New technologies force us to re-examine theories, no less in law than in science. Information technologies have radically changed social and commercial interactions, providing communication, access to data and computation resources on a scale barely imaginable just fifty years ago, let alone in the eighteenth century. But with these benefits have come threats as well. In particular, the use of information technologies vastly increases the scope and possibility of governmental and private parties’ interference with and surveillance of individuals, and, as a result, creates severe tensions on the jurisprudential theories used to protect basic liberties and privacies.\(^1\) The National Security Agency’s internet and surveillance activities revealed this summer by Edward Snowden are one symptom of these tensions.\(^2\) As our technological abilities increase, so do the threats to basic liberties.

---


Copyright © 2014 Journal of High Technology Law and Lon Berk.
All Rights Reserved. ISSN 1536-7983.
In this essay, I examine one of these tensions by looking at the impact of cloud computing on Fourth Amendment rights.³ Current Fourth Amendment jurisprudence leaves a gap that threatens to swallow the whole of the Amendment’s protections when applied incautiously in our current technological milieu.⁴ This is at least in part because that jurisprudence developed during times when technology imposed limitations not only upon surveillance, but, perhaps as importantly, upon the nature and volume of the papers and effects citizens, individually and collectively, had the power to create, use, and possess.⁵ The availability of technological innovations, including in particular, cloud computing, has vastly expanded what citizens can create and use and hence what governments can seize and search.⁶ Moreover, cloud computing has done so in a manner that exposes certain shortcomings in current Fourth Amendment jurisprudence.⁷

The use of mobile computing devices has enabled citizens in their personal and business lives to access and appropriate as their own a vast amount of valuable information.⁸ Cloud computing has

³ The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

See U.S. CONST. amend. IV (indicating that the Fourth Amendment is incorporated in the Fourteenth Amendment); see also Brokaw v. Mercer Cnty., 235 F.3d 1000, 1009 (7th Cir. 2000) (finding that the Fourth Amendment is incorporated in the Fourteenth Amendment).


⁵ See id. at 1344 (describing the Supreme Court’s traditionally narrow interpretation of Fourth Amendment protections granted to users of new technologies).


⁷ See id. (reiterating the gap in Fourth Amendment protections afforded to users of new technologies).

⁸ See id. at 2221-22 (describing the ability of Wireless Internet users to access data stored in a variety of places).
made this ever more available and economical so that an ever in-
creasing number of ordinary commercial and personal relationships
are mediated through “the cloud.”9 As a result, a realistic analysis of
the property, papers and effects of individuals can no longer be lim-
ited to what was available using 18th, 19th and even many 20th century
technologies.10 Rather, what we are able to document and create —
to appropriate from the information commons — has been expanded
well beyond what our predecessors were able to do and, perhaps,
even conceive of doing.11 As a result, the ordered liberty our consti-
tution protects needs to be understood in the context of our technolo-
gies and this, I argue below, may require a shift in some aspects of
our present Fourth Amendment jurisprudence that, perhaps, more
keenly reflects the assumptions and intentions of its original drafters.

One might contend that because the nature of current infor-
mination technology was not foreseen and perhaps not foreseeable by
the Fourth Amendment’s drafters, the Amendment has no application
to that technology.12 Such a view, however, would in effect concede
that the Amendment has no application in our present environment.13
It is a premise of this paper that Fourth Amendment jurisprudence
must take account of the technology ordinary citizens employ and the
property they create using that technology when applying the
Amendment’s protection.14 The security the Amendment expressly
protects is not one that depends upon the state of technology.15 Un-
fortunately, current jurisprudence does not recognize this fact and,
consequently, threatens to undermine the very “ordered liberty” some

9 See id. (expanding upon uses of cloud computing and accessibility of content to
the public).
10 See Shih Ray Ku, supra note 4, at 1332-50 (providing a historical perspective of
Fourth Amendment protections and the implications on modern technologies).
11 See Shih Ray Ku, supra note 4, at 1332-50 (expressing what we can document
and create is far beyond what predecessors imagined).
12 See Shih Ray Ku, supra note 4, at 1345 (discussing foreseeable applications of
the Fourth Amendment).
13 See Shih Ray Ku, supra note 4, at 1344 (highlighting potential problems when
applying the Fourth Amendment to modern technology).
14 See U.S. CONST. amend. IV (explaining the connection between person, property
and the Fourth Amendment).
15 See id. (describing the Fourth Amendment protection).
have held the Amendment and constitutional provisions were designed to protect.16

Section I

Cloud Computing and Big Data

Both commercial and personal computation make wide use of what is called “cloud computing.”17 Under certain circumstances, cloud computing can lead to the development of huge databases, which when mined, can provide clients and providers with useful information.18 Rather than possessing, maintaining and controlling their own data and computation resources, businesses and individuals are increasingly relying upon third-parties to provide and maintain both their data content and computation resources.19 The widespread use, for example, of tablets and smartphones is only possible because their users exploit computational resources located not on their devices, but on servers elsewhere.20 Under this model, access to hardware and software applications is provided to businesses and individuals by third-parties through network connections.21 Even relatively

16 See Palko v. Connecticut, 302 U.S. 319, 324-25 (1937) (explaining how protection under the 14th Amendment is implicit but is undermined by current jurisprudence).
17 See David Linthicum, What’s Driving Corporate Cloud Use? Home Cloud Use, INFOWORLD (Mar. 1, 2013), archived at www.perma.cc/0vtjGc1iqDU (describing the increase of cloud computing in both work and home environments).
18 See Mike Hogan, Cloud Computing & Databases: How Databases Can Meet the Demands of Cloud Computing, SCALEDB (Nov. 14, 2008), archived at www.perma.cc/0h8yEkJ2SUJ (describing the key benefits of cloud computing to provide users with easier accessibility of information through large database architecture).
19 See Linthicum, supra note 17 (explaining that third-party platforms such as iCloud, Dropbox, Google, Apps, and SaaS promote cloud adoption).
21 See Nicole D. Galli & Edward Gecovich, Cloud Computing and the Doctrine of Joint Infringement: ‘Current Impact’ and Future Possibilities, 11 J. MARSHALL REV. INTELL. PROP. L. 672, 677 (2012) (outlining five essential characteristics of cloud computing). For our purposes, cloud computing can be treated as the use by one party, the client, of computational resources of another, the provider, by means of communications over a network. See id. at 676-78. (defining cloud computing). Under usual models of cloud computing, it is treated as taking one of three forms:
mundane matters, such as entering an appointment in a calendar, may make use of the cloud. For instance, when an appointment is entered on a smart phone’s calendar through a voice instruction, the phone converts the instruction into a digital form and transmits it over a network to software on a server located elsewhere. This process employs a voice recognition algorithm, owned by the provider, but used by the client, to translate the voice instruction into the programming language of the device, which is then transmitted back to the device. Thus, the full use of mobile computing devices inextricably involves permitting third-parties — the cloud and network providers — access to information the consumer may treat as, and believe is, private. A consumer of these services may also keep his or her records, including tax returns and other financial information, health records, books, music and virtually any other imaginable content, on a server maintained by a cloud vendor, such as Amazon or Google. Equally, the user may track, save, and search for locations using the provider’s computational resources.

Infrastructure as a service (IaaS), under which the provider offers computers to clients; platform as a service (PaaS), under which the provider offers a computer platform to clients; and software as a service (SaaS), under which the provider offers application software to clients. See Jeff Caruso, IaaS vs. PaaS vs. SaaS, NETWORK WORLD (Nov. 2, 2011), archived at www.perma.cc/0nH9zFtBxPM (defining cloud computing models). For our purposes, the critical point is that one person is using the computational resources of another through a network. See id.; see also CLOUD COMPUTING: PRINCIPLES, SYSTEMS AND APPLICATIONS 3.3.5 55-6 (Nikos Antonopolous & Lee Gillam, eds., 2010) (explaining the technical distinction between models).

See Galli & Gecovich, supra note 21, at 674 (describing various consumer services that use cloud computing).


23 See, e.g., BigHand Launches New Server Based Speech Recognition Module, LEGAL IT INSIDER (Nov. 5, 2009), archived at www.perma.cc/0d4KyqPie8R (covering the launch of a server side voice recognition module).

24 See David Byrd, Cloud Privacy: An Unreasonable Expectation?, CHANNEL PARTNERS (Feb. 17, 2012), archived at www.perma.cc/0RKR1ppupCG (discussing the expectation of privacy on the Internet and special concern regarding cloud service providers).

25 See Robert Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, WORLD PRIVACY FORUM, 8-10 (Feb. 23, 2009), archived at www.perma.cc/0CCQuq8AJnE (listing the types of material saved by different cloud providers).

