NSA METADATA COLLECTION & STORAGE: AN INTERNMENT CAMP FOR CITIZENS' "EFFECTS"

David J. Robinson* & Julia Kaye Wykoff**

I. INTRODUCTION

James Madison, one of the architects of the Bill of Rights, said at the Federal Convention of 1787 that "[t]he means of defence agst. foreign danger, have been always the instruments of tyranny at home."[1] This statement may seem overstated in the context of metadata collection, but this admonishment has shown itself prescient over the last two hundred years.

Take, for example, President Franklin Delano Roosevelt's Executive Order 9066 issued little more than a year after the United States declared war on Japan. To protect the homeland from attacks like the one perpetrated at Pearl Harbor, Executive Order 9066 permitted United States military commanders to "prescribe military areas" from which all persons could be excluded or ordered to remain "subject to whatever restrictions" were established by those military commanders.[2] The stated rationale for Executive Order 9066 was "protection against espionage and against sabotage to national-defense material, national-defense premises, and national-defense utilities."[3] The result, of course, was internment of Americans citizens of Japanese ancestry.[4]

---

* David J. Robinson is the Deputy Director of the Fourth District and Acting Deputy Director of the Fifth District at the Illinois State's Attorneys Appellate Prosecutor's Office in Springfield, Illinois. David also teaches legal studies at Robert Morris University where he serves on the University's Advisory Board. He has authored numerous statewide and national publications.

** Julia Kaye Wykoff is an Assistant Appellate Prosecutor at the Illinois State's Attorneys Appellate Prosecutor's Office, Fourth District, in Springfield, Illinois. Julia graduated *magna cum laude* from Southern Illinois University School of Law in December 2014 where she served on the SIU Law Journal Board of Editors.

1. 1 James Madison, THE RECORDS OF THE FEDERAL CONVENTION OF 1787, 354 (Max Farrand ed., 1911) (ebook) (summarizing a speech by James Madison delivered on Friday, June, 29, 1787).
2. Korematsu v. United States, 323 U.S. 214, 227 (1944) (Roberts, J., dissenting).
3. *Id.*
4. *Id.* at 248 (Jackson, J., dissenting) (explaining of the government's evacuation and detention program that the Supreme Court may not be "asked to execute a military expedient that has no place in law under the Constitution.").

Today, we are faced with a less facially compelling, but potentially equally repugnant, Constitutional trespass: internment of citizens' personal property, their metadata.[5]

Under the Fourth Amendment, all persons have the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," which means citizens have the right to be free from warrantless government intrusion, or "trespass," into their persons, houses, papers, and effects.[6] We understand persons, houses and papers, but what exactly are "effects"? The Supreme Court of the United States recently explained that personal property, such as one's vehicle, constitutes an effect under the Fourth Amendment.[7] The court has also recently implied that citizens' cell-phone data constitutes an effect for purposes of Fourth Amendment analysis.[8] Thus, left unexplored, at least explicitly, by the court is whether citizens' metadata is an effect within the meaning of the Fourth Amendment. These authors posit that it is.

The National Security Administration (NSA) has been under fire for its compilation of American citizens' metadata in an attempt to target and eradicate terrorism, both abroad and domestically; this, admittedly, is a noble endeavor, but so was protecting the United States from Japanese espionage. This article examines whether the metadata collected and stored by the NSA is an "effect" within the meaning of the Fourth Amendment. These authors believe that it is and that such bulk collection—if conducted without consent, exigent circumstances and probable cause, or a warrant—is a trespass that implicates the Fourth Amendment.

