# Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs

Bryce Clayton Newell[1] and Joseph T. Tennis[1]
[1] University of Washington

**Abstract**
After Edward Snowden leaked classified intelligence records to the press in June 2013, government metadata surveillance programs – and the risk that large-scale metadata collection poses to personal information privacy – has taken center stage in domestic and international debates about privacy and the appropriate role of government. In this paper, the authors approach these questions by drawing upon theory and literature in both law and archival studies. This paper concludes that, because metadata surveillance can be highly intrusive to personal privacy – even more revealing in certain regards than the contents of our communications in some cases – and that certain types of metadata are inextricably linked with the records of our digitally mediated lives, legal distinctions that draw a line between communications "content" and metadata are inappropriate and insufficient to adequately protect personal privacy.
**Keywords:** privacy, surveillance, law, metadata, archival studies
**Citation**: Newell, B. C., & Tennis, J. T. (2014). Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs. In *iConference 2014 Proceedings* (p. 345–355). doi:10.9776/14109

**Acknowledgements**: The authors wish to thank Adam D. Moore for his comments and suggestions on a previous draft of this work, as well as the anonymous iConference reviewers for their insightful comments on the initial submission.
**Contact**: bcnewell@uw.edu, jtennis@uw.edu

## 1 Introduction

Surveillance in public spaces is becoming increasingly common, whether through state or privately-owned closed circuit surveillance cameras, location tracking made possible by GPS chips embedded in virtually all cellular phones and many other electronic devices, license plate recognition systems, or even by cameras wielded by many of the average people on the street and built into ubiquitous technologies like phones, tablets, and computers (Moore, 2010; Rushin, 2011). In the public spaces of the Internet, our communications, browsing histories, buying patterns, and information about our social networks are subject to acquisition by government agents for law enforcement or national security purposes. In our modern society, public spaces are increasingly laden with organizational surveillance, where corporations, organizations, or governments are the surveillance agents, and non-organizational forms of surveillance carried out by individuals (Marx, 2005). Virtually all of this surveillance encompasses metadata, or information about the various bits of digital information being created to document our public or private lives, and much of this information is being ingested into, and stored in large electronic databases that are shared with government agents and marketing companies interested in mining information about us – including the attendant metadata – to achieve their respective mandates.

Recent revelations about covert government surveillance practices in the United States, and in allied countries like Canada and the United Kingdom, have vigorously renewed public discussions about information and communication privacy. Because of the nature of the surveillance practices at issue, and the legal frameworks undergirding government action, many of these discussions have specifically focused on whether a person can maintain a legitimate expectation of privacy in metadata – or so-called "non-content" information – attached to their electronic activities such that the targeted (or even incidental) acquisition of related metadata by government agents should be subject to heightened legal protections. In

the United States, our presence in a public space (including online spaces) has generally equated to a waiver of any legally enforceable right to privacy for anything we do or say in those places – or in information about our physical location – on the premise that such information has been voluntarily disclosed to third parties by virtue of our very presence in public itself.

In this paper, we critically examine the proposition that government access to metadata should be subject to lesser legal standards than the actual content of interpersonal communications (i.e., the actual words spoken or written by the parties to a communication). We draw upon theory and literature in both law and archival studies, as well as judicial reasoning in relevant legal decisions of U.S. courts. More specifically, we argue that because metadata surveillance can be highly intrusive to personal privacy – even more revealing than the content of our communications in some cases – and that certain types of metadata are inextricably linked with the records of our digitally mediated lives (MacNeil, 2002), legal distinctions that draw a line between content and metadata are inappropriate and insufficient to adequately protect personal privacy. Of course, metadata will not generally give insight into the actual words spoken (or typed) in a communication (and thus, in this sense, is less revealing), but it may likewise reveal information that the contents might not, such as the frequency of communication between two individuals or other patterns of communication. As such, metadata can be very revealing, and even more so than the actual contents if what NSA analysts are concerned about is generally calling patterns, connections, and actual contact information (all contained in communications metadata). The high evidentiary value of metadata to government law enforcement and national security intelligence operations does provide a counterpoint to our argument. To deny law enforcement certain surveillance powers solely because of their efficacy is likewise inapt.

