you tell your roommate a secret, the government can ask your roommate what you shared.[123] These caveats are addressed in Part III. But for now, the key is that sharing access to a space does not eliminate your rights to a space. As long as your sharing stops short of opening the space to the general public, you retain rights in your shared space.[124]

B. *Does Formalizing the Sharing Arrangement Matter?*

Terms of Service involve more than just sharing, of course. Unlike informal sharing arrangements, Terms of Service formalize the relationship between computer network owner and computer network user. When we share space, formalization is uncommon. If you pick someone as a roommate, you won't specify in writing what music can be played in your apartment, or who has to take out the trash on Wednesdays, or who can enter the other's room or what remedies are permitted if rules are not followed. Such things are left to norms, or informal agreements, rather than to contract. Terms of Service are different. They write down, in glorious detail, the terms by which the provider is sharing its service with you the user.

The key question is, does formalizing the agreement make a difference? It seems intuitive that the answer is no. Formalizing the relationship between

---

protections for your papers and effects do not automatically disappear just because you share them with third parties.").

119 *See Hiibel vs. Sixth Jud. Dist. Ct. of Nev.*, 542 U.S. 177, 187 (2004) ("[T]he Fourth Amendment does not impose obligations on the citizen but instead provides rights against the government.").

120 *See* Byrd v. United States, 138 S. Ct. 1518, 1531 (2018) (Thomas, J., concurring) (emphasizing that the key issue was whether the petitioner could demonstrate that the rental car in question was "*his* effect").

121 *See infra* Part III for a discussion of the conditions under which otherwise-established Fourth Amendment rights can be forfeited in shared spaces.

122 *See infra* notes 218–19.

123 *See* Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no Fourth Amendment violation where person "was not relying on the security of" a protected space, but instead "was relying upon his misplaced confidence that [a communicant] would not reveal his wrongdoing").

124 *See* Maryland v. Macon, 472 U.S. 463, 469 (1985) ("[A person does] not have any reasonable expectation of privacy in areas . . . where the public was invited to enter and to transact business.").

owner and user may clarify that relationship. But express articulation should not itself alter it.

To see this, imagine two roommates share an apartment. Say they are friends who will be going to law school in the fall. In the summer before law school, they maintain a general custom that each is free to go into the bedroom of the other. They never talk about it; they just do it. Now imagine fall arrives and law school starts. Being law students, the two decide to put their agreement in writing. They might (heck, probably would) express their relationship in legalese. "I henceforth agree," they might write, "that I have no reasonable expectation of privacy against your access to my room." Or perhaps: "I hereby waive all rights, express and implied, of whatever source, to prohibit your presence in my room." What does the legal-sounding language add? Nothing, I think. Yes, it formalizes an informal agreement. But that alone does not change a person's rights.

And it turns out that this is not a new question. Contracts over space sharing are common in the context of what we might call *owner–user agreements*. Businesses often own property that they rent out to customers to use. The owner requires, as a condition of using the property, that the customer must agree to a contract drafted by the company's lawyers. In these owner–user agreements, the terms will cover what the user can and cannot do with the owner's property. It will also typically explain the owner's policies with respect to various aspects of the customer's use.

Terms of Service are a new kind of owner–user agreement. But others have been around for a long time. For example, anyone who has rented an apartment has signed a lease. The lease agreement agrees to give the customer use of the apartment, subject to various conditions, and the user agrees to rent the apartment in exchange for rental payments. Anyone who has rented a car has had to sign a rental agreement specifying the respective rights and powers of owner and renter of the car. Anyone who has rented a hotel room has encountered the same basic contract. It sets out the terms of access to the hotel rooms, and you agree to them when you agree to rent the room.

C. *The Effect of Owner–User Agreements on Car Rentals, Apartment Leases, and Hotel Rentals*

Case law on other owner–user agreements, such as rental car contracts, apartment leases, and hotel rental agreements, demonstrates that owner–user agreements have little or no effect on Fourth Amendment rights. Violating an owner–user agreement does not eliminate Fourth Amendment rights. Contractual rights between private parties are usually irrelevant to Fourth Amendment rights, and it is only in some specific cases where the terms of owner–user agreements can impact them.

The Supreme Court's recent decision on rental car contracts, *Byrd v. United States*,[125] is a natural starting point. Byrd was driving a rental car when he was stopped and the car was searched, yielding 49 bricks of heroin.[126] When Byrd moved to suppress the evidence, the trial court ruled that he had no standing to challenge the search because his name was not listed on the rental car contract as a valid driver.[127] In Fourth Amendment law, standing is the requirement that the defendant's own Fourth Amendment rights are at stake.[128] In other words, did *he* have a reasonable expectation of privacy? This was an issue in *Byrd* because the car had been rented by one Reed, who had then given the car to Byrd.[129] And critically, allowing Byrd to drive the car was in violation of the contract Reed had signed.

Specifically, an initialized addendum to the contract stated that "the only ones permitted to drive the vehicle other than the renter are the renter's spouse, the renter's co-employee (with the renter's permission, while on company business), or a person who appears at the time of the rental and signs an Additional Driver Form."[130] The contract drove home the point in all caps, which (with apologies for shouting) stated the following: "PERMITTING AN UNAUTHORIZED DRIVER TO OPERATE THE VEHICLE IS A VIOLATION OF THE RENTAL AGREEMENT."[131] For the district court, and then the court of appeals, the language in the rental agreement was controlling.[132] Byrd could not have any Fourth Amendment rights in the car because he was not an authorized driver under the contract.[133]

But the Supreme Court reversed.[134] "As anyone who has rented a car knows," Justice Kennedy began,

> car-rental agreements are filled with long lists of restrictions. Examples include prohibitions on driving the car on unpaved roads or driving while using a handheld cellphone. Few would contend that violating provisions like these has anything to do with a driver's reasonable expectation of privacy in the rental car—as even the Government agrees.[135]

---

125 138 S. Ct. 1518 (2018).

126 *Id.* at 1525.

127 *Id.*

128 *See id.* at 1530.

129 *Id.* at 1524.

130 *Id.* (quoting addendum to rental car contract).

131 *Id.*

132 *Id.* at 1525.