To get there, however, we examine first the background of the NSA's metadata collection and storage program. We then turn to the Supreme Court's decision in *United States v. Jones*, and how the *Jones* analysis applies to the NSA's metadata collection program. After suggesting a four-pronged analytical approach, we then explain why the NSA's metadata collection program constitutes a trespass to citizens' effects. Having done so, these authors conclude that warrantless collection and storage of such data—absent consent, exigency coupled with probable cause, or some other accepted exception to the warrant requirement—trespasses on a protected category under the Fourth Amendment.[9]

---

5. *Metadata* is the detail about a telephone call, including, for example, the length of the call, the phone number from which the call was made, and the phone number of the phone that received the call. ACLU v. Clapper, 785 F.3d 787, 793 (2d Cir. 2015).
6. U.S. CONST. amend. IV.
7. United States v. Jones, 132 S. Ct. 945, 949 (2012).
8. *See* Riley v. California, 134 S. Ct. 2473 (2014).
9. In so doing, we do not conclusively opine as to whether, for example, signing contracts of adhesion provide sufficient consent or whether a Foreign Intelligence Surveillance Act (FISA) Court order is a sufficient substitute for a traditional warrant.

II. BACKGROUND

We turn first to an examination of the NSA's metadata collection and storage program.

A. The NSA's Metadata Collection and Storage Program

Initially, we note that because only part the NSA's metadata collection and storage program has just recently been declassified, we do not know the full extent of the program. What we do know, however, is that it involves, *inter alia*, "bulk collection by the government of telephone metadata created by telephone companies in the normal course of their business but now explicitly required by the government to be turned over in bulk on an ongoing basis."[10] This telephone data does not appear to include voice content, but instead includes specific details about interactions engaged in by telephone—for example, the length of a call, the phone number called, information as to the type of equipment used to make the call, and routing numbers (which can convey information about a caller's location).[11] This data, when compiled in bulk can reveal "civil, political, or religious affiliations; [it] can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships."[12] As the United States Court of Appeals for the Second Circuit, has noted, the more data the government collects and analyzes, "the greater the capacity for such [data] to reveal ever more private and previously unascertainable information about individuals."[13] This is particularly concerning, given that "it is virtually impossible for an ordinary citizen to avoid creating metadata about himself on a regular basis simply by conducting his ordinary affairs."[14]

The NSA relies on section 215 of the USA Patriot Act[15] to obtain orders from the Foreign Intelligence Surveillance Act Court ("FISA Court").[16] Those orders authorize common carriers, such as telephone companies (e.g., Verizon and AT&T) to provide the NSA "on an ongoing daily basis . . . all call detail records or 'telephon[e] metadata'" created by

10. ACLU v. Clapper, 785 F.3d 787, 793 (2d Cir. 2015).
11. *Id.* at 793–94.
12. *Id.* at 794.
13. *Id.*
14. *Id.*
15. 50 U.S.C. § 1861(a)(1) (2012).
16. The FISA Court was originally established by the Foreign Intelligence Surveillance Act, which authorized the use of electronic surveillance to gather foreign intelligence information for periods of up to one year without a court order under certain circumstances. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783. The USA PATRIOT Act substantially revised section 215 by expanding the scope to include both "business records" and "any tangible things," and also expanded the reach of section 215 by eliminating restrictions on the types of businesses subject to FISA Court orders. *Clapper*, 785 F.3d 787, 795 (2d Cir. 2015).

those companies for communications (1) between the United States and abroad, as well as (2) wholly within the United States, "including local telephone calls."[17] Put another way, the order from the FISA Court authorizes the NSA to order telephone companies to "produce call detail records, every day, on *all* telephone calls made through its systems or using its services where one or both ends of the call are located within the United States."[18] The government's justification for this is, of course, that it is required to ferret out terrorist activity by searching across data to locate "contacts of contacts."[19]

Having outlined the NSA's metadata collection and storage program, we turn to the Supreme Court's opinion in *United States v. Jones*, which resurrected the trespass-to-property approach to Fourth Amendment jurisprudence.

B. The Trespass-to-Property Approach in Fourth Amendment Jurisprudence

In *United States v. Jones*, the Supreme Court held that the attachment of a Global Positioning System (GPS) tracking device to Jones' vehicle, and subsequent use of that device to monitor that vehicle's movements on public streets, constituted a search under the Fourth Amendment.[20] The government, according to the *Jones* majority, ran afoul of the Fourth Amendment when it "physically occupied private property for the purpose of obtaining information."[21] In other words, the government engaged in an unconstitutional *search* when it trespassed to his *effect*—namely, his vehicle—without a warrant.