However, that critique is misguided and misses the point of our central thesis. Under the Constitutional commitments in the United States to personal liberty from government intrusion, including the Fourth Amendment's prohibition on unwarranted search and seizure of personal information by government agents, metadata that is inextricably linked to our digital records must be subject to the same protections as the records themselves, such as the contents of our communications. Because modern technology has "changed the game" (Moore, 2010) by removing barriers to access and utilize the personal information of others, the law should similarly adapt and protect informational privacy when there are legitimate reasons to do so.

## 2 Metadata

Metadata is most commonly defined as "information about information," or "data about data." For our purposes metadata is human and machine readable assertions about resources. In our case, resources are records in the archival sense, and so come with them particular expectations about metadata. In the context of electronic communications, metadata includes information about the time, duration, and location of a communication as well as the phone numbers or email addresses of the sending and receiving parties. It also may include information about the device used (make/model and specific device identification number). Metadata is generated whenever we use electronic devices (such as computers, tablets, mobile phones, landline telephones, and even modern automobiles) or services (such as email clients, social networks, word processing programs, and search engines). Many of these activities generate considerable amounts of information (metadata) about our usage of these devices or services. In most cases, service providers collect and retain this information in databases that often can be traced directly to an individual person. The migration of those messages to other systems also generates metadata, depicting the provenance of the files as they are copied from one server to another.

For example, when a person makes a telephone call from a personal phone, electronic records are created and stored (by the service provider and/or on the device itself) that indicates the phone number called, the time the call was made, and the length of the call. Information is also created and stored about

the physical location of the device when the call was made. With cellular phones, location can be fairly accurately acquired through a variety of methods, including GPS, cell tower triangulation, and the presence of nearby WiFi signals (cf. Constandache, et al, 2010). Landline phones, computer initiated calls, and cellular phone calls made over WiFi signals can also often be tracked precisely, due to known locations of landline connections and Internet IP addresses. For purposes of email, metadata might include the time sent, the address of the recipient(s), the size of the file, the existence and size of attachments, and the text entered into the subject line of the email itself. The header, visible or invisible to the reader is also part of the metadata.

But metadata is not just associated with electronic *communications*, it also serves to document various properties of other facts, documents, or processes. For example, automated license plate recognition systems create metadata about the locations of vehicles at certain points in time. Taking a digital photograph often creates metadata about the location the photograph was taken, the aperture, focal length, and shutter speed settings of the camera. Word processing programs such as Microsoft Word can also save metadata such as the name of the author who created the document, the date of creation, the date on which the latest changes have been made, the name of the user who made the most recent changes, the total number of words and pages in a document, and the total length of time that a document has actually been edited (meaning: an employer could know exactly how much time an employee spent writing and editing a memo).

## 3 Metadata and Surveillance after Edward Snowden

After Edward Snowden leaked classified National Security Administration (NSA) documents to the press in June 2013, questions about the nature of government collection of communications metadata took a prominent place on the world stage. Snowden's first revelation was a classified court order from the secretive U.S. Foreign Intelligence Surveillance Court (FISC) that compelled Verizon, one of the largest U.S. telecommunications providers, to provide the U.S. government with all of its customers' telephone metadata on an ongoing basis – encompassing landline, wireless and smartphone communications. Other disclosures indicate that virtually all of the major U.S. telecommunications companies were subject to similar orders.

In a Congressional hearing, top U.S. officials claimed that they were only collecting information about numbers of the parties to communications (the sender and receiver of phone calls) and the duration of the calls. NSA and Justice Department officials, and high-ranking Congressional representatives, also claimed that since they were not collecting the actual contents of communications (e.g. the words spoken), the surveillance did not invade anyone's reasonable expectations of privacy. The officials claimed explicitly that they were not collecting geolocation data (e.g. the location of the device when the call was made or received), but nothing in the FISC order limited the government from obtaining this kind of information as well. Importantly, the U.S. authorities are legally restricted from collecting the actual contents of Americans' communications under the U.S. Constitution (although, as recent practice disclosed in the aftermath of Snowden's disclosures indicates, this may not mean as much in practice). However, government agencies are legally permitted to collect the contents (and metadata) of non-U.S. persons around the world without any prior judicial authorization.

If the evidentiary value of a record in the digital environment is defined by its metadata, then we have something that is inextricably linked to the record. Without metadata we do not have the record – we do not have evidence that is forensically sound and authentic. As in the cases mentioned above, record-level metadata is about dates, persons, and locations (MacNeil, 2002). Without these we have no authentic evidence, but we can also argue that collection dates, names of persons, and locations is a violation of privacy. That is: the context is content.