26 See id. at 6-7 (stating a cloud provider may scan or search user records).
tion of computation services involves permitting third party possession and - to some degree - control of private, confidential information.\(^{28}\)

The cloud consumer is known to use both storage and computation capacity only when it is required.\(^{29}\) Cloud computing makes the use of computation resources more efficient, and hence more affordable and widespread.\(^{30}\) Through programming techniques called “virtualization” that effectively permit a single server (or server group) to appear and operate as multiple servers, multiple businesses and individuals can operate their own computation systems on a single server system, obtaining the benefits of owning their own system without the expense of acquiring and maintaining the hardware.\(^{31}\)

Given these advantages of cloud computing, its frequency will increase as its advantages over individual ownership of computation resources become more widespread; or, as one commentator describes it:

The shift toward cloud computing is driven by many factors including ubiquity of access (all you need is a browser), ease of management (no need for user experience improvements as no configuration or back up is needed), and less investment (affordable enterprise solution deployed on a pay-per-use basis for the hardware, with systems software provided by the cloud providers). Furthermore, cloud computing offers many advantages to vendors, such as easily managed infrastructure because the data center has homogeneous hardware and system software. Moreover, they

\(^{28}\) See id. at 7 (finding that storing information in the cloud may be detrimental to privacy and confidentiality).
\(^{29}\) See Galli & Gecovich, supra note 21, at 676-77 (stating storage space may be reallocated when the user is finished using it).
\(^{30}\) See Galli & Gecovich, supra note 21, at 676 (describing advantages of cloud computing including increased resources at lower costs).
\(^{31}\) See Caruso, supra note 2121 (discussing the different program techniques of virtualization).
are under the control of a single, knowledgeable entity.  

Indeed, we have witnessed the impact of these incentives, with cloud computing expanding among consumers and businesses for personal and commercial computation needs.

The result of cloud computing has been not only a more efficient use of computation resources but a more equitable distribution. 33 People are able to obtain the benefits of massive data storage and computation capacity without the expense of investing in the hardware required. 34 Furthermore, under certain circumstances, cloud computing vendors may combine data regarding their users’ transactions and analyze that data to their, and their users’, advantage. 35 Examples of this phenomenon include iTunes software which permits users to upload their music to Apple servers, allowing them to analyze collections and determine the tastes of their users. 36 For example, they may find that there is a 90% chance that users liking music by one artist commonly also have a propensity for another artist and can then recommend this new artist to that user. 37 The vendors’ collection of this data thus works to the benefit of both the vendor itself as well as its customers. 38

32 See Antonopolous & Gillam, supra note 21, at 5 (describing an overview of the cloud standards).
34 See id. (explaining the decrease in computer hardware costs resulting from use of cloud computing).
36 See APPLE, TERMS & CONDITIONS (September 18, 2013), archived at www.perma.cc/0yptxWWREKS (describing Apple software available, like iTunes Match, that collects information about user preferences and gives personalized information).
37 See Christopher Mims, How iTunes Genius Really Works, MIT TECH. REV. (June 2, 2010), archived at www.perma.cc/0sCVDrKVpsj (describing how iTunes Genius operates).
38 See id. (discussing the benefits of iTunes Genius).
There is no need to focus on the actual intricacies of cloud computing or the collection of “big data.” What is essential for our purposes is that individuals in effect share computational resources maintained by a third-party for both storage and computations and, under some circumstances, permit that third-party to analyze a database generated from all information collected. The key element in these transactions for our purposes is: a consumer or client with a computing device (oftentimes mobile) that transmits information over a network to a cloud provider that owns and maintains computational infrastructure on which data is stored and computations performed. Consequently, a critical aspect of cloud computing is that the user’s information must, at least for a time, be held by and within the control of third-parties – the cloud vendor and the network owner(s).

It is this fact that creates problems under current Fourth Amendment jurisprudence. A personal diary may for example be maintained in a document stored on Google servers and updated from multiple computing devices. In effect the user’s papers — the effects of their intellectual efforts — are created and maintained at a lo-

40 See id. at 268 (describing how cloud computing retrieves and stores data).
41 See id. at 268-69 (noting how a user’s data is stored and controlled by third party server and providing an example of how information can be accessed by a third party server if necessary). See also Seny Kamara & Kristin Lauter, Cryptographic Cloud Storage (2010), archived at www.perma.cc/0MsUbNJe8YM (describing cryptographic cloud storage). Providing the network owners with access to data is not necessary, given cryptography. Id. A cryptographic method through which a key is maintained by a third-party so that multiple parties can transfer encrypted messages among themselves can be replaced by one not involving that third-party. Id. Thus, the provider and consumer need not allow the network provider to have access to their information. Id. Similarly, if two (or more) user wish to communicate through a cloud server, they may do so encrypting their messages, without providing the key to the provider. Id. Note, however, that for most uses of the cloud, for example, searching for locations, or transmitting emails, it is critical that the provider is able to receive some decrypted information and thus the consumer must provide some information about itself to the provider. Id.
42 See U.S. CONST. amend. IV (stating the lack of protection for information accessible to the public).
43 See Wilson, supra note 39, at 267 (describing the various of ways of storing information in the cloud).
cation distant from the user.\textsuperscript{44} The consumer may also use a map application on a server to obtain directions.\textsuperscript{45} Current Fourth Amendment jurisprudence does not make clear the security of such materials and, as we will see, may instead entail that they have little or no protection.\textsuperscript{46} Instead, when a person gives control over information to a third-party there may no longer be a privacy interest available to protect against seizure or search of that information.\textsuperscript{47} This principle, called the “Stranger Principle,” if employed in its current form would deprive information developed and maintained through cloud computing of virtually any Fourth Amendment protection.\textsuperscript{48} This seems wrong; the interest protected by the Amendment is the same whether a personal diary is stored in a safe in one’s bedroom or encrypted on a server farm in Poland.\textsuperscript{49} As such, unless the Amendment is to have only limited impact in the twenty-first century, something is missing from its present jurisprudential support.

Section II

A. Fourth Amendment Jurisprudence As A Reaction To Technology

The Fourth Amendment provides:

\textsuperscript{44} See Wilson, supra note 39, at 267-68 (detailing the creation and storage of user data in cloud computing).


\textsuperscript{46} See id. at 949-50 (expressing difficulties in determining what qualifies as a search under Fourth Amendment jurisprudence).

\textsuperscript{47} See Katz v. United States, 389 U.S. 347, 351 (1967) (“What a person knowingly exposes to the public even in his own home or office, is not a subject of Fourth Amendment protection” (citing Lewis v. U.S., 385 U.S. 206, 210 (1966))).

\textsuperscript{48} See Jeb Rubenfeld, The End of Privacy, 61 STAN. L. REV. 101, 107 (2008) (defining “Stranger Principle” as a concept that undoes the framework of the Fourth Amendment by determining root individuals’ privacy expectations in widespread social norms); see also Katz, 389 U.S. at 350 (adding another limitation to Fourth Amendment protection).

\textsuperscript{49} See U.S. CONST. amend. IV (defining citizens’ general rights of privacy from unwarranted searches and seizures); see also Jones, 132 S. Ct. at 951 (debating the ambiguity of the Fourth Amendment regarding the extent of protection against unwarranted and unlawful search and seizure with information that is intended as private).
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁵₀

The enforcement of the Amendment is generally understood to have started with trespass and to have evolved over time through confrontations with new surveillance technologies so that eventually, at least with respect to searches, the question of whether the Amendment’s protection has been violated developed into the question of whether there was a violation of a reasonable expectation of privacy.⁵¹

In *Olmstead v. United States*,⁵² during prohibition, government agents investigated a conspiracy to distribute alcohol.⁵³ The agents tapped phone lines leading into the targets’ houses and main office, without violating the premises, intercepting incriminating conversations.⁵⁴ Evidence was gathered for months, with stenographers auditing and recording multiple conversations.⁵⁵ The Court held that there was no violation of the Fourth Amendment because there was no “actual entrance into the private quarters of defendant and the taking away of something tangible.”⁵⁶

⁵⁰ U.S. CONST. amend. IV.
⁵³ See id. (recounting government officials’ investigation of a conspiracy to distribute liquor unlawfully).
⁵⁴ See id. at 456-57 (explaining how federal officers obtained evidence of a conspiracy without trespassing on defendants’ property).
⁵⁵ See id. at 457 (describing the government’s methods to obtain evidence).
⁵⁶ See id. at 464. But see Gouled v. United States, 255 U.S. 298, 313 (1921) (finding a violation of the Fourth Amendment where an army intelligence officer gained access to defendant’s office and carried away several documents). *Olmstead* distinguished *Gouled* contending that there was no actual entry into defendants’ premises and that nothing tangible was taken. See *Olmstead*, 277 U.S. at 464. Instead, *Olmstead* reasoned there was only testimony of “voluntary conversations secretly overheard.” Id.
[O]ne who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and ...the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.\textsuperscript{57}

Accordingly, \textit{Olmstead} held (5-4), that there was no violation of the Fourth Amendment.\textsuperscript{58}

Justices Holmes, Brandeis, Stone and Butler dissented.\textsuperscript{59} Justice Brandeis’ dissent focused on the interest in personal privacy that he argued was invaded by the tapping of private conversations, and he reasoned:

\begin{quote}
It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence…\textsuperscript{60}
\end{quote}

[The makers of the Constitution] conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.\textsuperscript{61}

\textit{Olmstead} was followed by a series of cases, focusing on the distinction between trespassory and non-trespassory incursions into

\begin{footnotes}
\item[57] \textit{Olmstead}, 277 U.S. at 466.
\item[58] See \textit{id.} at 469 (affirming judgment of the Circuit Court of Appeals).
\item[59] See \textit{id.} (detailing dissenting opinions).
\item[60] See \textit{id.} at 474-75 (Brandeis, J., dissenting).
\item[61] See \textit{id.} at 478-79 (Brandeis, J., dissenting). It is commonly thought that Justice Brandeis’ reasoning eventually prevailed and became the foundation of Fourth Amendment jurisprudence. See \textit{Katz v. U.S.}, 389 U.S. at 353 (holding \textit{Olmstead} no longer controlling in light of recent electronic technologies).
\end{footnotes}
constitutionally protected areas.\textsuperscript{62} As telephone technology became increasingly part of life, with parties increasingly relying upon it to conduct their private affairs, the treatment of the technology that supported \textit{Olmstead}’s reasoning became more difficult to maintain.\textsuperscript{63} Finally, in \textit{Katz v. United States}, the Supreme Court adopted a different test for determining whether or not a search was unreasonable, which employed the ideas underlying Brandeis’ dissent in \textit{Olmstead}.\textsuperscript{64}