---

17. *Clapper*, 785 F. 3d at 795 (quoting *In re* FBI for an Order Requiring the Production of Tangible Things, No. BR 13-80, 2013 WL 5460137, at ¶ 1 (FISA Ct. 2013).
18. *Id.* at 796.
19. *Id.* at 797

> The government explains that it uses the bulk metadata collected pursuant to these orders by making "queries" using metadata 'identifiers' (also referred to as 'selectors'), or particular phone numbers that it believes, based on 'reasonable articulable suspicion,' to be associated with a foreign terrorist organization. The identifier is used as a 'seed' to search across the government's database; the search results yield phone numbers, and the metadata associated with them, that have been in contact with the seed. That step is referred to as the first 'hop.' The NSA can then also search for the numbers, and associated metadata, that have been in contact with the numbers resulting from the first search—conducting a second 'hop.' Until recently, the program allowed for another iteration of the process, such that a third 'hop' could be conducted, sweeping in results that include the metadata of, essentially, the contacts of contacts of contacts of the original 'seed.' The government asserts that it does not conduct any general 'browsing' of the data.

Id. (internal citations omitted).

20. United States v. Jones, 132 S. Ct. 945 (2012).
21. *Id.* at 949.

Law enforcement had suspected Jones of narcotics trafficking.[22] The government applied to the United States District Court for the District of Columbia for a search warrant to attach a GPS tracking device to Jones' wife's vehicle.[23] The court issued the warrant, specifying "installation of the device in the District of Columbia and within 10 days."[24]

On the 11th day, agents installed the GPS tracking device to Jones' vehicle while it was parked in a public parking lot.[25] The government tracked his vehicle for the next 28 days, and used information garnered by the tracking device to indict him.[26] Jones moved to suppress all the evidence obtained through the GPS tracking device.[27] The trial court granted his motion in part and denied it in part,[28] suppressing all data gathered when Jones' vehicle was parked in the garage adjoining his home.[29] However, the court found that all other evidence 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."[30] Jones was later convicted following a jury trial.[31] The United States Court of Appeals for the District of Columbia reversed.[32]

The Supreme Court granted the government's writ of certiorari to determine whether the GPS monitoring of Jones' vehicle constituted a "search" within the meaning of the Fourth Amendment.[33] The Court first analyzed the pertinent language of the Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[34] The Court concluded that it was "beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment."[35]

Having so concluded, the Supreme Court held that the attachment of the GPS tracking device was a "search," relying on accepted concepts of property law dating back to the mid-18th century.[36] The Court noted that:

> [O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without

22. *Id.* at 946.
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.* (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).
31. *Id.* at 949.
32. *Id.*
33. *Id.*
34. *Id.*
35. *Id.* (citing United States v. Chadwick, 433 U.S. 1, 12 (1977)).
36. *Id.* at 949 (citing Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765)).

> his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law.[37]

The Supreme Court explained that Fourth Amendment jurisprudence had long been tied to common law trespass,[38] adding that Fourth Amendment analysis had merely expanded in the twentieth century.[39] In *Katz v. United States*, the Court began to recognize that the Fourth Amendment primarily protected "people, not places."[40] In the aftermath of *Katz*, the Court moved away from the property based analysis, focusing instead—at least primarily—on the citizen's "reasonable expectation of privacy."[41] Although the court never extinguished a property based Fourth Amendment analysis, the reasonable expectation of privacy standard took center stage throughout much of the 20th century.