## 4 Problems with Binary Fourth Amendment Theory

Legal definitions of privacy in the Fourth Amendment search context have often been crafted to force conclusions about potential privacy violations based on binary distinctions: either a form of investigation or information gathering by government agents constitutes a search or it does not (Kerr, 2013). The binary nature itself is not problematic – in fact it may be highly desirable. However, certain strict application of the third-party doctrine and the public/private dichotomy may improperly restrict Fourth Amendment protections of personal privacy.

Traditional trespass-based decisions, recently reinvigorated by the Supreme Court's decision in *United States v. Jones* (2012), have determined whether a search has occurred on the basis of whether a property interest has been infringed by a government agent. The two-pronged *Katz* reasonable expectations of privacy test (which requires that 1) an individual must have exhibited a subjective expectation of privacy and, 2) that the expectation must be one that society is prepared to recognize as reasonable or legitimate) (Katz v. United States, 1967), despite the allure (or dangers) of its "hypothetical reasonable person" standard, has failed to modernize in pace with investigative technologies used by law enforcement around the country and remains subject to binary distinctions of legal significance. Fourth Amendment law is riddled with binary distinctions granted legal significance by the courts, including the public/private dichotomy and the third-party doctrine (or the idea that once information is released to any third-party, privacy interests *vis-à-vis* the government, when acquiring the information from the third-party, are waived).

Indeed, despite calling for empirical evidence (at least on its face) of societal expectations of privacy when examining the constitutionality of criminal investigations conducted by government agents, this hypothetical reasonable person has rarely (if ever) been a stand-in for relevant social science research on what members of the contemporary society actually expect(ed) (see Blumenthal, et al, 2009); rather courts have applied the test as a proxy for the work of social scientists and socio-legal scholars. It has been suggested that the prevalence of binary dichotomies in Fourth Amendment case law is a consequence of courts (and lawyers) attempting to find "easy lines to draw in court" (Selbst, 2013). However, the difficulties faced by the courts to apply the *Katz* test uniformly, problematic application of the third-party doctrine in cases involving government use of emerging technologies, and a resounding call by commentators that Fourth Amendment legal theory is in chaos (and has been for some time), suggest that the lines may not be as easy to draw at all. Perhaps the time has come to rethink Fourth Amendment theory and reduce the legal significance of some of the problematic binary distinctions that have plagued court decisions for years, such as certain applications of the third-party doctrine that would lessen the privacy interests in certain types of metadata.

In light of the opinions of the Justices in *Jones*, which signal the possibility that a majority of the Justices might be open to revisiting Fourth Amendment theory in light of modern technologically-aided police practices (Kerr, 2013), we argue for advancing a normative approach to privacy in Fourth Amendment jurisprudence that is sensitive to context (not bound by purely binary distinctions) and the increasingly revealing capacity of metadata surveillance, especially when such information is collected, stored, and mined in the aggregate.

## 5 Defining and Defending Privacy

Throughout this paper, we define informational privacy as the right to control access to and uses of personal information (Moore, 2010; 2007). This definition explicitly recognizes that individuals should have some rights to control not just access to personal information, but also some subsequent uses of that information (Moore, 2010), even after disclosure to third parties in certain circumstances. This definition will be informed by the mosaic theory of the Fourth Amendment (the idea that multiple searches for information by government agents, even if each is justified on its own, may become unjustified under the Fourth

Amendment by virtue of the greater intrusion made possible by aggregating and analyzing the information as a larger set, which may reveal patterns and sensitive information not obtainable through any individual search and potentially not relevant to the purposes of the individual searches themselves) recently considered in the wake of recent decisions in the *United States v. Jones* (2012) and *United States v. Maynard* (2010). This version of the mosaic theory, adopted from federal practices attempting to balance disclosing documents to the public under the Freedom of Information Act (FOIA) while preserving national security interests, is premised on the idea that any individual piece of information is generally less useful than when combined with other pieces of information. We argue that a person's right to limit access to and use of certain personal information (e.g. a person's current or past geographic location) that has not been kept strictly "secret" (by virtue of the fact that is was available in a public space) should still, in some circumstances, remain legally enforceable under the Fourth Amendment's guarantee of freedom from unreasonable search or seizure.