Like \textit{Olmstead}, \textit{Katz} involved wiretapping, although not of conversations from a home and offices, but from a phone booth.\textsuperscript{65} \textit{Katz} was a bookmaker using a telephone booth to transmit wagering information across state lines.\textsuperscript{66} Government agents attached an electronic listening and recording device to the outside of the telephone booth, obtaining recordings of Katz’s side of the calls.\textsuperscript{67} The recordings were introduced at trial and Katz was convicted and appealed.\textsuperscript{68}

On appeal, the government argued that the surveillance did not violate the Fourth Amendment because the recording device was on the outside of the telephone booth and did not infringe upon a “constitutionally protected area.”\textsuperscript{69} Katz contended the Fourth Amendment had been violated because there was a violation of his right of privacy.\textsuperscript{70} The Supreme Court rejected both arguments, stating:

\begin{quote}
In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by
\end{quote}

\textsuperscript{62} See Goldman v. United States, 316 U.S. 129, 134 (1942) (concluding electronic surveillance accomplished without physical penetration of petitioner’s premises did not violate Fourth Amendment); see also Berger v. New York, 388 U.S. 41, 55 (1967) (holding that the state’s eavesdrop statute violated the Fourth Amendment).

\textsuperscript{63} See \textit{Katz}, 389 U.S. at 353 (holding that the trespass standard is no longer controlling for Fourth Amendment protection).

\textsuperscript{64} See \textit{id.} (reiterating the holding).

\textsuperscript{65} See \textit{id.} at 349 (describing the location of the wiretap).

\textsuperscript{66} See \textit{id.} at 348 (describing the defendant’s charges).

\textsuperscript{67} See \textit{id.} at 348-54 (illustrating the government’s actions).

\textsuperscript{68} See \textit{id.} at 348-49 (explaining decisions at trial and appeal’s level).

\textsuperscript{69} See \textit{Katz}, 389 U.S. at 352 (explaining government’s argument that they did not violate defendant’s Fourth Amendment rights).

\textsuperscript{70} See \textit{id.} at 349 (reiterating the defendant’s argument that the wiretap violated the privacy of booth users).
incantation of the phrase “constitutionally protected area.” Secondly, the Fourth Amendment cannot be translated into a general constitutional “right to privacy.” That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.\textsuperscript{71}

The Court reasoned that:

\begin{quote}
[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.\textsuperscript{72}
\end{quote}

The Court then noted that telephone technology had become a “vital” part of private communications.\textsuperscript{73} Where the \textit{Olmstead} court had analogized use of a telephone to a broadcast of one’s voice into public areas, the \textit{Katz} court adopted another view of the technology, stating:

\begin{quote}
[A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.\textsuperscript{74}
\end{quote}

In his concurrence, Justice Harlan adopted a reasonable expectation of privacy test: “[T]he rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited

\begin{footnotesize}
\begin{footnote}{\textsuperscript{71} See \textit{id.} at 350.}
\end{footnote}
\begin{footnote}{\textsuperscript{72} \textit{Katz}, 389 U.S. at 351.}
\end{footnote}
\begin{footnote}{\textsuperscript{73} See \textit{id.} at 352 (discussing the privacy expectations of a telephone booth user).}
\end{footnote}
\begin{footnote}{\textsuperscript{74} \textit{Id}.}
\end{footnote}
\end{footnotesize}
an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”

Justice Black dissented, reasoning that the Fourth Amendment protected only “tangible” things and that conversations did not qualify as such.

The jurisprudence from \textit{Olmstead} to \textit{Katz} involved an evolving incorporation of telephone use in social life. As the phone increasingly became a part of that life, the Court’s treatment of the technology as akin to a radio broadcast became more and more strained, until, in \textit{Katz}, the Court was forced to abandon its prior treatment of that technology and recognize that it had become a method of engaging in private, even intimate, conversations, requiring and deserving Fourth Amendment protection.

\textbf{U.S. v. Jones}

The stress created by the Fourth Amendment basing its protections on such an individualistic notion of privacy recently came to the forefront. In \textit{United States v. Jones}, the Supreme Court unanimously held that tracking a driver’s movements for over a month by a GPS device attached to the bottom of the driver’s vehicle constituted a violation of the Fourth Amendment. The decision, however, was based upon two different theories, and a careful reading of the

\begin{itemize}
\item \textit{Id.} at 361 (Harlan, J., concurring).
\item \textit{See id.} at 365 (Black, J., dissenting) (outlining Justice Black’s position).
\item \textit{See Olmstead}, 277 U.S. at 456-57 (demonstrating the Supreme Court’s initial interpretation of telephone use for Fourth Amendment purposes); \textit{see also Katz} 389 U.S. at 352 (describing Supreme Court’s modernized conception of telephone use).
\item \textit{See Katz}, 389 U.S. at 352 (delineating the telephone’s modern role for personal use).
\item \textit{See Jones}, 132 S. Ct. at 948-54 (discussing the unconstitutionality of warrantless GPS monitoring of individuals).
\item \textit{See id.} at 949 (holding the warrantless use of a GPS device violates the Fourth Amendment). \textit{Jones} was recently applied by the Third Circuit in \textit{United States v. Katzin}. \textit{See United States v. Katzin}, 732 F.3d 187 (3d Cir. 2013). \textit{Katzin} held that not only was the attachment of a GPS device to an automobile a violation of the Fourth Amendment, but that the good faith exception to the exclusionary rule did not apply, even though the activity in question occurred before \textit{Jones} was decided. \textit{Id.} (discussing the court’s holding).
\item \textit{See Jones}, 132 S. Ct. at 954 (noting that the GPS placement was a search as it was located on a constitutionally protected area).
\end{itemize}
justices’ different opinions suggests the possibility that future cases squarely presenting the issues raised by the cloud computing model may find no Fourth Amendment protection. The justices’ different opinions suggests the possibility that future cases squarely presenting the issues raised by the cloud computing model may find no Fourth Amendment protection. Part of the struggle between these theories may arise out of the unsuitability of the reasonable expectations test to deal with the contractually created papers and effects upon which cloud computing depends. For example, when using GPS devices in cars or smartphones, the provider and customer’s agreements create an arrangement that allows a third-party to use the client’s location repeatedly in order to provide useful content regarding matters such as nearby restaurants, coffee shops or shopping malls, directions and emergency assistance. In exchange for these services the client, if not explicitly, then at least implicitly, arguably has given the third party the ability and right to use its information for some of its own purposes, thereby allowing the third-party to retain information on the client’s searches and travels to determine the interests of similar persons, thereby permitting targeted advertising and marketing arrangements that are of value. But the ability and right given to the third-party is nonetheless one that, at least for the majority of ordinary users of mobile computation devices, is believed to go no further; the user has given the provider information (that may be of use to the provider) in exchange for consideration that includes at least in part information that may be of use to the user.

In Jones, government agents were investigating a suspected narcotics distributor, and attached a small global positioning system (GPS) tracking device on the undercarriage of the suspect’s Jeep.

82 See id. at 949-54 (discussing the two different opinions, the majority’s 18th century guarantee against unreasonable searches and the concurring justices’ exclusively Katz’s reasonable-expectation-of-privacy test).
83 See Couillard, supra note 6, at 2238-39 (discussing the reasonable expectations test as it relates to cloud computing); see also Jones, 132 S. Ct. at 951-52 (explaining that the reasonable expectation theory is not sufficient by itself for Fourth Amendment concerns dealing with electronic tracking devices).
84 See Jones, 132 S. Ct. at 963 (describing how cellphones permit the tracking and monitoring of users).
86 See id. (mentioning the benefit garnered by users who allow access to their data).
87 See Jones, 132 S. Ct. at 948 (explaining how agents planted a GPS tracker under the Jeep).
The device was installed without a warrant. Over the next 28 days, the government used the device to track the Jeep without the knowledge of its owner and collected more than 2000 pages of data. The District Court denied a motion to suppress this information, except with respect to information obtained while the vehicle was in the garage adjoining the suspect’s home, reasoning that the remaining information was admissible because “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”

After his conviction, the suspect appealed to the D.C. Circuit, contending that the Fourth Amendment had been violated by agents “tracking his movements 24 hours a day for four weeks with a GPS device they had installed on his Jeep without a valid warrant.” The government, citing United States v. Knotts, argued that there was no Fourth Amendment violation because “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”

The United States Court of Appeals for the D.C. Circuit distinguished Knotts, noting that that decision left open the question of whether a warrant would be required in a case involving 24-hour surveillance.

“[A] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,” not that

88 See id. (noting agents had obtained a warrant permitting the installation of the device within ten days in Washington D.C., but installed it on the eleventh day in Maryland). They also replaced its battery, without a warrant, while the Jeep was in Maryland. Id.
89 See id. (describing government collection of vehicle location data within 50 to 100 feet over a four-week period).
90 See id. (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).
93 See id. at 281; see also Jones, 132 S. Ct. at 948 (citing the Knotts ruling).
94 See Maynard, 615 F.3d at 556 (distinguishing between Knotts and the present case due to the lack of ruling on whether a warrant would be required for 24-hour surveillance).
such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it…Here the police used the GPS device not to track Jones’s “movements from one place to another,” but rather to track Jones’s movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place.