Picking up on this trend in *Jones*, the government argued that Jones' reasonable expectation of privacy was not violated, because his vehicle was operated on public roadways.[42] The Supreme Court, however, disagreed, drawing on the aforementioned property based roots of the Fourth Amendment.[43] In resurrecting the property based approach, the Court explained that *Katz* did not eradicate the property based approach, but rather added additional protection to citizens.[44] The *Jones* majority pointed to its 1969 holding in *Alderman v. United States*, in which the Court held that it "[did not] believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home."[45]

Undaunted, the government further posited that the Supreme Court's 1983 ruling in *United States v. Knotts* was controlling.[46] In *Knotts*, the government had placed a "beeper" in a barrel of chloroform to track its movements.[47] The *Knotts* Court held that "there had been no infringement of Knotts' reasonable expectation of privacy since the information obtained—the location of the automobile carrying the container on public roads, and the location of the off-loaded container in open fields near

---

37. *Id.* (citing Entick v. Carrington, 95 Eng. Rep. 807, 817 (C.P. 1765)).
38. *Id.*
39. *Id.*
40. *Id.* at 950 (citing Katz v. United States, 389 U.S. 347, 351 (1967)). In *Katz*, defendant's Fourth Amendment rights were violated when the government attached an eavesdropping device to a public telephone booth. *See* Katz v. United States, 389 U.S. 347, 351 (1967).
41. *Id.* (citing *Katz* 389 U.S. at 360).
42. *Id.*
43. *Id.*
44. *Id.* at 952.
45. *Id.* at 951 (citing Alderman v. United States, 394 U.S. 165, 180 (1969)).
46. *Id.* at 951 (citing United States v. Knotts, 460 U.S. 276, 278 (1983).
47. *See* United States v. Knotts, 460 U.S. 276, 278 (1983).

Knotts' cabin—had been voluntarily conveyed to the public."[48] The *Jones* majority found this argument unpersuasive, given that the *Knotts* majority relied on the defendant's expectation of privacy, noting that "[t]he *Katz* reasonable-expectation-of-privacy test ha[d] been *added to*, but not *substituted for*, the common-law trespassory test."[49] And because no *trespass* had occurred in *Knotts*—unlike in *Jones*—the government had not run afoul of the Fourth Amendment.

The government also relied on another so-called "beeper" case, *United States v. Karo*.[50] *Karo*, according to the Supreme Court, was distinguishable, however, because the beeper in *Karo* was installed prior to the defendant's possession of the container.[51] The court explained as follows: "Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location."[52] In contrast, Jones "possessed the [property—a vehicle—] at the time the government trespassorily inserted the information-gathering device[.]"[53] Hence, the unconstitutional government trespass.

In following this property-based approach, the majority in *Jones* concluded that the government unconstitutionally "physically occupied private property for the purpose of obtaining information."[54] The court further concluded, therefore, that Jones' Fourth Amendment rights had been violated when the government attached a GPS monitoring device to his vehicle—an "effect"—and used information from the device to monitor his movements.[55]

Having (1) outlined the NSA's bulk data collection process, and (2) established that the "reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test,"[56] we turn to whether the NSA's metadata collection and storage program implicates the Fourth Amendment as a trespass to American citizens' effects. As part of this analysis, we begin by demonstrating how the Supreme Court has applied the property based, trespass analysis to each of the specific Fourth Amendment categories: persons, houses, papers, and effects.

---

48. Jones, 132 S. Ct. at 951–52 (citing *Knotts*, 460 U.S. at 281–82).
49. *Id.* at 952 (emphasis added).
50. *Id.*
51. *Id.* (citing United States v. Karo, 468 U.S. 705 (1984)).
52. *Id.*
53. *Id.*
54. *Id.* at 949.
55. *Id.* at 946.
56. *Id.* at 952 (emphasis added).