In essence, we are arguing for a right to privacy in certain information (specifically metadata that forms an essential part of a record about an identifiable individual) that, when viewed discretely or in the aggregate is generally not qualitatively or quantitatively available to the public at large (or, as Judge Ginsburg of the Circuit Court for the District of Columbia phrased it, such information is not *actually* or *constructively* exposed to the public (United States v. Maynard, 2010)). The aggregation of the metadata associated with our electronic communications and digital records of our physical movements over a substantial time period allows law enforcement to easily discover information that is both qualitatively and quantitatively different than what is knowingly and voluntarily exposed to the public at large, even though it is (in essence) just an aggregation of distinct bits of information individually exposed to the public. Tracking a person's cell phone or logging their Internet browsing patterns also allows the government to track individuals while they are inside a private building or in the sanctity of their homes – distinctly private information.

In this pursuit, we will examine the proposition made by Justice Sotomayor in *Jones* that the time has come to rethink the legal significance of allowing a third party access to personal information when considering privacy interests in public spaces. By restricting the third-party rule in our Fourth Amendment analysis, such that any release of information to a third party is not necessarily a complete and total waiver to all forms of access and use by anyone at all, we respect the drastic changes in technological possibilities and their proper role in government investigations while maintaining checks on improper abuse of authority.

## 6 The Third Party Doctrine

The third-party doctrine has been described as "the Fourth Amendment rule scholars love to hate" (Kerr, 2009). For years, it has been subjected to voluminous amounts of criticism, both by legal scholars and state courts (Kerr, 2009). The Supreme Court has upheld the rule, holding that citizens "assume the risk" that what they disclose to a third party will be transferred on to the government, but has not explicitly defended it (Kerr, 2009). And now, after *Jones*, criticism of the rule has reached the Supreme Court itself.

In its early years, the third-party doctrine was applied in cases involving undercover agents and confidential informants (Kerr, 2009). These cases held that defendants could not claim Fourth Amendment violations based off of conversations with government agents – sometimes wearing wires – because the "the Fourth Amendment does not protect 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it'" (Kerr, 2009, *quoting* Hoffa v. United States, 1966). In later cases, the Court applied the doctrine to business records. In *United States v. Miller* (1978), the Supreme Court held that a bank depositor does not have any reasonable expectation of privacy in financial information (in the form of deposit slips, checks, and bank records) because such information was conveyed voluntarily to the bank and "exposed to their employees in the ordinary course of business." As such, the court found that,

> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.... [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed" (United States v. Miller, 1978).

In her concurrence in *United States v. Jones* (2012), Justice Sotomayor stated that the time had come for Fourth Amendment jurisprudence to discard the premise that legitimate expectations of privacy could only be found in situations of near or complete secrecy. Sotomayor argued that people should be able to maintain reasonable expectations of privacy in some information voluntarily disclosed to third parties. The opposite and historical view of the court, Sotomayor stated, was "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" (United States v. Jones, 2012). Sotomayor considered that logs of phone calls, text messages, websites visited, email correspondence, purchase histories from online retailers, and geolocational information were all forms of information that were technically disclosed to third parties through mundane tasks, but where such disclosure should not constitute waiver of all privacy interests (United States v. Jones, 2012). "[W]hatever the societal expectations," Sotomayor stated, these forms of information

> "can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection" (United States v. Jones, 2012).

If one purpose of the Fourth Amendment's warrant requirement is to prevent government agents from engaging in fishing expeditions then the third-party doctrine, when applied to aggregate collection and mining of metadata, would clearly frustrate the original purpose and intent of the Amendment itself.

As stated by Justice Sotomayor, the situation with prolonged geolocational tracking is different precisely because the technological surveillance "evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'" (United States v. Jones, 2012, *citing* Illinois v. Lidster, 2004) and allows the government to obtain personal information about individuals that is qualitatively and quantitatively different in kind than what would be discovered alternatively. The likelihood that, in the case of physical tailing, such a time consuming and resource intensive investigation would be carried out regularly without a sound basis is very small. Police are very unlikely to devote such time and resources to this kind of visual surveillance except in cases that really warrant it. On the other hand, the ease and convenience of obtaining records from wireless providers could allow government agents virtually unfettered ability to conduct this sort of surveillance in a wide variety of cases, including "fishing expeditions" not based on any level of suspicion (probable cause or otherwise).