The D.C. Circuit first addressed whether the information that the police obtained by tracking Jones was “actually exposed.” To answer this question, the Court found that the analysis begins with the question of “not what another person can physically and may lawfully do but rather [with the question of] what a reasonable person expects another might actually do.” Thus, the court reasoned, the questions regarding expectation of observations from overhead flights turned on whether the flights at that level were sufficiently routine enough so that it would be unreasonable for someone from the ground to expect that their property will not be observed from that height. Using this test, the D.C. Circuit concluded that:

[T]he whole of a person’s movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places,

---

95 Id. at 557-58 (quoting Knotts and comparing to the case at bar).
96 Id. at 559 (framing the issue as whether the information that police obtained by tracking Jones was exposed).
97 Id. (introducing the Court’s analysis of lawful behavior in terms of tracking).
98 See id. (citing Justice O’Connor’s concurring opinion in Florida v. Riley, 488 U.S. 445, 450 (1989), affirming that air travel is a routine part of modern life and it is not an invasion of privacy for property to be observed from planes at high altitudes).
people, amusements, and chores that make up that person’s hitherto private routine.99

Noting that when it comes to privacy, “the whole may be more revealing than its parts.”100 The Court also held that the information collected was not “constructively exposed” either.101

The whole of one’s movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.102

The Court found that a “reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects his movements to remain ‘disconnected and anonymous.’”103 Thus, the Court concluded, there was no constructive disclosure either.104 Finding that the expectation was reasonable and the search unreasonable, the Circuit Court reversed Jones’ conviction.105

99 Maynard, 615 F.3d at 560 (holding that it is unreasonable to follow a person’s movements for a month).
100 Id. at 561 (discussing the composition of privacy and constructive exposure to the public).
101 Id. at 561-62 (establishing the Court’s holding about the nature of the information collected).
102 Id. (explaining that the entirety of one’s movements over a period of time provides more information than singular actions contained within that entirety).
104 See Maynard, 615 F.3d at 561 (finding that when analyzing the whole in terms of the parts, the information obtained by the police was not constructively exposed).
105 See id. at 568 (holding that the information that the police discovered was not constructively exposed).
The Supreme Court in Jones unanimously affirmed the Circuit Court’s decision, but it did so through three concurring opinions. The court’s opinion was drafted by Justice Scalia, joined in by Chief Justice Roberts and Justices Kennedy, Thomas and Sotomayor. The Court’s opinion was based not on the Katz reasonable expectations test, but upon the earlier line of cases that tied Fourth Amendment jurisprudence to common-law trespass. Noting that Katz did not overrule this earlier precedent, Justice Scalia reasoned:

Jones’s Fourth Amendment rights do not rise or fall with the Katz formulation. At bottom, we must “assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” ...[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas (“persons, houses, papers, and effects”) it enumerates. Katz did not repudiate that understanding.

Justice Scalia noted that the Jeep on which the GPS device had been installed was an “effect” within the meaning of the Fourth Amendment and concluded that “the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search.’” Justice Sotomayor wrote a separate concurring opinion, stressing that the critical issue was whether the Government had “obtain[ed] information by physically intruding on a constitutionally protected area.” She noted that

the government had installed a Global Positioning System (GPS) tracking device on [the] Jeep without a

---

106 See Jones, 132 S. Ct. at 948-64 (examining the court’s split decisions).
107 See id. at 947 (noting the respective judges who joined in the opinion).
108 See id. at 953 (establishing that the Court based its opinion on jurisprudence that tied electronic surveillance to common-law trespass).
109 Id. at 950 (explaining that Katz did not change the Fourth Amendment interpretation).
110 Id. at 949 (concluding that the act of the Government placing tracking devices on the vehicle of a target constitutes a search within the meaning of the Fourth Amendment).
111 Id. at 954 (Sotomayor, J., concurring) (quoting Scalia J. majority’s opinion).
valid warrant and without Jones’ consent, then used that device to monitor the Jeep’s movements over the course of four weeks. The Government usurped Jones’ property for purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection.\textsuperscript{112}

She noted that the government could obtain the same results by “enlisting factory- or owner- installed vehicle tracking devices or GPS-enabled smartphones.”\textsuperscript{113} She went on to note that in such circumstances, the trespass test employed by the court’s opinion gave little guidance, and that the \textit{Katz} test would have to be applied.\textsuperscript{114} “Under that rubric,” she wrote, “I agree with JUSTICE ALITO [concurrence] that at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’”\textsuperscript{115} Justice Sotomayor noted the ease of collecting GPS data and then storing and mining it years into the future.\textsuperscript{116} Noting the chilling effect the existence of such a database might have on associational and expressive freedoms, Justice Sotomayor noted that the result would be “a too permeating police surveillance.”\textsuperscript{117} It followed then that “[m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”\textsuperscript{118}

Justices Alito, Ginsburg, Breyer and Kagan did not join in the court’s opinion but concurred in the result based upon an opinion written by Justice Alito.\textsuperscript{119} The opinion noted that basing the decision on the warrantless trespass of chattels, by placing a GPS device on the outside of a car, “strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case

\begin{itemize}
\item \textsuperscript{112} See \textit{Jones}, 132 S. Ct. at 954.
\item \textsuperscript{113} \textit{Id.} at 955.
\item \textsuperscript{114} See \textit{id.} (providing in cases of non-physical invasion on property the trespassory test provides little guidance).
\item \textsuperscript{115} \textit{Id.} (quoting Alito J. concurrence).
\item \textsuperscript{116} See \textit{id.} at 956 (highlighting the efficiency of GPS data for governmental purposes).
\item \textsuperscript{117} \textit{Id.} (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
\item \textsuperscript{118} See \textit{Jones}, 132 S. Ct. at 957.
\item \textsuperscript{119} See \textit{id.} (Alito, J., concurring) (noting the Justices’ positions).
\end{itemize}
Instead, Justice Alito applied the *Katz* test, finding that “relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable.” Alito expounded:

But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual’s car for a very long period.

Five justices thus found that the use of a GPS device attached without a warrant to the outside of an automobile to track movements of a suspect violated the Fourth Amendment. Five justices found the same activity violated the *Katz* test, and thereby violated the Fourth Amendment. The two concurring justices, Justice Sotomayor and Justice Alito, expressly found that the *Katz* test and trespassory test were implicated and noted that the issues raised in the majority opinion may require revisiting the notion that information in a third-party’s hands is no longer entitled to Fourth Amendment protection. What the decision leaves open then is whether the government might seize the same information if maintained by a third-party. For example, assuming that the suspect used a GPS device on his smart phone permitting his location to be tracked, would the government be permitted to seize that information from the provid-

---

120 *Id.* at 958.
121 *See id.* at 964 (quoting *Knotts*, 460 U.S. at 281-82) (reiterating the limitation on expectations of privacy while driving on public roads).
122 *Id.*
123 *See id.* at 948 (implying that GPS tracking on a vehicle constitutes a violation of the Fourth Amendment).
124 *See Jones*, 132 S. Ct. at 950-52 (illustrating the history of the Fourth Amendment and how it applies to this circumstance).
125 *See id.* at 955-57 (discussing the use of the *Katz* test and trespassory test); *see also id.* at 959, 964 (J. Alito, concurring) (declaring an individual has no reasonable expectation of privacy over information disclosed to third parties).
126 *See Jones*, 132 S. Ct. at 957 (discussing the probable necessity for voluntary disclosure to third parties).
er? The opinion does not address this issue explicitly. But none of the justices, except perhaps Justice Sotomayor, addressed this fundamental issue. The four justices that based their opinion on the trespass cases had no need to address this question; while the four justices that used the Katz test, at least implicitly, through the Stranger Principle, arguably would permit such a seizure. Thus, we have no answer from Jones to the question whether information and material produced through cloud computing enjoys Fourth Amendment protection.

Jones in the Cloud

In most metropolitan areas, police monitor how long a motor vehicle has been parked in a limited parking zone by placing a chalk mark on the tire and ground. Under the Jones’ majority’s reasoning, this practice appears to violate the Fourth Amendment. Placing the chalk mark on the vehicle’s tire appears to constitute a trespass no less than does placing a GPS device on a vehicle’s undercarriage. In City of Sandusky v. DeGidio, the chalk mark was placed on the tire for the express purpose of determining whether the car is parked longer than the two-hour limit. Yet at the time the chalk mark was placed on the tire, there was no reason to think that the car would not be moved within the limit, there was no exigency requiring such an intrusion in order to obtain information about

127 See id. at 949 (illustrating that a GPS device installed on a vehicle is in violation of the Fourth Amendment).
128 See id. at 964 (noting that this opinion does not address if a cell phone’s tracking information can be seized from the provider).
129 See id. at 955 (Sotomayor, J., concurring) (cautioning the government may be able to monitor GPS tracking devices on smartphones).
132 See Jones, 132 S. Ct. at 957 (discussing the principles concluded by the majority’s reasoning).
134 See City of Sandusky, 555 N.E.2d at 680-81 (emphasizing the police officer placed chalk on the defendant’s tire to determine whether vehicles were parked in violation of the city’s two hour limit).
the driver’s movements. In this circumstance, what the government agent did is virtually identical to what the agents did in Jones. But surely the traffic officer’s placing of the chalk mark did not violate the Fourth Amendment. Something is therefore missing from the reasoning in Jones.