133 *See id.* at 1525 (citing United States v. Byrd, No. 14-CR-321, 2015 WL 5038455, at *2 (M.D. Pa. Aug. 26, 2015)).

134 *Id.* at 1531.

135 *Id.* at 1529.

The same was true, Justice Kennedy explained, of contractual terms on who was an unauthorized driver. Even assuming that the contact could be read to be void if an unauthorized driver took the wheel, "the Government fail[ed] to explain what bearing this breach of contract, standing alone, has on expectations of privacy in the car."[136]

The problem with the government's argument was a fundamental mismatch between the nature of Fourth Amendment rights and purpose of rental car contracts. Establishing a reasonable expectation of privacy in the car required showing "lawful possession and control and the attendant right to exclude."[137] In contrast, rental contract terms merely "concern[ed] risk allocation between private parties"[138] if something went amiss. The two inquiries were fundamentally different: "that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car."[139] The Court then remanded to the lower courts for consideration of whether Byrd had that lawful possession and control over the car.[140]

Lower court case law on apartment leases has reached a similar conclusion.[141] The often-cited case of *United States v. Washington*[142] is illuminating. Following the arrest of George Young, the police searched Young's apartment without a warrant and found Young's nephew Washington with drugs and a loaded gun.[143] When charges followed, the government argued that Washington lacked standing to challenge the search—that is, he lacked a reasonable expectation of privacy—because his stay was in violation of the lease terms.

The government focused on three violations of the lease that, in its view, ensured that Washington had no reasonable expectation of privacy in the apartment. First, Young's apartment lease "barred multiple occupants,"[144] which the government claimed did not allow Washington's presence. Second, the lease prohibited tenants from using their apartments "for illegal

136 *Id.*

137 *Id.* at 1528.

138 *Id.* at 1529.

139 *Id.*

140 *Id.* at 1530.

141 *See, e.g.*, *State v. Jacques*, 210 A.3d 533, 542 (Conn. 2019) ("[T]he failure to pay rent, on its own, does not result in the loss of one's expectation of privacy."); *United States v. McClendon*, 86 F. App'x 92, 95-96 (6th Cir. 2004) ("While the arrangement may have violated [the defendant's] rental agreement with the housing authority, the Government has cited no authority for the proposition that such a violation renders McClendon's expectation of privacy in his bedroom unreasonable.").

142 573 F.3d 279 (6th Cir. 2009).

143 *Id.* at 281-82.

144 *Id.* at 284.

activity,"[145] such as Washington's drug dealing. Third, there was evidence that the rent had not been paid, as the lease required.[146] In the government's view, the contract rights governed and Washington could not have standing.[147]

The Sixth Circuit disagreed.[148] According to Judge Boggs, "the very premise of the government's argument" was "flawed."[149] "The landlord's mere authority to evict a person" based on a violation of the lease, Judge Boggs reasoned, "cannot of itself deprive that person of an objectively reasonable expectation of privacy."[150] To lose standing, the landlord had to actually evict the tenant from the apartment.[151] The lease violation alone wasn't enough, as "the landlord's failure to evict an occupant who is in technical violation of the lease effectively waives whatever authority the landlord has to treat a person as a trespasser."[152] The lease violation gave the landlord legal authority to seek eviction. But by failing to invoke that legal authority, the landlord did not end the period of lawful possession under landlord-tenant law or the Fourth Amendment.[153]

The *Washington* court bolstered the point by noting "the intolerable implications"[154] of the government's position. Violating lease terms by paying late "is a common occurrence, especially in economically turbulent times."[155] If the lease controlled, and "a landlord's unexercised authority over a lodging with overdue rent alone divested any occupant of a reasonable expectation of privacy, millions of tenants and their guests would be deprived of Fourth Amendment protection."[156] This was too much for the court to take: "[W]e reject the notion that the Constitution ceases to apply in these circumstances."[157]

Judge Easterbrook's recent opinion for the Seventh Circuit in *United States v. Thomas* echoes the point.[158] Thomas was a meth dealer with warrants out for his arrest.[159] In an effort to avoid the authorities, Thomas used a fake ID—

145 *Id.*
146 *Id.*
147 *Id.*
148 *Id.* at 284-86.
149 *Id.* at 284.
150 *Id.*
151 *Id.*
152 *Id.* (citing 49 AM. JUR. 2D Landlord and Tenant § 260 (2009); and then citing 52 C.J.S. *Landlord & Tenant* § 185 (2009)).
153 *See id.* at 285-86.
154 *Id.* at 284.
155 *Id.* at 285.
156 *Id.* at 284-85.
157 *Id.* at 285.
158 65 F.4th 922 (7th Cir. 2023).
159 *Id.* at 923.

a driver's license in the name Frieson Alredius—to rent an apartment.[160] After federal authorities arrested Thomas outside his building, they spoke with his landlord and learned that he had rented the apartment using the Alredius identity instead of his real identity. Agents then searched the apartment with the landlord's consent but without a warrant, finding drugs and drug paraphernalia.[161] In defending the warrantless search of Thomas's apartment, the government argued that Thomas had no reasonable expectation of privacy in the apartment because he had obtained the lease in violation of state laws banning the use of fake IDs.[162]

The Seventh Circuit disagreed. First, echoing *Washington*, Judge Easterbrook explained that eliminating an expectation of privacy in a home requires a landlord to secure an eviction order, not merely identify a lease violation.[163] Second, violating the law to get the lease does not end a person's rights in the apartment in the way that a burglar would lack rights in a house he entered, or a person would lack rights in stolen property. The doctrine "does not extend so far," Judge Easterbrook contended, that it would eliminate an expectation of privacy for a person who pays for an apartment using drug proceeds or signs a lease while intending not to pay, despite the criminal means of obtaining the lease.[164]

Case law on Fourth Amendment rights in hotel rooms is largely in accord. Violating the rental agreement does not itself eliminate Fourth Amendment rights; actual dispossession from the room for the violation is needed. A perhaps-extreme example is *United States v. Cunag*, in which the defendant rented a hotel room under false pretenses.[165] Cunag gave the hotel a fake name and fake phone number; paid for the room with the credit card of a dead woman; and showed the hotel a fake ID that had a stranger's picture and the dead woman's name on it.[166] The hotel initially gave Cunag a room, but later realized what had happened, locked him out, and filed a police report.[167] Cunag nonetheless managed to get into the room, and the hotel staff brought

160 *Id.*

161 *Id.* at 923-24.