However, this position could potentially limit some important investigations from proceeding as efficiently as they might have based purely on departmental lack of resources to conduct extensive visual surveillance. But requiring a warrant, based on affirmation of probable cause, before allowing government agents to collect and analyze such extensive digital information, should not be a serious impediment to most investigations and would help restrict this sort of surveillance to legitimate investigations. Additionally, other exceptions to the Fourth Amendment's warrant requirement, such as the emergency doctrine (United States v. Goldenstein, 1972; Roberts, 1975), would continue to ameliorate these concerns in practice when time is of the essence.

However, by limiting a strict application of the third-party doctrine, new questions emerge about where lines should be drawn between permissible and impermissible tactics in other contexts. For example, what are the important differences (if any) between aggregating geolocational information, bank records, "private" communication or messages on a social network like Facebook, web browsing or search histories,

or electronic purchase histories collected and archived over time? The mosaic theory, originally announced by Judge Ginsburg in *United States v. Maynard* (2010), may begin to help us sort out these difficult questions.

## 7 Public Surveillance, the Mosaic, and the Fourth Amendment

Some scholars have claimed that recent (and even not so recent) advances in digital technologies and surveillance capabilities mean that we should rethink whether we can maintain any legitimate expectations of privacy while out in public – or in "public facts." In *United States v. Jones* (2012), Justice Sotomayor proposed that the third-party doctrine should be abandoned (or at least rethought) in the face of confronting Fourth Amendment challenges related to investigative use of new technologies. Justice Alito's separate concurrence in that case expressed concern about the robustness of the "reasonable expectations of privacy test" – even while advocating its use in that case – because of the potential that the widespread use of new surveillance technologies could resign the populace to subjectively expect less privacy than should be afforded under the Constitution (United States v. Jones, 2012).

Indeed, geolocational tracking technologies – which have now been used by law enforcement agencies for some time – allow law enforcement to easily compile thousands of pages of information about our present and past travels – in very exacting detail – and to mine that information indiscriminately for patterns (in *United States v. Jones* (2012), for example, prosecutors presented over 2,000 pages of data about Jones's location over a 28 day period sourced from a physical tracking device installed in the rear bumper of a vehicle Jones regularly drove). The NSA's metadata surveillance practices, recently exposed to greater scrutiny by Edward Snowden, allow the government to conduct similar analysis with the calling and communications histories of everyday citizens, even those not suspected of committing any crime.

Courts have also clearly stated that Fourth Amendment law has failed to keep pace with advancing technological possibilities. In one recent Ninth Circuit case, the court stated:

> "The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored" (Quon v. Arch Wireless, 2008).

In *United States v. Maynard (*2010) (the predecessor Court of Appeals decision to *United States v. Jones* (2012)), the judge held that the government violated the suspects' Fourth Amendment rights when they tracked a vehicle for 24 hours a day over a 28 day time-period. Importantly, while announcing the "mosaic theory", the court found that:

> "…unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil… [and] the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts" (United States v. Maynard, 2010).

The court compared this case of prolonged modern surveillance with prior national security cases where the government regularly invoked the "mosaic theory" to shield certain otherwise public records from disclosure under the Freedom of Information Act because, "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene" (United States v. Maynard, 2010, *citing* CIA v. Sims, 1985). This concern was later voiced loudly by the Justices in the Supreme Court's decision in *United States v. Jones* (2012), which upheld the decision of the Circuit Court (but on trespass grounds, rather than under the *Katz* reasonable expectations of privacy test).

Combining the third-party doctrine with the modern realities of massive data collection possible because of the ubiquitous nature of contemporary communications devices means that location data, even historical data, is becoming much easier for law enforcement to obtain without the need to secure a warrant supported by probable cause, even without planting physical devices and risking committing physical trespass. Indeed, the police in *Jones* did obtain historical geolocation information from Jones's wireless provider, but chose to rely on the data collected through a physical tracking device installed on Jones's vehicle during the trial. The present ability of law enforcement to so easily amass and mine such enormous amounts of personal information through simple technological tools and coordination with service providers (such as wireless service providers, email providers, or social network service providers) begs an examination of current Fourth Amendment theory, the reasonable expectations of privacy test, and the third-party doctrine.