III. ANALYSIS

To be clear, the determination of whether a trespass to a protected Fourth Amendment category has occurred is merely a sub-part of one prong of a four-pronged analysis that must be undertaken when deciding whether a violation of the Fourth Amendment has occurred. These four prongs, which these authors urge should be used whenever a court is analyzing these metadata cases, are as follows:

> (1) Has the Fourth Amendment been activated?[57] That is, has there been some government action?[58] If so:
> (2) Has the government engaged in an unreasonable "search" or "seizure" of a person, house, paper, or effect?[59] That is, has there been a trespass to one of these protected categories in order to obtain information,[60] or has the government run afoul of a citizen's reasonable expectation of privacy? If so:
> (3) Did the government obtain a particularized warrant authorizing it to engage in the search or seizure?[61] That is, has the government obtained written authorization from a detached third-party magistrate particularly describing the places (or persons) to be searched and items (or persons) to be seized?[62] And, if not:
> (4) Does some exception to the warrant requirement exist?[63] That is, did the government have (a) consent, (b) exigent circumstances

---

57. For purposes of this article, we assume government action, recognizing that third parties are initially collecting the data, but apparently do so at the direction of the government.
58. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (explaining the Fourth Amendment applies only to government action; a search by a private person does not violate the Fourth Amendment—indeed, the Fourth Amendment does not prohibit the government from using information discovered by a private search, because the private search has already frustrated any expectation that the information will remain private).
59. As previously stated, we limit the analysis here to trespass.
60. *See* Jones, 132 S. Ct. at 961, n. 5 (a "trespass" only implicates the Fourth Amendment when a "meaningful interference" with property occurs, which means that a trespass is not a "search" unless it is done by the government to "obtain information").
61. Although we do not squarely address the issue here, we note that the FISA Court orders authorizing this metadata collection look more like the type of general warrant the Fourth Amendment was designed to prevent, than the particularized warrant envisioned by the Founders.
62. *See* Katz v. United States, 389 U.S. 347, 357 (1967).
> "Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.

Id. (citations omitted)
63. Although we do not squarely address this issue either, we point out that (a) much of the metadata in question may be subject to a release signed as part of an adhesion contract that was part of the setup agreement with the cellular service provider and (b) such metadata may be subject to warrantless review under particularized exigencies.

> and probable cause, or (c) a particularized national security interest?[64]

One other point before proceeding to our analysis under the second prong of the aforementioned approach: these authors do not, and need not, address whether the NSA's metadata collection program violates citizens' right to privacy under the Fourth Amendment. That analysis runs parallel to, although it sometimes overlaps, the trespass analysis.[65] The right-to-privacy analysis is unnecessary, when—as we posit has occurred under the NSA's metadata program—a trespass to an "effect" has occurred for the purpose of obtaining information. At the moment the government-sanctioned trespass occurs in order to obtain information, however brief or slight so long as unreasonable, the Fourth Amendment is implicated.[66] We use the term "implicated" advisedly in this context, given that we do not endeavor to answer the ultimate question: "Is the NSA's metadata collection and storage program Constitutional?" Instead, we seek only to convince the reader that the metadata collected and stored is an "effect" that has been trespassed upon by the government for the purpose of obtaining information.

To that end, we begin with a review of Fourth Amendment cases involving government trespass to demonstrate how ensconced the property rights approach is in Supreme Court jurisprudence. The property rights approach is, as the following cases reveal, separate from the oft-used reasonable expectation of privacy test, but is also used as a corollary. To put it another way, the tests are often applied separately, but occasionally the tests overlap, given that the property rights approach is rooted in protection of individual rights and liberty.[67]

A. Trespass to Persons, Houses, Papers, or Effects Runs Afoul of the Fourth Amendment

"[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas

---

64. *See e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 219, (1973) (consent); Payton v. New York, 445 U.S. 573, 589, (1980) (exigent circumstances); and United States v. Ramsey, 431 U.S. 606, (1977) (national security).

65. *See* Terry v. Ohio, 392 U.S. 1 (1968); Riley v. California, 134 S. Ct. 2473 (2014).

66. *See* United States v. Jones, 132 S. Ct. 945, 961, n. 5 (2012) (noting that a "trespass" only implicates the Fourth Amendment when a "meaningful interference" with property occurs, which means that a trespass is not a "search" unless it is done by the government to "obtain information").