162 *Id.* at 923. According to the Court, Thomas violated two statutory sections: GA. CODE ANN. § 16-9-4(b)(1) (2023), which in relevant part prohibits using a fake ID, and GA. CODE ANN. § 16-9-121(a)(4) (2023), which prohibits using a fake ID to further a fraud or other crime.

163 *See Thomas*, 65 F.4th at 924 ("[H]ow she was entitled to protect this interest bears on the reasonableness of Thomas's expectation of privacy. The landlord could have sought to terminate Thomas's lease because of his deception . . . . There is a difference, however, between bringing eviction proceedings against a fraudulent (or felonious) tenant and inviting the police to search his residence." (emphasis omitted) (citations omitted)).

164 *Id.* at 925.

165 386 F.3d 888, 889 (9th Cir. 2004).

166 *Id.*

167 *Id.* at 890.

the police to the room to eject him; when they opened the door, they realized Cunag was inside actively doing drugs.[168]

The Ninth Circuit ruled that, by the time the drugs were discovered, Cunag had lost his expectation of privacy in the room: the hotel "took justifiable affirmative steps to repossess [the] room . . . and to assert dominion and control over it when they discovered and confirmed that Cunag had procured occupancy by criminal fraud and deceit."[169] But the court was careful to note that obtaining the room by fraud, in violation of the rental agreement, was itself not enough to lose Fourth Amendment rights. In the Ninth Circuit, "even if the occupant of a hotel room has procured that room by fraud, the occupant's protected Fourth Amendment expectation of privacy is not finally extinguished until the hotel justifiably takes 'affirmative steps to repossess the room.'"[170] The hotel's affirmative steps to repossess the room eliminated privacy rights; violation of the contract alone did not.[171]

What's the upshot of this case law? The role of owner–user agreements is not a new question for Fourth Amendment law. Violations of those agreements do not eliminate Fourth Amendment rights. In the Supreme Court's words, from *Byrd*, whether such contracts "between private parties" are violated "has little to do with" Fourth Amendment rights if an individual "otherwise has lawful possession."[172] Those contracts may set in motion acts that then impact such rights, such as eviction from an apartment or a hotel room. But the "very premise" that such private agreements control Fourth Amendment rights is "flawed," as the Sixth Circuit put it in *Washington*: rights allocation among private parties presents a very different question than rights against government action.

D. *The Special Case of Government Spaces and Government Policies*

If my argument is right, many courts have misunderstood the Fourth Amendment implications of Terms of Service. How could they have made that mistake? Courts mistook a special case for the general rule. Seeking precedents on the role of contract in Fourth Amendment rights, they found case law from the special case of shared *government* spaces—the one context where agreements *do* define Fourth Amendment rights—and applied it uncritically to the different setting of private contracts. When that overlooked limit is appreciated, it becomes clear that the cases linking Terms of Service and Fourth Amendment rights are based on a straightforward error.

---

168 *Id.*

169 *Id.* at 895.

170 *Id.* (quoting *United States v. Dorais*, 241 F.3d 1124, 1128 (9th Cir. 2001)).

171 *Id.*

172 *Byrd*, 138 S. Ct. at 1529.

To appreciate this mistake, we need to understand the Supreme Court's ruling on government workplace privacy in *O'Connor v. Ortega*.[173] As part of a sexual harassment investigation at a state government hospital, a physician's hospital office was thoroughly searched. The physician, Dr. Ortega, later sued, leading to an eventual ruling on how the Fourth Amendment applied to a government workplace. The four-Justice plurality opinion, by Justice O'Connor, opted for a middle ground: public employees could have some Fourth Amendment rights, but they were different from rights in private offices.[174]

The plurality's reasoning in *Ortega* is not a model of clarity. But read carefully, the thinking goes like this. In a government office, the employer is a government actor. A reasonable expectation of privacy against government intrusions therefore depends on the employer's practices and policies. While a private employee has a reasonable expectation of privacy in their office against the government generally, as in *Mancusi v. DeForte*,[175] the Fourth Amendment rights of government employees depend on "operational realities of the workplace" and "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[176]

Note the critical difference. In a private sector office, sharing space does not affect Fourth Amendment rights unless the space is open to the public. That's *Mancusi*. But in a government setting, sharing space with others eliminates rights. The question becomes: how often is the workplace actually entered by others, or what rules are in place to permit that entry?[177] Justice Scalia, concurring in the judgment, protested that the reasonable expectation of privacy test should apply the same way regardless of whether the office is run by the government or the private sector.[178] But the premise of the *Ortega* plurality opinion is that government workplace privacy is critically different. The employer's practices and policies control.

Indeed, lower courts have read the *Ortega* plurality's statement about "legitimate regulation" reducing Fourth Amendment rights as imposing a simple binding rule: government workplace privacy polices control Fourth

---

173 480 U.S. 709 (1987).

174 *Id.* at 717-18 (O'Connor, J., plurality opinion).

175 *See* 392 U.S. 364, 369 (1968) ("[The defendant] still could reasonably have expected that only [union colleagues] and their personal or business guests would enter the office . . . This expectation was inevitably defeated by the entrance of state officials . . . .").

176 *Ortega*, 480 U.S. at 717 (O'Connor, J., plurality opinion).

177 *Id.* at 717-18.

178 *Id.* at 730-31 (Scalia, J., concurring in the judgment) ("There is no reason why this determination that a legitimate expectation of privacy exists should be affected by the fact that the government, rather than a private entity, is the employer.").