## 8 Finding a Legal Basis for Metadata Privacy

Since Justice Harlan announced a two-part test in a concurring opinion in *Katz v. United States* (1967) in 1967, whether or not a person maintains a right to privacy – for Fourth Amendment search purposes – is based on whether any subjective expectation of privacy maintained by the individual asserting the privacy interest is "one that society is prepared to recognize as reasonable" (Katz v. United States, 1967). Generally in the United States, courts have found that information released to the public could not be the subject of any legitimate expectation of privacy under this test. From 1967 until the *United States v. Jones* (2012) decision in 2012, the reasonable expectation of privacy test largely succeeded the prior focus on whether the government has violated a property right, such as by committing trespass, in conducting a search. Justice Scalia's majority opinion in *United States v. Jones* (2012), however, reinvigorated the trespass doctrine for searches where physical trespass had occurred, while allowing for the continued use of the *Katz* test when non-trespassory interests are allegedly violated.

Despite the radical shift that some of the dicta in the *United States v. Jones* (2012) decision might indicate for future of Fourth Amendment doctrine, Justice Sotomayor's call for greater protections for some activity occurring in the public sphere is not the first time the idea has been suggested in the courts. In the *Katz v. United States* (1967) decision itself, Justice Stewart stated that

> "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" (Katz v. United States, 1967).

In that case, the government had placed a listening device to the exterior of a public phone booth, and had recorded the defendant making phone calls. The court found that Katz maintained a reasonable expectation of privacy in his conversations while inside the phone booth, even though it was in a public place, because the court felt that

> "…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*" (Katz v. United States, 1967).

The court continued it's "discrediting" of the view that only trespass could raise constitutional questions, elaborating that

> "…once it is recognized that the Fourth Amendment protects people – and not simply 'areas' – against unreasonable searches and seizures, it becomes clear that the reach of that Amendment

> cannot turn upon the presence or absence of a physical intrusion into any given enclosure" (Katz v. United States, 1967).

Reading this language alongside Sotomayor's concurrence in *United States v. Jones* (2012), parallels begin to emerge. The expectation that shutting the glass door to a public phone booth makes the conversation private is entirely consistent with the proposition that emails sent to an associate, purchase histories shared only with the online merchant, geolocational information shared only with a cellphone service provider, or a social networking status update visible only to a select groups of friends (due to actively setting and maintaining privacy settings to ensure such limited publication), could also be considered legitimate contexts where a reasonable expectation of privacy vis-à-vis the government could adhere (Newell, 2011).

However, the historical reliance on the third-party doctrine would presumably discredit these otherwise reasonable expectations merely because the information was disclosed to an intermediary (Google, Facebook, Verizon, T-Mobile, Amazon) or a select group of friends. Thus, the government is free to demand and subpoena this information from these intermediaries without obtaining a warrant or attesting in court to probable cause. However, the "vital role" that the public telephone played in facilitating private communication (even in public spaces) in 1967 has been superseded by a variety of electronic wireless communications technologies (cell phones, email, text messaging, and private messaging on social media websites) that also collect and transmit a wealth of data (such as geographic coordinates) that find no easy corollary in the *Katz* analogy.

Some lower federal courts have begun to question a strict application of the third-party doctrine as well. In 2010, the Sixth Circuit addressed the question of whether the government violated the Fourth Amendment when agents compelled an ISP to turn over the contents of the defendant's emails without first obtaining a warrant (United States v. Warshak, 2010). In that case, the Sixth Circuit held that, even though the subscriber agreement allowed the ISP to access the contents of its clients' emails in certain circumstances, "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy" (United States v. Warshak, 2010). The court found that this conclusion was consistent with the *Katz v. United States* (1967) holding, because the telephone service company in the prior case also had a legal right to listen to phone calls in certain cases.

The *United States v. Warshak* (2010) court also differentiated the facts in that case from those in *United States v. Miller* (1978), because the third-party ISP was merely an intermediary rather than the intended recipient (as the bank was in *Miller*). Under the rationale in this case, the government could not demand the information from the intermediary corporation or service provider, but the conclusion would not necessarily extend to information released by the recipients of the communication, such as the email recipient or Facebook friend. Whether this was the right result, or merely a step in the right direction, remains the subject of some controversy. However, as evidenced by the recent indication by the five concurring justices in *United States v. Jones* (2012) (Sotomayor was the most explicit, but Alito's opinion can also be read this way) that they may be willing to rethink Fourth Amendment theory (Slobogin, 2012), the time may be ripe for further challenges to precedent. Indeed, the fact that the *United States v. Jones* (2012) decision followed from the introduction of the mosaic theory in the lower court's decision signals that the justices may be willing to entertain this issue in coming years.