What distinguishes the chalk mark from the GPS device is not the officers’ trespass, but what the officers obtained through their trespass. In City of Sandusky, they obtained limited information; that is, information about the period during which an automobile was parked in a zone during a discrete time. In the Jones case, they obtained information about a citizen’s movements and travel for an entire month. That distinction is what drove Justice Alito’s reasoning. He based his conclusion that the Fourth Amendment had been violated on the “expectation …that law enforcement agents and others would not … secretly monitor and catalogue every single movement of an individual’s car for a very long period.”

His use of the word ‘secretly’ in this context may be highly significant. Of course, nowadays, it is expected and, in fact, even encouraged, that certain vendors do monitor and catalogue our movements. That, after all, is a common service that smart phones

135 See id. (reiterating the purpose of placing the chalk on the tire).
136 See Jones, 132 S. Ct. at 948 (describing how the tracking device was placed on the undercarriage of the plaintiff’s Jeep).
137 See Sandusky, 555 N.E.2d at 680-82 (failing to address the constitutionality of the police officer in the holding).
138 See Jones, 132 S. Ct. at 957 (evaluating the different type of information that results from long-term monitoring).
139 See Sandusky, 555 N.E.2d at 680-82 (demonstrating that there was a distinct purpose for the information obtained through the use of the chalk mark).
140 See Jones, 132 S. Ct. at 948 (explaining the length of time in which the agents monitored the vehicle’s movements).
141 See id. at 957 (establishing that his decision in this case was based upon a Fourth Amendment analysis of long-term monitoring).
142 See id. at 964 (Alito, J., concurring) (reasoning that the Fourth Amendment had been violated due to the expectation that the movement of an individual’s vehicle would not be secretly monitored for a long period of time).
143 See id. (stressing the importance of Justice Alito’s use of the word “secretly” in his concurrence).
144 See Mark Stockley, Is Your Smartphone Broadcasting Your Movements When You Shop?, NAKED SECURITY (Oct. 25, 2013), archived at
and other devices incorporating GPS devices provide.\textsuperscript{145} We know, for example, that a certain application might keep track of the roads on which we jog; we know that another application might keep track of the books or newspapers we read; and that another keeps track of the music to which we listen and the websites we visit.\textsuperscript{146} In fact, in many cases, we want this monitoring to occur: it allows us to find more easily jogging routes, books, newspapers, music and websites that fit with our interests and desires.\textsuperscript{147} And so we in fact do expect at least some others to monitor and catalogue our movements — at least we do if we are not naïve about the manner in which the applications we use work.\textsuperscript{148} What distinguishes this circumstance from that at issue in \textit{Jones} is that we have agreed to permit certain vendors to conduct this monitoring and cataloguing in exchange for our receiving certain benefits the vendor provides.\textsuperscript{149} This transaction, however, appears restricted.\textsuperscript{150} By agreeing to permit our vendors to collect information, we have not necessarily also consented to others

\textsuperscript{145} See \textit{id.} (providing that GPS monitoring is a common service provided by smartphones and similar devices).

\textsuperscript{146} See \textit{The #1 Running App, Map My Run} (Sep. 24, 2013), archived at www.perma.cc/0wpcys9Hkdr (describing how Map My Run tracks where someone runs through their mobile device); see also \textit{iBooks by Apple}, \textit{iTunes Preview} (Sep. 24, 2013), archived at www.perma.cc/0DSU14Jt1Mp (providing ways to download and read books using iPhones and iPads); see also \textit{Pandora Radio By Pandora Media, Inc.}, \textit{iTunes Preview} (Sep. 24, 2013), archived at www.perma.cc/0XPHB9aF9o3 (detailing the ways in which the application allows consumers to customize their radio based on their individual music preferences); see also \textit{iPad Built-in Apps, Apple} (Sep. 24, 2013), archived at www.perma.cc/0pwxasmZJs (listing the functions of the web-browser app and consumer’s options to share sites, read articles, and track their browsing history).

\textsuperscript{147} See \textit{iPad Built-in Apps, supra} note 146 (further detailing the benefits to consumers of being monitored).

\textsuperscript{148} See Stockley, \textit{supra} note 144 (concluding that if we use GPS-related applications, there is a reasonable expectation that we are aware we could be monitored).

\textsuperscript{149} See \textit{Jones}, 132 S. Ct. at 958 (explaining respondent’s reasonable expectations of privacy were violated by the four week long monitoring of the movements of the vehicle he drove).

\textsuperscript{150} See Stockley, \textit{supra} note 144 (noting the disadvantages of making ourselves vulnerable to GPS monitoring through WiFi-capable devices).
including the government collecting the same information, even though the Stranger Principle would seem to suggest otherwise.  

In *Smith v. Maryland*, for example, government agents requested a phone company to install a pen register at its central office to record the numbers dialed from the telephone at the defendant’s home.  

The pen registers disclose only the telephone numbers that have been dialed.  

They do not reveal communications or even whether there was a connection.  

The Defendant contended that he had a reasonable expectation of privacy in the phone numbers that he dials.  

This argument was rejected by the court because:

We doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies...

Justices Stewart, Marshall, and Brennan dissented.  

Justice Marshall noted that although the petitioner may have disclosed the number to the company in order to make the call, he did not assume the risk of disclosure to the government.  

He wrote:

---

151 See Rubenfeld, *supra* note 48, at 112 (explaining, hypothetically, that if an individual were given the consent to enter into another individual’s household, the first individual’s natural assumption would be that entry was permitted).

152 See *Smith v. Maryland*, 442 U.S. 735, 737 (1979) (describing installation of pen register to record numbers dialed from the telephone at petitioner’s home).

153 See id. (defining the information gathered from a pen registry).

154 See id. at 741 (explaining the functions of a pen register).

155 See id. at 742 (highlighting the petitioner’s argument that pen registers have limited capabilities therefore, he presumed an expectation of privacy).

156 See id.

157 See *Smith*, 442 U.S. at 746 (Stewart and Brennan, JJ., dissenting); see id. at 748 (Marshall, J., dissenting).

158 See id. at 749 (Marshall, J., dissenting) (describing the privacy expectations of telephone users).
In my view, whether privacy expectations are legitimate within the meaning of Katz depend not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society.159

Despite the dissent’s statement, over the course of time, the Katz test has been used to uphold a variety of types of searches to be outside the Fourth Amendment’s scope.160

In the circumstances in Jones, assuming Jones had a privately operated GPS device, a simplistic application of the third-party rule would eliminate the constitutional protection.161 If data regarding Jones’s travels was already in a third-party’s control, under the reasoning of Smith v. Maryland, it would arguably be entitled to no Fourth Amendment protection.162 By permitting the third-party to have access to that information, the subject assumed the risk, the argument goes, of the information being transmitted by that third-party elsewhere.163 Yet, if that reasoning is accepted, and information in a third-party’s hands is held as sufficient to deprive that information of Fourth Amendment protection, then the distinction between a physical intrusion of a vehicle when chalked and the physical intrusion of placing a GPS under a vehicle in Jones cannot be sustained.164 For purposes of the Fourth Amendment, what was obtained in Jones — data generated by the suspect’s driving for approximately one month — should not even be considered in the analysis.165 It is just as unprotected as what was obtained by the chalk mark — data con-

159 See id. at 750 (quoting Justice Marshall’s dissent).
160 See id. at 740 (applying a Katz analysis to searches outside of the Fourth Amendment’s scope).
161 See id. at 743-44 (applying the concept that there is no constitutional privacy in information when a third party is involved).
162 See Henderson, supra note 133, at 450-51 (discussing the possibility that Jones should be analyzed with the third party analysis rule).
163 See Jones, 132 S. Ct. at 957 (explaining that people voluntarily release information to third parties and can reasonably expect diminished privacy).
164 See Henderson, supra note 133, at 450-51 (illustrating that a third party analysis would change the outcome in Jones).
165 See Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (reasoning that the information of a vehicle’s whereabouts is not an effect).
cerning parking during a discrete period of time.\textsuperscript{166} Moreover, the driver would have no constitutionally protected privacy expectation as to his driving patterns over a month as he has turned that information over to a third-party.\textsuperscript{167} Application of the \textit{Katz} test, in the context of cloud computing, appears to deprive the majority opinion of its rationale in the circumstances where the driver has a private GPS device.\textsuperscript{168}

A desire to avoid this issue may have been the cause of the oddness of \textit{Jones}.\textsuperscript{169} At least four of the justices may have recognized the challenge application of the Stranger Principle poses to the Fourth Amendment, but did not confront it.\textsuperscript{170} Justice Alito’s concurring opinion plainly addressed the issue and applied the \textit{Katz} test to conclude that the government’s warrantless collection of data regarding Jones’ movements over a month violated the Fourth Amendment.\textsuperscript{171} That test, however, in the context of cloud computing threatens to undermine the very privacy interests it is designed to protect.