Amendment rights in the government workplace.[179] You just read the policy. If a public employer announces a policy that its employees have no rights, then the words of that policy control. All Fourth Amendment rights in the government workplace evaporate.[180]

This rule has been widely applied to government employee rights in workplace computers. For example, in *United States v. Thorn*, the defendant worked at an agency of the Missouri Department of Social Services ("DSS").[181] The office had a policy governing privacy in the government's computers at work: "Employees *do not* have any personal privacy rights regarding their use of DSS information systems and technology."[182] It elaborated: "An employee's *use* of DSS information systems and technology indicates that the employee understands and *consents* to DSS'[s] right to inspect and audit all such use as described in this policy."[183] Thorn's workplace computer was searched and CSAM was found.[184] Applying the *Ortega* plurality opinion, and citing a long list of similar government workplace cases, the Eighth Circuit readily concluded that the policy was binding: "In light of the express limits placed upon his computer use by the agency's computer-use policy, the District Court correctly determined that Thorn had no legitimate expectation of privacy in the contents of his office computer."[185]

It is easy enough to miss that the *Ortega* rule is limited to the government employment context. Courts occasionally miss this, citing *Ortega* and its progeny in cases involving private workplace settings.[186] The mistake has also led to at least one revised opinion on panel rehearing, when a court initially misapplied the *Ortega* rule to private employment and held that a workplace policy eliminated a reasonable expectation of privacy; and later handed down a new opinion holding that, despite the workplace policy, the employee had a reasonable expectation of privacy under *Mancusi v. DeForte*.[187]

---

179 *See, e.g.*, *City of Ontario v. Quon*, 560 U.S. 746, 756-57 (2010). Whether the plurality or concurring opinion is binding has not been resolved by the Supreme Court, however. *See, e.g.*, *id.* ("It is not necessary to resolve whether [the] premise [that the *O'Connor* plurality controls] is correct.").

180 *See infra* notes 181–85 and accompanying text.

181 375 F.3d 679, 681-82 (8th Cir. 2004).

182 *Id.* at 682.

183 *Id.*

184 *Id.* at 681.

185 *Id.* at 683 (citing United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002); then citing *United States v. Simons*, 206 F.3d 392, 398 (4th Cir.2000); then citing *United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir.); and then citing *Leventhal v. Knapek*, 266 F.3d 64, 73-74 (2d Cir.2001)).

186 *See, e.g.*, *Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002) (citing *Ortega*, and cases citing *Ortega*, in a discussion of an office at a private electronics company).

187 *See* United States v. Ziegler, 456 F.3d 1138, 1143-46 (9th Cir. 2006) (initially ruling that a private sector workplace policy eliminated a reasonable expectation of privacy under a case relying on *Ortega*), *withdrawn on panel rehearing*, United States v. Ziegler, 474 F.3d 1184, 1189-90 (9th Cir.

The doctrinal distinction is subtle at first, so the confusion is understandable. But there is a right and a wrong answer here. The *Ortega* rule applies to government space, as an employer policy in that context is imposed by the government against a citizen. But it does not apply in private sector spaces, as a policy imposed by a private actor not regulated by the Fourth Amendment does not have the same effect.

Why is this distinction important? The cases linking Terms of Service to Fourth Amendment rights—the case law explored in Section I.B.—trace back their reasoning to this error. If you follow the authorities back, the precedential basis of those cases generally derives from erroneous reliance on public sector environments that applied the special *Ortega* rule. At some point, some court missed the government workplace limit, uncritically applied the government workplace rule to the private sector, and then wrongly concluded that workplace policies generally control Fourth Amendment rights.

A brief example of how this happened may be useful. Take the Seventh Circuit's 2019 decision in *United States v. Adkinson*,[188] which was in turn relied on by the Pennsylvania Supreme Court's 2021 ruling in *Commonwealth v. Dunkins*.[189] *Adkinson* justified its holding that the defendant's Terms of Service had extinguished his Fourth Amendment rights by noting that "[a] defendant can voluntarily consent in advance to a search as a condition of receiving contracted services."[190] The court cited *Medlock v. Trustees of Indiana Univ.* in support of this proposition.[191] But a reading of *Medlock* reveals it to be a public university case involving inspection policies at a state college dormitory.[192] It is a case about consenting to a government search, not a case about private contracts.[193]

The CSAM scanning cases show the same dynamic. The more recent cases cite the earlier cases, and the earlier cases rested on public employment cases applying the Ortega rule. Consider the widely cited case of *United States v. Stratton*, from 2017, which involved the Terms of Service of Sony PlayStation devices.[194] *Stratton* relied on case law about a public university professor whose workplace account was monitored, which monitoring was deemed

2007) (ruling, in the same case, that the workplace policy did not eliminate a reasonable expectation of privacy because private-sector workplace policies are governed by *Mancusi*).

188 916 F.3d 605 (7th Cir. 2019).

189 263 A.3d 247, 264 (Pa. 2021) (T]he plain language of [the workplace] policy and Dunkins' . . . acquiescence in that policy[] resulted in a clear waiver of any expectations of privacy that Dunkins had . . . ." (citing *Adkinson*, 916 F.3d at 631)).

190 *Adkinson*, 916 F.3d at 610.

191 *Id.*

192 *See Medlock v. Trustees of Indiana Univ.*, 738 F.3d 867, 872 (7th Cir. 2013).

193 *Id.*

194 229 F. Supp. 3d 1230, 1233 (D. Kan. 2017).

lawful under *Ortega*.[195] The same is true of *United States v. Bode*,[196] from 2013, which relied on public employment cases applying *Ortega* to say that violating the Terms of Service of a messaging system had eliminated a user's Fourth Amendment rights.[197] Many recent cases such as *Pauli* rely on *United States v. Ackerman*,[198] which in turn relied on *United States v. Wilson*.[199] When you read *Wilson*, it turns out to cite and rely on the same government network cases.[200] The same is true of other CSAM scanning cases with similar holdings: most either rely on government workplace cases based on *Ortega* or rely on other cases that did so.[201] The shaky doctrinal edifice rests on misapplications of the government-only special rule of *Ortega*.[202]

III. Terms of Service and Rights-Losing Doctrines

If Terms of Service don't alter reasonable expectations of privacy, do they have any Fourth Amendment effect at all? This part considers other ways that

---

195 *Id.* at 1241-42 (discussing *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002)).

196 No. ELH–12–158, 2013 WL 4501303, at *16 (D. Md. Aug. 21, 2013) ("[M]uch if not all of the case law [cited here] which has recognized the possibility of a reasonable expectation of privacy in email, has also recognized that whether a user has a reasonable expectation of privacy in an electronic communication[] stored or transmitted by a third-party service can be affected by the terms of service at issue.").

197 *Id.* at *17-20. The case law relied upon in *Bode* includes *Angevine*, *id.* at *19, also relied on by *United States v. Stratton*, 229 F. Supp. 3d 1230, 1241-42 (2017).