67. *See id.* at 949 ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizure'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous"). *Id.*

('persons, houses, papers, and effects') it enumerates."[68] This is reflected in the Supreme Court's precedent.

1. Trespass to "Persons"

In the landmark decision, *Terry v. Ohio*, the Supreme Court was tasked with determining whether a "stop and frisk," what we now know as a "*Terry stop*," was reasonable under the Fourth Amendment.[69] The majority concluded that it was.[70] As part of its analysis, however, the court extolled the virtues of the Fourth Amendment's protections against trespasses to the person: "This inestimable right of personal security belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of secret affairs."[71] The court continued, citing its predecessor court from 1891: "No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."[72]

2. Trespass to "Houses"

In *Florida v. Jardines*, the Supreme Court considered whether law enforcement officers' warrantless use of a drug-sniffing dog on the front porch of Jardines' home was a violation of the Fourth Amendment.[73] Based on the dog's positive alert, officers had obtained a warrant to search Jardines' home.[74] Upon entering the home, officers discovered that Jardines was growing cannabis inside.[75]

The Supreme Court analyzed Jardines' Fourth-Amendment claim as a trespass to property under *Jones*, rather than under the reasonable expectation of privacy test from *Katz*.[76] The court explained as follows: "At the Fourth Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[77] Because the officers entered into the curtilage of Jardines' home (a recognized part of a citizen's home), namely, his

68. Jones, 132 S. Ct. at 950.
69. Terry, 392 U.S. at 4.
70. *Id.* at 31.
71. *Id.* at 8–9.
72. *Id.* at 9 (quoting Union Pac. R. Co. v. Botsford, 141 U.S. 250, 251 (1891)).
73. Florida v. Jardines, 133 S. Ct. 1409 (2013).
74. *Id.* at 1411.
75. *Id.*
76. *Id.* at 1412 ("It is unnecessary to decide whether the officers violated Jardines' expectation of privacy under Katz v. United States . . . ."). *Id.*
77. *Id.* at 1414 (citing Silverman v. United States, 365 U.S. 505, 511, (1961)).

porch, for the purpose of obtaining information, the "investigation of Jardines' home was a 'search' within the meaning of the Fourth Amendment."[78]

3. Trespass to "Papers"

In *Ex Parte Jackson*, Jackson had petitioned the Supreme Court for writs of habeas corpus and certiorari, seeking his release after being sentenced to jail until he could pay a $100 fine imposed by a New York court.[79] Jackson had been convicted under a federal statute for "knowingly and unlawfully depositing . . . in the mail of the United States . . . a circular concerning a lottery offering prizes, enclosed in an envelope . . . ."[80] The court denied Jackson's writ but, in so doing, noted as follows: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[81] The court continued, "[w]hilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household."[82]

4. Trespass to "Effects"

In *Riley v. California*, the Supreme Court considered whether the search of a cell phone was lawful as a search incident to arrest.[83] In concluding that the searches incident to the arrests in that case were incompatible with the Fourth Amendment, the court observed "[m]ore substantial privacy interests are at stake when digital data is involved."[84] Indeed, the court noted, in today's modern world, a citizen's cell phone contains copious amounts of data, including, but not limited to: bank accounts, emails, text messages, photos, videos, and social media networks.[85]

---

78. *Id.* ("The officers entered the curtilage here: The front porch is the classic example of an area 'to which the activity of home life extends'"). *Id. See also* Oliver v. United States, 466 U.S. 170, 180 (1984) (the area "immediately surrounding and associated with the home"—the curtilage—is "part of the home itself for Fourth Amendment purposes." Jardines, 133 S. Ct. at 1412 (citing Oliver v. United States, 466 U.S. 170, 180 (1984)).
79. *Ex parte* Jackson, 96 U.S. 727, 728 (1877).
80. *Id.*
81. *Id.* at 733.
82. *Id.*
83. Riley v. California, 134 S. Ct. 2473 (2014).
84. *Id.* at 2480.
85. *Id.* at 2478–79.