The \textit{Katz} test was developed as a response to a new technology, in particular, wiretapping.\textsuperscript{172} In \textit{Olmstead}, government agents tapped telephone lines on public streets outside Roy Olmsted’s home and office.\textsuperscript{173} The Supreme Court held that the wiretapping “did not amount to a search or seizure within the meaning of the Fourth

\textsuperscript{166} See Henderson, \textit{supra} note 133, at 450-51 (reasoning that a chalk mark is not within the bounds of the Fourth Amendment).
\textsuperscript{167} See \textit{Smith}, 442 U.S. at 743-44 (suggesting the lack of privacy would exist when a third party obtained vehicle driving sequences).
\textsuperscript{168} See \textit{Jones}, 132 S. Ct. at 952 (explaining the \textit{Katz} test as adding, not substituting, to the common law trespassory test). \textit{But see Katz}, 389 U.S. at 353 (articulating the third party test as possibly controlling over the common law test).
\textsuperscript{169} See \textit{Jones}, 132 S. Ct. at 952 (emphasizing the \textit{Katz} reasonable expectation of privacy test).
\textsuperscript{170} See \textit{id.} at 958 (Alito, J., concurring) (stating the reasonable expectation of privacy test undermines the Fourth Amendment).
\textsuperscript{171} See \textit{id.} at 964 (addressing Justice Alito’s concurring opinion and its application to the \textit{Katz} test).
\textsuperscript{172} See \textit{id.} at 959-60 (illustrating the development of the \textit{Katz} test in response to wiretapping).
\textsuperscript{173} See \textit{Olmstead}, 277 U.S. at 456-57 (describing the taps used on the phones by the agents).
Amendment.” The majority reasoned that the wiretapping did not violate Olmstead’s property rights as “[t]here was no entry of the houses or offices…”

The struggle between the Jones’s opinions reflects the same sort of struggle that led from Olmstead to Katz. The Olmstead majority interpreted the use of a telephone, not as a private instrumentality, but as a public one, analogizing its use to that of a broadcasting device that projects conversations outside the home, just as a radio broadcast or even a megaphone would. Thus, the conversations at issue had as much protection as would conversations that were conducted by the use of, for example, megaphones by neighbors to communicate with each other across a street. Any interest in protecting the content of their conversation was forfeited by virtue of the manner in which it was conducted. Similarly, with the telephone analogized to such a device, any interest in protecting the content of the conspiratorial conversations was forfeited by projecting the discussions outside of the office and home.

With party lines, indeed the initial use of the telephone would be little different from a broadcast and, initially at least, the Olmstead Court’s treatment of the telephone device given that context is not only understandable but, in fact, justified. It does not take long for

---

174 See id. at 466 (deciding that wiretapping did not amount to a search and seizure).
175 See id. at 464 (concluding that there was no effective entry to the houses or offices because there was no searching or seizing, only hearing).
176 See Jones, 132 S. Ct. at 948-64 (reflecting the struggle between the majority and dissenting opinions). Compare Olmstead, 277 U.S. at 466 (describing how wiretapping did not violate the Fourth Amendment), with Katz, 389 U.S. at 360-61 (addressing a physical or electronic intrusion into a reasonable expectation of privacy violates the Fourth Amendment).
177 See Olmstead, 277 U.S. at 466 (describing that the use of a telephone is analogous to broadcasting to the public).
178 See id. (noting that a telephone within the house is not protected by the Fourth Amendment). “The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside.” Id.
179 See id. at 464-65 (explaining that because telephone conversations enter the public domain, they are not protected by the Fourth Amendment).
180 See id. at 466 (stating “…the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment”).
the users of a party line to learn that, if you want to have a private conversation, a party line is not the place on which to conduct it. But, of course, as the use of the telephone was incorporated into our ways of living and private lines became more available, the analogy of a telephone to a megaphone is no longer appropriate. The telephone became part of one of many devices citizens used to conduct private business and communications, becoming more and more akin to the use of conversations in a home or private office, rather than broadcast from home to home. Our way of living evolved to depend upon the private use of phone lines to conduct our affairs, and what the conspirators thought they were doing in Olmstead by conducting their business/criminal affairs over phone lines became in fact what all citizens did — over time the phone lines became devices used for private conversations and were expected to be treated as such.

Seen in this context, the transition from Olmstead to Katz is best understood as a function of the transition of our use of telephones, and in particular, the development of citizens’ use of those devices as part of their private network, rather than as part of a general broadcast. And, the fact that the Olmstead decision was written during this transition explains the tension between the majority’s reasoning and that of the dissenting members, especially Justice Butler’s. This focused more on the agreements, both spoken and explicit, that were developing with respect to the telephone’s use.

181 See id. (providing an example of having a conversation over a party line that resulted in a legal interception of the voices outside the home).
182 See Jones, 132 S. Ct. at 962 (discussing how technology can change expectations of privacy). “Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.” Id.
183 See Olmstead, 277 U.S. at 487 (Butler, J., dissenting) (discussing how telephone conversations are private and privileged).
184 See id. (discussing how telephones are commonly used for transmitting messages concerning personal information with privileged parties).
185 See Katz, 389 U.S. at 352 (describing the expectation of privacy resulting from the new mode of telecommunication).
186 See Olmstead, 277 U.S. at 486-87 (Butler, J., dissenting) (lamenting how the constitutional framing of the issue precluded ethical evaluation and concluding that petitioners deserve a new trial).
187 See id. (noting the evolution of telecommunications and the implicit agreement between private parties).
But, extension of the Katz doctrine and the Stranger Principle to our current use of technology seems inconsistent with the interest underlying the Fourth Amendment. Much of our current use of technology inextricably involves our giving other parties access to personal information that would otherwise be treated as private.\footnote{See Conor Myhrvold, Study Reveals a Confused View of Mobile Phone Privacy and Security, MIT TECH. REV. (Aug. 3, 2012), archived at www.perma.cc/U6P7-VWWX (stating many cell phone users’ perception of private information in the public realm).} For example, technologies used to dictate memos or other items often involve the transmission of voice recordings to a vendor’s server which, using its voice recognition software, transcribes the recording into a memo that is emailed or otherwise transmitted to the user.\footnote{See David Talbot, Wiping Away Your Siri “Fingerprint,” MIT TECH. REV. (June 28, 2012), archived at www.perma.cc/0KhT3Jaoh1Y (describing how voice recognition software transcribes the user’s speech and stores the data on Apple’s servers).} Email accounts, of course, are stored on separate servers.\footnote{See Eric Kangas, Understanding Email Services: What Are They and What Do You Need?, LUX SCIENTIAE, archived at www.perma.cc/06x5ZdXis11 (describing how email messages travel through intermediate servers and arrive at the recipient’s server).} Additionally, a wide range of individual data involving purchases, internet searches, and communications are made through and maintained by third-parties.\footnote{See id. (explaining that the increased use of cellular and smart phones allows information about one’s whereabouts to be accessible by third parties).} And, of course, the ever increasing use of cellular and smart phones gives access to information regarding our movements to third-parties.\footnote{See id. (describing the idea that developments in technology have led to what was once private information being exposed to the public).} All of these developments involve our giving access to information to others that we otherwise expect to remain private.\footnote{See id. (articulating that through a Fourth Amendment perspective, unprotected information cannot reasonably be expected to remain private).} Current Fourth Amendment jurisprudence, therefore, could treat all this information as unprotected, as a simplistic application of the Stranger Principle entails that information put into a third-party’s hands is not intended to, nor reasonably expected to be, maintained as private.\footnote{See id. (articulating that through a Fourth Amendment perspective, unprotected information cannot reasonably be expected to remain private).} But that appears wrong. The security protected by the Fourth Amendment should include the security of
the data we generate, whether we permit that data to be held by and collected by a third-party, or whether we hold it and collect it ourselves.\textsuperscript{195} In fact, most of us do not have the resources to collect such data or effects. If the Fourth Amendment is to have application in the modern world, we must understand it in a manner that applies to our current use of technology.\textsuperscript{196} Such an understanding may be derived from looking closer at Justice Butler’s dissent in \textit{Olmstead} and considering cloud computing in the context of a Lockean theory of property.\textsuperscript{197} Such an approach may not only be more consistent with the original intent of the Amendment, but may as well provide cloud computing with the constitutional protection it deserves.\textsuperscript{198} But before turning to that issue, we need to address one other.

\section*{Section III}
\textbf{The Tangible vs. Intangible Dilemma}

One might argue that information extraction and acquisition is different from acquisition of resources within the scope of the Fourth Amendment.\textsuperscript{199} Information that is acquired, it might be contended, is an intangible resource, rather than a tangible one, and therefore, it might be argued, the Fourth Amendment has no application.\textsuperscript{200} It protects the security of “persons, houses, papers, and effects,” which are tangible, while information is not.\textsuperscript{201} The view derives from the notion that “persons, houses, papers, and effects” are tangible items,

\textsuperscript{195} See id. (declaring that the Fourth Amendment should protect any data we develop regardless of our security interests).
\textsuperscript{196} See Goldman, \textit{supra} note 191 (alleging that the protections of the Fourth Amendment should be interpreted in a way that is up to date with modern technology).
\textsuperscript{197} See \textit{Olmstead}, 277 U.S. at 487-88 (Butler, J. dissenting) (reaffirming that the scope of the Fourth Amendment should not be limited to the literal meaning of its words, and modern technology should be afforded its protections).
\textsuperscript{198} See id. at 488 (Butler, J. dissenting) (discussing the original purposes of the Fourth Amendment).
\textsuperscript{199} See Paul Ohm, \textit{The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property}, 2008 STAN. TECH. L. REV. 2, 3-5 (arguing that a re-conception of the seizure clause is needed to address the advent of intangible resources).
\textsuperscript{200} See id.
\textsuperscript{201} See U.S. CONST. amend. IV (listing tangible items secured by the Fourth Amendment).
having a spatiotemporal location,\textsuperscript{202} and is bolstered by the view that the second clause of the Amendment requires that a warrant describe “the place to be searched and the persons or things to be seized.”\textsuperscript{203} Katz, of course, rejected the notion that the Fourth Amendment controls only the seizure of tangible items, and expressly extended Fourth Amendment protection to the recording of oral statements, overheard without any “technical trespass…under local property law.”\textsuperscript{204} Thus, searches need not be only of tangible items, but of content, or data, as well.\textsuperscript{205} But underlying this reasoning was the idea that there was an expectation of privacy by the individual, something which we have seen leads to the Stranger Principle.\textsuperscript{206} If we are prepared to jettison that Principle, we must find another basis for treating data as property within the scope of the Amendment.