198 296 F. Supp. 3d 1267, 1272 (D. Kan. 2017).

199 No. 15-02838, 2017 WL 2733879, at *7 (S.D. Cal. June 26, 2017) (finding that the "express monitoring policy . . . which Defendant agreed to, rendered Defendant's subjective expectation of privacy . . . objectively unreasonable."). The Ninth Circuit ultimately reviewed the result in *Wilson* and reversed, holding that the Fourth Amendment was violated, but did so without expressly addressing the argument that Terms of Service were relevant. *See* United States v. Wilson, 13 F.4th 961, 980 (9th Cir. 2021).

200 *See Wilson*, 2017 WL 2733879, at *7 (citing cases involving government employers, including: United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) (public university); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (same); and United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (federal agency)).

201 *See, e.g.*, United States v. Sporn, No. 21-10016, 2022 WL 656165, at *10-11 (D. Kan. Mar. 4, 2022) (citing *Ackerman* and *Stratton*); United States v. Bohannon, 506 F. Supp. 3d 907 (N.D. Cal. 2020)(citing *Ackerman*).

202 This article has concluded that Terms of Service have "little or no" relevance to expectations of privacy, so let me point out two contexts in which such Terms might be relevant. First, it's possible that Terms violations permit providers to suspend accounts that might trigger a revocation of a preexisting reasonable expectation of privacy by analogy to the lease and rental context. *See supra* notes 141–64 and accompanying text. Whether such a theory is viable will have to wait for another day, but it is at least an open question that could implicate Terms of Service. Second, in the context of non-content records, it's possible that the knowing disclosure requirement of the third-party doctrine might be met in some cases, at least in part, by evidence that the disclosure was included in the Terms of Service. This theory depends on how a court interprets the knowing disclosure requirement, which is another murky area of law I cannot resolve here. Again, though, it is at least an open question.

Terms of Service might influence Fourth Amendment protections. It focuses on four doctrines—the private search doctrine, third-party consent, direct consent, and abandonment—that some courts have thought are impacted by Terms of Service. The four doctrines share a common theme: they are ways that a person who has initial rights in account information might later lose them.

This part argues that Terms of Service are irrelevant to all four doctrines. Terms of Service cannot define what private action is; they cannot determine whether a provider can exercise third-party consent; they cannot determine when Terms with a private actor amount to consent to a government search; and their violation does not amount to abandonment of Fourth Amendment interests. Terms might, at the margins, clarify certain relationships relevant to Fourth Amendment rights. But it is the actual relationships, not the Terms of Service, that matter. In part this is because private contracts shed little to no light on the concern of these doctrines. These doctrines are about actual practices, not formal policies. And in part this is because of the actual role of such Terms. While they exist on paper, Terms are rarely read and even more rarely understood.

The Section begins by introducing the four doctrines and explaining their differences and connections. It then goes through each doctrine and explains why it does not determine the scope of Fourth Amendment rights. It begins with private searches; turns next to third-party consent; then considers direct consent; and ends with abandonment.

A. *Four Ways to Lose Rights in Shared Space*

Most of this essay has focused on whether a person has established Fourth Amendment rights in information in shared spaces. That question is normally addressed, in litigation, under two guises: first, whether a person can have Fourth Amendment rights in that kind of information generally;[203] and second, whether that particular defendant has shown that his rights are the ones implicated in order to establish Fourth Amendment standing.[204]

We now consider the converse question: what does it take to *lose* otherwise-established Fourth Amendment rights in shared spaces? This question involves the intersection of four related doctrines: the private search

203 *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2212, 2220-21 (2018) (concluding that collection of at least seven days of historical cell site location records is protected under the Fourth Amendment).

204 *See, e.g.*, Byrd v. United States, 138 S. Ct. 1518, 1523-24 (2018) (assessing whether a particular defendant had sufficient legitimate interest in property to move for suppression of the fruits of its allegedly unlawful search).

doctrine,[205] consent,[206] third-party consent,[207] and abandonment.[208] The thrust of these doctrines is that, when it comes to shared spaces, both suspects and co-occupants have two ways to withdraw otherwise-existing Fourth Amendment rights: each can relinquish rights through their own action, and each can relinquish rights to the government.

The private search doctrine and third-party consent are the means for co-occupants to relinquish rights. When the co-occupant acts on their own, without government involvement, it triggers the private search doctrine. The co-occupant is a private actor outside the Fourth Amendment, so any search and seizure they independently conduct is permissible.[209] When the co-occupant relinquishes rights to the government, in contrast, that triggers the third-party consent doctrine. The government asks for the co-occupant's consent to a search and the government then searches, which is permitted so long as the co-occupant had actual or apparent authority over the items searched.[210] Note the different scope: the private search doctrine permits any private conduct, while third-party consent is bounded by actual or apparent common authority.

Abandonment and consent apply when the suspect himself is responsible for giving up the right. If a person gives up their interest in the item generally, not directly to the government, it will implicate abandonment doctrine.[211] By taking steps that a reasonable observer would understand as no longer wishing to have any interest in the property, the suspect loses their reasonable expectation of privacy and the property is abandoned.[212] On the other hand, if a suspect gives permission to the government to search, then that is a question of consent—what I will also call direct consent, to avoid confusion with third-party consent.[213] The government's search is rendered reasonable

205 For an overview, see generally 1 WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.8(b) (6th ed. 2020).

206 *See generally* 4 *id.* §§ 8.1–.2.

207 *See generally* 4 *id.* §§ 8.1–.2.

208 *See generally* 1 *id.* § 2.6.

209 *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114-15 (1984) (private freight carrier was a private actor, and any search of private packages was permitted under the Fourth Amendment).

210 *See, e.g.*, Fernandez v. California, 571 U.S. 292, 294 n.1, 307 (2014) (holding that a "lawful occupant [having common authority over] a house or apartment should have the right to invite the police to enter the dwelling and conduct a search.").

211 *See, e.g.*, Abel v. United States, 362 U.S. 217, 241 (1960) (holding that suspect who threw items away in a trash can in a hotel room that he then vacated had abandoned the items).