The recognition of the Court in *Katz v. United States* (1967) itself of this relationship between the Fourth Amendment, private communications, and technological change, provides ample support for the proposition that these new forms of private communication (and the variety of additional opportunities they provide, both to government and individuals) should be carefully protected as well, preserving the idea that new technologies should receive carefully considered protections under the Fourth Amendment.

## 9 Conclusion

In archival science, context is everything. Metadata provides essential context for many records, especially digital records created by electronic communications and the use of digital devices like smartphones, computers, and tablets. Context, as provided by metadata, is vital to the authenticity of these records. Without understanding where a record originated (when, by whom, where) by reference to certain metadata attached to that record, we cannot claim evidentiary or forensic authenticity – we want to understand the authenticity of a document so that we might understand the original act or fact. That context, in the form of metadata, is *for the most part* inextricably linked to the digital record, means that a record does not properly exist (in an authentic state) without the metadata.

Artificial legal distinctions between the content of electronic communications and the associated metadata do not properly respect the essential connection between these two sources of data. These distinctions also obscure the reality that large-scale metadata surveillance and data-mining provide government agents with personal information about peoples' communications that are often just as revealing as the actual words spoken – the "content" of a communication. Because metadata surveillance can be highly intrusive to personal privacy and because certain types of record-level metadata (including dates, persons, and locations) are inextricably linked with the records of our digitally mediated lives, legal distinctions that draw a line between communications "content" and metadata are inappropriate and insufficient to adequately protect personal privacy. The law should account for these deficiencies, and protect record-level metadata with the same protections as content – making metadata surveillance requests subject to judicial authorization under the Fourth Amendment's warrant requirement. After all: the context is content.

## 10 References

Blumenthal, J.A., Adya, M., and Mogle, J. (2009). The Multiple Dimensions of Privacy: Testing Lay 'Expectations of Privacy.' *University of Pennsylvania Journal of Constitutional Law, 11*, 311-374.

CIA v. Sims, 471 U.S. 159 (1985).

Constandache, I., Choudhury, R.R., & Rhee, I. (2010). *Towards Mobile Phone Localization without War-Driving.* Paper presented at the Proceedings of 2010 IEEE INFOCOM Conference, 14-19 March, San Diego, CA. doi: 10.1109/INFCOM.2010.5462058.

Hoffa v. United States, 385 U.S. 293 (1966).

Illinois v. Lidster, 540 U.S. 419 (2004).

Katz v. United States, 389 U.S. 347 (1967).

Kerr, O.S. (2009). The Case for the Third-Party Doctrine. *Michigan Law Review, 107*, 561-601.

Kerr, O.S. (2012). The Mosaic Theory of the Fourth Amendment. *Michigan Law Review, 111*, 311-354.

MacNeil, H. (2002). Establishing and Maintaining Trust in Electronic Records: The Final Report of the Authenticity Task Force. In *The Long Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, pp. 1–33 and appendices 1 and 2.

Marx, G.T. (2005). Surveillance and Society. In G. Ritzer (ed.), *Encyclopedia of Social Theory.* Thousand Oaks, CA: SAGE Publications.

Moore, A.D. (2007). Toward Informational Privacy Rights. *San Diego Law Review, 44*, 809-846.

Moore, A.D. (2010). *Privacy Rights: Moral and Legal Foundations.* University Park, PA: Penn State Press.

Newell, B.C. (2011). Rethinking Reasonable Expectations of Privacy. *Richmond Journal of Law and Technology, 17*, art. 12, 1-62.

Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008).

Roberts, M. (1975). The Emergency Doctrine, Civil Search and Seizure, and the Fourth Amendment. *Fordham Law Review, 43*, 571-589.

Rushin, S. (2011). The Judicial Response to Mass Surveillance. *University of Illinois Journal of Law, Technology & Policy, 2011(2)*, 281-328.

Selbst, A.D. (2013). Contextual Expectations of Privacy. *Cardozo Law Review, 35*, ___ (forthcoming 2013).

Slobogin, C. (2012). Making the Most of Jones v. United States in a Surveillance Society: A Statutory Implementation of Mosaic Theory. *Duke Journal of Constitutional Law & Public Policy, 8*, 1-37.

United States v. Goldenstein, 456 F.2d 1006 (1972).

United States v. Jones, 132 S. Ct. 945 (2012).

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

United States v. Miller, 425 U.S. 435 (1978).

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