In other contexts, courts have found that data is tangible, material property.\textsuperscript{207} For example, the United States Copyright Act defines “copies” as “material objects … and from which the work can be perceived, reproduced or otherwise communicated either directly or with the aid of a machine or device.”\textsuperscript{208} The issue has arisen as to whether copyright infringement occurs by loading computer software from read only memory to random access memory.\textsuperscript{209} The general

\begin{itemize}
  \item \textsuperscript{202} See \textit{id.}; see also Alderman v. United States, 394 U.S. 165, 179 (1969) (suggesting that “papers” and “effects” are tangible property).
  \item \textsuperscript{203} See \textit{Katz}, 389 U.S. at 365 (Black, J. dissenting) (“The first clause [of the Fourth Amendment] protects ‘persons, houses, papers, and effects’…. These words connote the idea of tangible things with size, form, and weight, things capable of being searched, seized, or both”).
  \item \textsuperscript{204} See \textit{id.} at 353 (emphasizing that Fourth Amendment protection should be afforded to the recording of oral statements in addition to tangible items).
  \item \textsuperscript{205} See \textit{id.} (affirming that Fourth Amendment protections do not apply exclusively to tangible items but also to data).
  \item \textsuperscript{206} See \textit{id.} at 360-61 (Harlan, J. concurring) (providing that the core reason data is afforded Fourth Amendment protection is due to the reasonable expectations of privacy held by individuals).
  \item \textsuperscript{207} See ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996) (holding that software and data are “fixed in a tangible medium of expression” and “within the subject matter of copyright”).
  \item \textsuperscript{208} 17 U.S.C. § 101 (2013).
  \item \textsuperscript{209} See MAI Sys. Corp. v. Peak Computer, 991 F.2d 511, 519 (9th Cir. 1993) (presenting the issue of the occurrence of copyright infringement when loading computer software from read only memory to random access memory).
\end{itemize}
rule is that it does. Because random access memory is temporary and eliminated once power to the computer is turned off, defendants have argued that the copy is not a “material object” “from which the work can be perceived….” But this argument has been rejected. For example, the Ninth Circuit has held:

[I]t is generally accepted that the loading of software into a computer constitutes the creation of a copy under the Copyright Act.…[S]ince we find that the copy created in the RAM can be “perceived, reproduced, or otherwise communicated,” we hold that the loading of software into the RAM creates a copy under the Copyright Act.

There may be something initially plausible about treating data as intangible — after all, it does not matter what particular hardware stores our data, so long as it can be accessed when we want it. But the reasoning is fundamentally flawed and arguably should not be followed; to see why, we need to consider on a general level what a computer is and does. For example, a computer can be seen as a device that has many on/off switches and manipulates them exceptionally quickly so that data becomes a state of these on/off switches. Data is in a fundamentally physical state, not an intangible one, even if we might store the same data through different configurations of the on/off switches.

Imagine a device with eight slots that can contain one marble each. If a marble is in a slot, we say the slot is on; and, if the slot is empty, we say it is off. For ease of reference, let’s call the first slot “0,” the second “1,” and so on, with the eighth slot called “7.” We

\footnotesize

210 See id. at 518 (holding that copyright infringement does in fact occur when loading computer software from read only memory to random access memory).
211 See id. at 517-18 (presenting Peak Computer, Inc.’s argument to the Court that random access memory is temporary and not a “material object”).
212 See id. at 518 (determining that software loaded into random access memory is “fixed” for purposes of copyright law).
213 Id. at 519.
215 See id. (providing a similar explanation of binary information storage).
can physically design this device, perhaps using spring releases so that if a marble of a certain weight is dropped into a slot that contains a marble, both marbles will pop out of that slot with one of them dropping into the next highest numbered slot, if such a slot exists. So, for example, if we drop a marble into slot 5, the marble will stay there if slot 5 was empty, and, if there was already a marble in slot 5, the new marble will pop into slot 6 and the old marble discarded from the device. Then, if slot 6 was empty, the marble will stay there, and otherwise, the new marble in slot 6 (that is, the old one from slot 5) will be dropped into slot 7. If slot 7 has a marble, both will be dumped from the device. Let’s call this device a “marble byte.” We might, moreover, combine more marble bytes together in a fashion that has marbles leaving the slot 7 of one device to go into the slot 0 of another. For instance, we might put 16 of these devices together, each device labeled “0”, “1”, “2”, “3”, “4”, “5”, “6”, “7”, “8”, “9”, “A”, “B”, “C”, “D”, “E”, and “F” and set them up so that when a marble drops out of slot 7 of device 8, that marble is dropped into slot 0 of device 9, and similarly, when a marble is dropped out of slot 7 of device 9, a marble is dropped into slot 0 of device A, and so on. We can call this conglomeration of marble bytes “marble words” and store information.

Now, if we store information in this device, we are doing no more than establishing a physical arrangement of the marbles. And if somehow or another, we had stored the number 9 in a marble byte as described two paragraphs back and someone took it from us, we would conclude that something tangible had been taken. When we store the number 9, we drop marbles into slots – that is a physical, tangible operation, just as putting ink to paper is. It is because of the efforts of thousands of researchers over hundreds of years that we can replace that ink and paper with other tangible devices that are astromically more efficient at storing information and performing computations.216

We could eventually put as many of these devices together as we wanted and construct different sorts of mechanisms for having marbles transfer from slots to slots and bytes to bytes. If we were, for

instance, to put together one billion of these marble bytes, we would have created a giga-marble byte, in effect a hard-drive with one gigabyte of capacity, for treating our marble slots each as a bit, with eight of them forming a byte and the 16 forming a word.\textsuperscript{217} We can also imagine that if certain slots contain a marble, the device’s method of transferring marbles is changed.\textsuperscript{218} For instance, say we have marble bytes 0, 1, 2, and 3 and that the device is designed so that if byte 3 contains no marbles, bytes 0, 1, and 2 operate as described before; but, if a marble appears in slot 1 of byte 3, then when a marble is put into slot 7 of byte 1 and that slot already contains a marble, then one marble is transferred to slot 0 of byte 0 and another is transferred to slot 0 of byte 2.\textsuperscript{219} Different configurations of bytes would, in this device, lead to different methods of transferring marbles from slot to slot.\textsuperscript{220} In principle, we could create an enormous marble device that is programmable and that could do (although much slower and using much more space) any computation that could be done by a modern digital computer.\textsuperscript{221} It is the failure to appreciate that there is little principled difference (ignoring size and speed) between what we can do with marbles and what we can do with charges that may lead to the notion that data is not tangible.

That information is tangible property protected by the Fourth Amendment is supported by \textit{Boyd v. United States},\textsuperscript{222} which protected information in an invoice.\textsuperscript{223} That case involved seizure of an in-

\begin{footnotesize}
\begin{enumerate}
\item See \textit{MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY} 528 (11th ed. 2007) (defining gigabyte). One gigabyte is equal to one billion bytes. \textit{Id.}
\item See Lon Berk, \textit{CBI for the Cloud}, 21 A.B.A. COMM. INS. LITIG. COVERAGE 1, 7 (2011), archived at www.perma.cc/0N97GDiafNy (noting how the method of transferring marbles can change).
\item See \textit{id.} (describing marble example).
\item See \textit{id.} (explaining different configurations of bytes).
\item See \textit{id.} (providing functions of an enormous marble device). This is a consequence of Church’s thesis, which roughly is that any type of computation device developed will perform precisely the same set of computations as any other type. \textit{Id.} at n.15; see also Amir M. Ben-Amram, \textit{The Church-Turing Thesis and its Look-Alikes}, 36 ACM SIGACT NEWS 113, 113-14 (Sept. 2005), archived at www.perma.cc/CSH9-3C7R (referencing Church’s axiom but contrasting as to implications for modern computing software codes).
\item 116 U.S. 616 (1866).
\item See \textit{id.} at 638 (concluding the required notice to produce an invoice in the case was unconstitutional and void).
\end{enumerate}
\end{footnotesize}
voice.\textsuperscript{224} By statute the defendant was obligated to produce it.\textsuperscript{225} The court held that that was an unreasonable search and seizure, distinguishing between contraband, in which the government had a possessory interest, and the invoice relating to that contraband, to which only the defendant had a possessory interest, and held that the latter could not be seized absent warrant.\textsuperscript{226} Thus, it seems appropriate to conclude that data is property protected by the Fourth Amendment.