212 *See id.*

213 *See* Schneckloth v. Bustamonte, 412 U.S. 218, 223 (1973) (explaining that, in a case in which respondent's brother gave police permission to search respondent's car, the "precise question" at issue was whether consent had been voluntarily given).

by the suspect's voluntary permission.[214] Again, note the different scope: a person who consents to a government search lets the government search at that time but otherwise retains Fourth Amendment rights in the property, while a person who abandons property gives up their Fourth Amendment rights entirely.[215]

The differences among these four doctrines are subtle, and judges sometimes puzzle over their precise relationship.[216] But we can appreciate the main differences if we imagine a search of physical space. Imagine that Abby and Bob are partners who live together in an apartment. Bob stores his illegal drugs there, and the government has begun to investigate him. Bob is the suspect, and Abby is the co-occupant. Consider four distinct ways that Bob's drugs might end up in law enforcement hands in the absence of probable cause or a warrant.

First, Abby can take steps to relinquish Bob's rights. She might go into Bob's room, take the drugs, and bring them to the police station. That is a private search, in which Abby as a private actor is not regulated by the Fourth Amendment.[217] Next, the police may come to the apartment when Bob is not present and ask Abby to consent to a search for Bob's drugs. If Abby permits the search, and the drugs are in a place in the apartment over which she has authority, the government can search areas of Abby's actual or apparent common authority under the third-party consent doctrine.[218]

Bob can relinquish his own rights, too. The police might come to the apartment when Bob is home and ask Bob to consent to a search. If Bob tells the police it's okay for them to search, consent applies and they can search as far as a typical reasonable person would conclude was the scope of Bob's consent.[219] Finally, if Bob moves out of the apartment and tells Abby he is never coming back, leaving the drugs behind, he will have abandoned them.[220]

---

214 *See id.* at 233-34 (recognizing that where consent "was not given voluntarily," government searches were rendered unreasonable under the Fourth Amendment).

215 *See supra* notes 205–10 and accompanying text.

216 For example, in *Georgia v. Randolph*, 547 U.S. 103 (2006), a spouse consented to a law enforcement search and led officers to the bedroom where the suspected evidence was located. *Id.* at 107. The majority treated this as a question of third-party consent. *Id.* at 108-109, 122-23. Justice Thomas, dissenting, argued that the spouse was a private actor and therefore the search should be treated as a private search. *See id.* at 148-49 (Thomas, J., dissenting).

217 *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

218 The common authority can be actual, or, as in *Illinois v. Rodriguez*, 497 U.S. 177, 188-89 (1990), be reasonably perceived to exist but not actually exist.

219 *See* Florida v. Jimeno, 500 U.S. 248, 251 (1991) ("The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?").

220 *See, e.g.*, United States v. Fisher, 56 F.4th 673, 686 (9th Cir. 2022) (finding that defendants who sold house had abandoned electronic storage devices left behind in attic).

Bob's abandonment of his property eliminates his Fourth Amendment protection.

We can summarize the relationship among these four doctrines with the following chart:

DOCTRINE	RELEVANT ACTOR	GOVERNMENT INVOLVEMENT?	SCOPE
Private Search	Co-occupant	No	Any
Third-Party Consent	Co-occupant	Yes	Within common authority
Direct Consent	Suspect	Yes	What a reasonable person would perceive
Abandonment	Suspect	No	What appears abandoned

The key question becomes how Terms of Service intersect with these doctrines in the context of Internet accounts. In my view, there is little or no intersection. Terms of Service have no effect themselves; at most, they might be evidence of a relationship that does. But it is the relationship, not the Terms, that matter. A tour through each doctrine explains why.

B. *Irrelevance to the Private Search Doctrine*

Start with the private search doctrine, by which the co-occupant can act on their own outside the Fourth Amendment. The irrelevance of Terms of Service to the private search doctrine should be straightforward. In the Internet setting, the private search doctrine hinges on the relationship between the government and the Internet provider. The key question: is the provider acting as the agent of the government? If the provider is acting independently, it is a private actor and the Fourth Amendment does not apply.[221] If the provider is acting on the government's behalf, it is a government actor and the Fourth Amendment applies to its action.[222]

221 *See, e.g.*, United States v. Rosenow, 50 F.4th 715, 730 (9th Cir. 2022) (explaining that internet providers do not become government agents merely by complying with mandatory reporting statutes because, under the statutes, providers "are free to choose not to search their users' data. Therefore, when they do search, they do so of their own volition.").

222 For example, in *Commonwealth v. Gumkowski*, 167 N.E.3d 803 (Mass. 2021), a state trooper asked the cellular and Internet service provider Sprint to voluntarily disclose a suspect's cell-site

Nothing in that question is directly affected by Terms of Service, which ultimately concern a different relationship—that between the provider and the user, rather than the provider and the government. Granted, it's possible that Terms of Service might include passages that shed light on the government-provider relationship. In that sense, Terms could be relevant evidence even if they are not actually operative. For example, in *United States v. Rosenow*,[223] Yahoo and Facebook investigated Rosenow's account usage after receiving reports that he was using the accounts to further child sex trafficking.[224] In holding that Yahoo and Facebook were private actors, the Ninth Circuit relied in part on the fact that Rosenow's alleged conduct violated the providers' Terms of Service.[225] The providers were acting to enforce their Terms, the argument went, rather than to help the government; the Terms of Service violation helped show independent interest.[226]

Even then, though, the Terms of Service are relevant for what they reflect rather than their language. Terms might be evidence of a provider practice or a private interest. But the ultimate question would be whether an agency relationship existed between the government and the provider, not whether the Terms claimed or suggested they would.

C. *Irrelevance to Third-Party Consent*

A trickier case is the effect of Terms of Service on third-party consent, which applies when the co-occupant consents to a government search. The government can rely on third-party consent to search when the consenting private actor has actual or apparent common authority. The classic statement of common authority is from *United States v. Matlock*,[227] which explained that the concept was not about property interests—thus, a landlord could not consent to an apartment search,[228] and a hotel clerk could not consent to a room search[229]—

location records without a warrant. *Id.* at 810. Sprint agreed. *Id.* at 812. The Court ruled that Sprint's voluntary disclosure constituted Fourth Amendment state action: when "law enforcement instigates the search by contacting the cell phone company to request information, there is State action. That Sprint could have refused to provide records in response to [the state trooper's] request does not change the fact that he instigated the search." *Id.* at 812.