Section IV

Locke, Butler and the Cloud

Given the acceptance of data as property protected by the Fourth Amendment, we still need some basis for treating the warrantless seizure of such property as a violation of the Amendment.\textsuperscript{227} Locke had a theory of the creation and acquisition of property that may have application to cloud computation in a manner that provides a way out of the \textit{Jones} dilemma; very roughly, he viewed the world as consisting of resources that initially belong to everyone in common.\textsuperscript{228} Individuals are then able to appropriate portions of these resources for their own private use even if this is done without the consent of all, or even anyone.\textsuperscript{229} The manner through which this is done is by mixing one’s labor with the world’s resources.\textsuperscript{230} Once the individual mixes his or her labor with a resource, the resource becomes that individual’s property and it is set off from the com-

\textsuperscript{224} See id. at 618 (describing claimant’s production of the invoice).
\textsuperscript{225} See id. at 617-18 (mentioning defendant’s statutory obligation to produce the invoice).
\textsuperscript{226} See id. at 638 (describing the law which authorized production of the invoice as unconstitutional).
\textsuperscript{228} See \textit{John Locke, Second Treatise of Civil Government}, Ch. V., § 25 (Thomas Hollis ed., 1764) (describing universal commonality of property and resources).
\textsuperscript{229} See id. at § 26 (arguing that individuals must claim common resources for themselves).
\textsuperscript{230} See id. at § 27 (setting forth the premise that individual labor creates a right of exclusivity to the labored resource).
mons. Only the individual or individuals that mixed their labor with the property are entitled to use it, even though it was derived from the common, which all initially had the right to use.

This very roughly is Locke’s labor theory of acquisition. It derives from the view that each person has ownership over his or her body and labor and therefore acquires a right to what is part of the common by mixing his or her own body and labor in the extraction of what was held in common. Thus, the private ownership or dominion over one’s body and labor overcomes the common interest in the resource. Thus, for example, we imagine that arable land is a part of the commons. Individuals that fence off a portion of the land, plow it, plant it, irrigate it and generally develop it so that eventually they harvest a crop, under Locke’s theory, have a property right not only in that land that they used their labor to develop, but in the crop that they harvest.

We can use such a theory to analyze the accumulation of information in a database. Information is the resource being “harvested” by the mixing of labor by the owners and users of data. For instance, let us consider a map application such as one that might have been at issue in Jones. The user/client enters an address, is provided directions, and the server retains the client’s locations.
Eventually, as more transactions occur, the server has a database from which it can determine such things as which stores people at certain locations are likely to visit, or which movie theaters, or restaurants.\textsuperscript{240} It might also be able to determine that certain clients prefer certain kinds of stores, or theaters.\textsuperscript{241} It can then advise such clients when they are near such stores, or theaters, provide information about businesses of the sort the client prefers in his or her location, and provide focused advertising to that client.\textsuperscript{242} Under this model, both the clients and the server profit from this arrangement; the client obtains directions and useful information and the server obtains revenue.\textsuperscript{243}

Seen in Lockean terms, we can interpret these transactions as follows; the clients and server are extracting information; they are “mixing their labor”-the clients through entering location searches, the server through providing locations -and thereby developing a database, which, seen in this way is their “effect,” and is therefore entitled to protection.\textsuperscript{244}

Through cloud computing providers are able to utilize private efforts for collecting locational data.\textsuperscript{245} For example, those using mobile devices with GPS, permit the provider to collect information about their travels.\textsuperscript{246} In exchange, they receive valuable computation services from the provider, including access to data on points of interest in the vicinity of the consumer at various times, and emergency road service.\textsuperscript{247} We can look at this as an agreement under

\textsuperscript{240} See Macisaac, \textit{supra} note 85 (asserting capability of GPS to target people in small areas).
\textsuperscript{241} See Macisaac, \textit{supra} note 85 (discussing the targeted advertising campaigns run by GPS-friendly locator devices).
\textsuperscript{242} See Macisaac, \textit{supra} note 85 (describing how the GPS location can be used for advertising).
\textsuperscript{243} See Macisaac, \textit{supra} note 85 (describing the perceived potential of companies to use location orientated advertisements to their advantage).
\textsuperscript{244} See Locke, \textit{supra} note 228, at § 27 (describing how applying labor to something that exists in nature creates property of the laborer).
\textsuperscript{245} See Macisaac, \textit{supra} note 85 (stating user’s capability to supply location data to providers).
\textsuperscript{246} See Macisaac, \textit{supra} note 85 (reaffirming device-level GPS use supplies location information to providers).
\textsuperscript{247} See Macisaac, \textit{supra} note 85 (stating value to end user in finding points of interest).
which the labor of the cloud vendor and the cloud consumer are combined to extract information that is of use to both parties from the raw information in its uncollected form.  

If we were to put this into the Lockean format, we might describe the circumstance as follows. Information exists in the natural world in a form that is only of use if extracted through the labors of individuals. The fact that the information has been extracted through their labor gives them a right to consume that information and to use it for their purposes. But that fact also gives them the right to exclude others from using the information collected as well, as it is only through the use of one’s own labor that the information may be set-off and supplied separately.

Seen in this context, a search or seizure of information by a government agent should be treated no differently from a search or seizure of any other natural resource acquired from the world through the use of individuals’ labor. While it is merely a technological innovation that permits us to acquire information on the scale that we have done through cloud computing, its acquisition is no different from any other acquisition. The information is no different from any other effect of a person’s labor and should be treated, for purposes of the Fourth Amendment, exactly as any other property.

---

248 See Locke, supra note 228, at § 27 (building on Locke’s theory of entangling labor and common property).
249 See Locke, supra note 228, at § 27 (applying Locke’s labor theory of acquisition to cloud computing).
250 See Locke, supra note 228, at § 28 (comparing cloud computer labor with transformation of common property).
251 See Locke, supra note 228, at § 28 (applying the individual right to exclude to the collection of electronic data).
252 See Locke, supra note 228, at § 27 (reasoning that information is segregated because of individual labor).
253 See Boyd, 116 U.S. at 633 (private property is entitled to protection under the Fourth Amendment); see also Locke, supra note 228 (stating that individual labor gives individual claim to property).
254 See Couillard, supra note 6, at 2220 (arguing that intangibles are akin to personal property).
255 See Couillard, supra note 6, at 2220 (reasoning that there is an expectation of privacy in cloud computing).
This approach is not without precedent\textsuperscript{256}. Although \textit{Katz} is often seen as arising from the reasoning of an \textit{Olmstead} dissent, there was another dissent in \textit{Olmstead} that urged a different approach to the Amendment’s application\textsuperscript{257}. In his \textit{Olmstead} dissent, Justice Butler had reasoned that

\begin{quote}
[t]he contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between whom they pass. During their transmission the exclusive use of the wire belongs to the persons served by it. Wire-tapping involves interference with the wire while being used. Tapping the wires and listening in by the officers literally constituted a search for evidence. As the communications passed, they were heard and taken down.\textsuperscript{258}
\end{quote}

Justice Butler thus focused, not on the individual expectations of privacy, but on the agreements among parties that permitted telephonic technology to be used\textsuperscript{259}. Such a view of the technology would have placed the government’s eavesdropping squarely at odds with the language of the Fourth Amendment providing that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…”\textsuperscript{260}. In Justice Butler’s analysis, through contract, the telephone company and its users had established an “effect,” admittedly one not present (and which could not be present) in 1787, but an effect nonetheless\textsuperscript{261}. It was something owned by the company and user and, as such, something that should have been directly protected as secure against an unreasonable search and seizure\textsuperscript{262}. Nonetheless, instead

\begin{itemize}
\item \textsuperscript{256} See \textit{Katz}, 389 U.S. at 353 (holding electronic interception of phone conversations violates the Fourth Amendment).
\item \textsuperscript{257} See \textit{Olmstead}, 277 U.S. at 487 (Butler, J., dissenting) (interpreting Fourth Amendment protections broadly to include telephone conversations).
\item \textsuperscript{258} Id.
\item \textsuperscript{259} See \textit{id}. (arguing that contracts between telephone companies and users envision an expectation of privacy).
\item \textsuperscript{260} U.S. CONST. amend. IV.
\item \textsuperscript{261} See \textit{Olmstead}, 277 U.S. at 487 (Butler, J., dissenting) (interpreting contract between telephone companies and telephone users).
\item \textsuperscript{262} See \textit{id}. (pulling contracts within the purview of the Fourth Amendment).
\end{itemize}
of adopting Justice Butler’s view of the technology and the relationships between the user and provider, the Supreme Court in *Katz* adopted the reasonable expectation of privacy test, more in line with Brandeis’ dissent; that test, as we saw, is ill-suited to address many of the technologies upon which we presently rely.263 These would be better served by adopting a version of Butler’s view.264

**Conclusion**

In sum, as cloud computing increases and the technology becomes more and more incorporated into our private and public lives and affairs, the strain uncovered by *Jones* will become more and more evident. Among other things, it has most recently led to opposing views of the NSA’s surveillance.265 Returning to principles underlying Locke’s theory of acquisition and Justice Butler’s *Olmstead* dissent may point the way to resolve this strain and allow Fourth Amendment jurisprudence to address computation and data in the cloud. Such a view would protect both the innovations of technology and the fundamental liberty underlying constitutional values.

---

263 See *Katz*, 389 U.S. at 352 (delineating the expectation of privacy test).
264 See *Olmstead*, 277 U.S. at 487 (Butler, J., dissenting) (concluding that classifying the contract as an effect would provide better Fourth Amendment protection in the digital age).