223 50 F.4th 715 (9th Cir. 2022).

224 *Id.* at 726-27.

225 *See id.* at 730 (holding that the Stored Communications Act only authorizes Internet service providers to "access information already contained on *their* servers as dictated by their terms of service," and no more, such that accessing a user's account usage data was private action rather than an action encouraged by or on law enforcement's behalf).

226 *See id.*

227 415 U.S. 164 (1974).

228 *Id.* at 171 n.7 (citing Chapman v. United States, 365 U. S. 610 (1961)).

229 *Id.* (citing Stoner v. California, 376 U. S. 483 (1964)).

> but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.[230]

At first blush, it seems plausible that Terms should influence if not define the scope of third-party consent. Imagine a Term that tracks the common authority definition. Something like this: "User agrees that the provider has joint access and control over the user's private data and assumes the risk that provider will consent to a search of that data." We can imagine a version with a prospective trigger, too: "User states that, in the event user violates any Terms of Service, user expressly wishes that provider will consent to a law enforcement search to investigate the circumstances of the violation." Doesn't the user who agrees to that term consent to the provider having common authority? At first blush, terms that are tailor-made to the legal standard might seem definitive proof the test was satisfied.

But I disagree. Common authority requires actual shared use or control, not just a recognized right of access or control. Recall the test: "mutual use of the property by persons generally having joint access or control for most purposes . . . ."[231] As the D.C. Circuit has noted, this is not about a "legal right" to act, but about "the actual circumstances"[232] of mutual use. Terms of Service might establish a legal right. But for common authority to exist, there would need to be a common experience or understanding that data is effectively shared, not just that the provider is allowed to look at it.[233] Terms of Service might be relevant to establishing that common experience or understanding, but they cannot on their own establish mutual use.

This isn't to doubt that mutual use might exist in some cases. The easiest case is cell site location records protected under *Carpenter v. United States*.[234] Such records are generated by cell providers in the course of providing connectivity, and they are used by providers for network purposes.[235] Users may not know the records exist, and ordinarily they have no direct way of accessing them.[236] Given that CSLI is created and used by providers, not

---

230 *Id.*

231 *Id.*

232 United States v. Whitfield, 939 F.2d 1071, 1074 (D.C. Cir. 1991).

233 *See id.* at 1075 (overturning a warrantless search of an adult child's bedroom in his parent's home because law enforcement could only find joint, but not mutual use).

234 138 S. Ct. 2206, 2217 (2018) ("[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.").

235 *Id.* at 2211-12.

236 My sense, from having asked this question to various audiences, is that some know the records exist while others do not.

users, it seems clear that cell providers would ordinarily have a right to consent to a government search of user CSLI records under the common authority test.[237]

How the common authority test might apply to contents is murkier. In the physical world, hotel clerks and landlords lack common authority over hotel rooms and apartments they oversee.[238] It's plausible that Internet providers have the same relationship to the contents of user communications. Perhaps Internet providers like Google or Facebook are like the landlords of their users' virtual spaces, and accordingly they lack third-party consent authority over a search of content. On the other hand, it's at least possible to view providers differently. Does it matter that user contents are mere data on a server, mixed together with other user data and easily transferred from place to place? Does it matter if user files can be scanned for advertising purposes, or to look for viruses or scan for CSAM? Perhaps that different role does not alter the nature of the common authority, but it is currently unclear.

However this is resolved, the resolution does not hinge on Terms of Service. Common authority should or should not exist based on how the contents of files are generated, used, and accessed, not because of what Terms of Service might say. It's the substance, not the form, that matters.

D. *Irrelevance to Direct Consent*

But perhaps Terms of Service are relevant to direct consent instead? On this theory, agreeing to Terms of Service authorizes the government to search your protected data. Imagine Terms of Service like this: "By using this service, I permit provider to work with the government, and to search my data as the government's agent, in the event provider deems it appropriate." Perhaps agreeing to such Terms would amount to consent to a law enforcement search, just as it says?[239]

Again, I think this is wrong. It is based on two mistakes. First, even assuming that users see and understand the relevant Terms, such hypothetical conditional Terms do not generate actual consent to a government search. Under *Florida v. Jimeno*,[240] the scope of consent is determined by asking "what

---

237 Providers would presumably exercise that right only when it appears to be lawful under 18 U.S.C. § 2702, a provision of the Stored Communications Act that prohibits voluntary disclosure of user account records subject to certain statutory exceptions. But that is a statutory question, not a constitutional one.

238 *See* Chapman v. United States, 365 U.S. 610, 616-18 (1961) (holding that landlord could not consent to the search of a house rented to another); Stoner v. California, 376 U.S. 483, 484 (1964) (holding that hotel clerk could not consent to search of hotel room).

239 This was the theory of *United States v. DiTomasso*, 56 F. Supp. 3d 584 (S.D.N.Y 2014), *aff'd on different grounds*, 932 F.3d 58 (2d Cir. 2019). *See supra* notes 94–106 and accompanying text.

240 500 U.S. 248 (1991).

would the typical reasonable person have understood by the exchange between the officer and the suspect?"[241] When a person signs up for an account with a private provider, however, there is no such exchange at all. The user is entering a relationship with a private provider. The government's future role is an abstraction. True, there is a possibility that the government might someday be involved, and that, if it is involved, the provider might act as the government's agent. But consent is permission; the mere act of proceeding after receiving such an abstract future conditional warning is insufficient to generate consent.[242]

Second, the consent theory is particularly problematic because Terms of Service are rarely read.[243] When we consider the effect of Terms of Service, we need to distinguish how they look on paper from how they operate in real life. Fourth Amendment law is concerned with actual relationships, not legal forms. And in real life, Terms of Service are generally ignored. They consist of pages of legalese that users scroll by on the way to using Internet services.

Studies have shown the point.[244] In one experiment, researchers created a fake social media site called NameDrop, Inc.[245] The designers of the study watched to see how many people actually tried to read the Terms of Service, and, among that subset, how many succeeded and understood what they read.[246] This was possible because NameDrop's Term of Service had a rather extraordinary Term: all users of NameDrop agreed "to immediately assign their first-born child to NameDrop, Inc."[247] According to the findings, 74% of users did not view the Terms of Service, and most who viewed them scrolled through the legalese too quickly to understand them.[248] Only about 7% of site users actually objected to the term.[249]

The NameDrop study echoes our common experience. Most people do not read Terms of Service. The few who try to read them don't get very far. Terms of Service are like warnings on mattress tags: some lawyer somewhere

241 *Id.* at 251.

242 *See* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (holding, in the Wiretap Act context, that a telephone user did not consent to monitoring when he was told that the telephone owner "might" monitor the phone, but not that they "were" monitoring the phone).

243 See Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUSINESS INSIDER (Nov. 17, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/NN5C-SE9P] (discussing studies that show that few Americans read Terms of Service).

244 *See id.*

245 Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMMC'N, & SOC'Y 128, 128 (2018).

246 *Id.* at 130.

247 *Id.* at 134.

248 *Id.* at 135, 137.

249 *Id.* at 138.

came up with some language that they wanted to insert, but normal people just ignore them out of a sense that they don't matter and there is nothing you can do about them anyway.[250]

Given that, it would be wrong to interpret clicking on the link "I agree" as actual agreement to the Terms. The 93% of study participants who accepted NameDrop's Terms of Service did not actually agree to immediately assign the company their first-born children. It's just legal noise that normal most people ignore. Users who agree to Terms of Service no more consent to a search than NameDrop users assign away their first-born children.

E. *Irrelevance to Abandonment*

The last doctrine to consider is abandonment. Can agreeing to Terms amount to an abandonment of rights in data? To take on the best case that it does, imagine Terms that match the legal test: "By using this service, I agree to waive all rights in my data and henceforth claim no legal interest in the data."[251] Or perhaps the Term might be contingent on a future event. Consider this one: "I agree that if I ever violate any Terms of Service, I wish that violation to be understood, and agree to it being understood, as a waiver of all rights in data and an abandonment of any interest in the data." Should that agreement be binding, such that using the service, or committing the predicate act that triggers the language, should amount to abandonment?

This argument is related to the consent claim, and it should fail for similar reasons.[252] But let me add two more points. First, abandonment doctrine is just an application of the reasonable expectation of privacy test. A person is deemed to have abandoned their Fourth Amendment rights when their conduct relinquishes a reasonable expectation of privacy.[253] Given that, there is nothing distinctly new about phrasing the issue as a matter of abandonment instead of whether a person has a reasonable expectation of privacy. The scope of expectations of privacy based on violations of owner–user agreements was addressed in Part II, and that analysis is not substantively different if rephrased under the rubric of abandonment.

---

250 With mattress tag warnings, however, the warnings are not intended for the consumer at all. Mattress tag warnings are for the mattress manufacturer or seller, who cannot by law remove the tag so the consumer can learn what was used to stuff the mattress. *See* Textile Fiber Products Identification Act, 15 U.S.C. § 70c.

251 This is not far from the actual Terms in *Commonwealth v. Dunkins*, 229 A.3d 622, 626 (Pa. Super. 2020), which the Superior Court relied on for an abandonment theory. *See supra* notes 29–36 and accompanying text.

252 *See supra* notes 239–50 and accompanying text.

253 *See* United States v. Juszczyk, 844 F.3d 1213, 1214 (10th Cir. 2017) ("Property is considered abandoned if the owner lacks an objectively reasonable expectation of privacy.")

Second, the act of signing up for an Internet account, and thus agreeing to Terms of Service, is a particularly unlikely act to construe as abandonment. In the Fourth Amendment setting, abandonment asks if the person took acts that should be understood as disavowing an interest in the property.[254] But a person who signs up for an account is seeking to use the account. It seems difficult to construe the act of signing up as intending to claim a disavowal of specific rights. That is particularly so because the records that the user will create or otherwise store in the account are sufficiently private that courts have concluded they are protected by a reasonable expectation of privacy. It defies common sense to treat the act of creating a private space with private data as having abandoned any privacy interest in that data.

That might be enough to make the Terms binding as a matter of contract law, a matter I will leave to the contracts scholars.[255] But it is not enough to amount to Fourth Amendment abandonment. Clicking on Terms of Service is a formality—the step you need to take before you can access a service—rather than a genuine assertion of intent to follow what the Terms say. Companies with millions or even billions of users worry about being sued, giving them an incentive to include language that gives companies broad rights and users relatively few to minimize corporate liability. This is the technological and economic reality. But Fourth Amendment rights are not at the mercy of these business decisions.

CONCLUSION

The scope of the Fourth Amendment online is often framed by the scope of the third-party doctrine.[256] Under the third-party doctrine, 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."[257] Under this rule, a promise to keep information secret has no effect. The third-party doctrine applies, and no rights exist, even if the suspect has shared his information with a party that swears six ways from Sunday that the confidentiality of the information will be preserved.

---

254 *See id.*

255 For a critique, see David A. Hoffman, *Defeating the Empire of Forms* 109 VA. L. REV. 1367, 1371-74 (2023) (acknowledging the problems posed by widespread use of form contracts and advocating a new approach).

256 *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2214-17 (2018) (discussing whether historical cell site records are protected by reference to the scope of the third-party doctrine).

257 United States v. Miller, 425 U.S. 435, 443 (1976).

Terms of Service raise the converse problem. Terms of Service matter only if the third-party doctrine does not apply. That is, the records must first be protected by the Fourth Amendment for the question of whether contractual Terms eliminate rights to make a difference. Instead of asking whether promises of confidentiality can create Fourth Amendment privacy, as the third-party doctrine poses, we ask whether contractual promises of its absence can eliminate rights that would otherwise exist. In both cases, the answer is the same. The intersection of contracts and the Fourth Amendment is a two-way street. Agreements cannot create Fourth Amendment rights. Nor can they take them away.

Broadly speaking, how Fourth Amendment law applies to the Internet is uncertain and evolving. The evolution of the law is still in its early stages. It understandably tempting for judges, faced with novel claims, to seek refuge in the clear language of Terms of Service. In a judicial record, the Terms give the appearance of certainty. They make it look like the defendant has sealed his own fate by clicking "I agree." But appearances can be deceiving. Terms of Service are private contracts, not agreements with the government. They have little or no impact on Fourth Amendment rights.