> [C]ell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, *a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record*. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.[86]

Based on the unique and personal nature of cell phone data, coupled with a cell phone's low security risk to an arresting officer, the Supreme Court held that the "interest in protecting officers safety [did] not justify dispensing with warrant requirement" for searches of cell phone data.[87] In so holding, the *Riley* court established a rare bright-line rule under the Fourth Amendment when it declared that data searches of cell phones, regardless of type, are unlawful incident to arrest. Thus, the Supreme Court—at a minimum—implicitly recognized that data (not just photographs and text messages, but "distinct types of information that reveal much more in combination than any isolated record"[88]; i.e. metadata)—were "effects" upon which the government could not trespass.

Having established that the property based, trespass analysis is firmly ensconced in Supreme Court jurisprudence and that it applies to each of the aforementioned Fourth-Amendment categories, we turn to whether the NSA's metadata collection and storage program is a trespass to citizens' effects.

B. Metadata Collection and Storage as a Trespass to an Effect

Although the Supreme Court did not explicitly do so in *Riley v. California*, the Court suggested in the most direct terms that metadata, particularly metadata compiled from a cell phone, is an effect under the Fourth Amendment. In explaining why a search of a suspect's cell phone incident to arrest ran afoul of the Fourth Amendment, the court noted that a cell phone "collects in one place many distinct types of information that reveal much more in combination than any isolated record."[89] The clear implication from *Riley* is that part of what is protected from government

86. *Id.* (Emphasis added.)
87. *Id.* at 2486.
88. *Id.* at 2478–79.
89. *Id.* at 2479.

intrusion is the information that reveals information—cell phone numbers, call history, mobile internet searches. This *is* metadata. And because this information that reveals information, the metadata, is not a person, as outlined in *Terry v. Ohio*, or a house, as outlined in *Florida v. Jardines*, or papers as outlined in *Ex Parte Jackson*, it must be *effects*, akin to the cell phone data from *Riley v. California*. To put it simply, citizens' metadata is an "effect"[90] because it is their personal property.[91]

So, the question is: "Has the government trespassed on citizens' personal property, their effects, through the NSA's metadata collection and storage program?" According to *United States v. Jones* it has.

Recall that in *Jones*, the Supreme Court concluded that the government had trespassed on Jones' "effect" by "physically occup[ying Jones'] private property for the purpose of obtaining information."[92] This is precisely what the government has done through the NSA metadata collection and storage program. The government has physically occupied, that is, taken control of, through collection and storage, citizens' metadata (which we have demonstrated above is an effect under *Riley v. California*[93]) for the purpose of obtaining information. Indeed, the government's stated purpose for collecting and storing the metadata is to obtain information to combat terrorism.[94]

Some analysts argue that this type of government conduct could not have been envisioned by the Founders, the afore-quoted James Madison among them, because they could not have conceived of the type of potential global terrorist activity the government is now facing, and the corresponding action required to address it.[95] The following hypothetical demonstrates why that position is misguided.

Imagine it is 1771. King George III, suspicious of colonial revolt, dispatches British soldiers to present colonial business owners—among these, printers and blacksmiths—with a writ of assistance, a general warrant, ordering those business owners to covertly report to the Crown all information about purchases made by colonists.

---

90. *Effects*, BLACK'S LAW DICTIONARY (10th ed. 2014) (Effects are "[i]tems of a personal character" such as "personal property").

91. *Property*, BLACK'S LAW DICTIONARY (10th ed. 2014) (Personal Property is "[a]ny movable or intangible thing that is subject to ownership and not classified as real property.")

92. United States v. Jones, 132 S. Ct. 945, 949 (2012).

93. Riley, 134 S. Ct. 2473.

94. ACLU v. Clapper, 785 F.3d 787, 795 (2d Cir. 2015).

95. *See* Fred Fleitz, *NSA Data Collection: Necessary, or Unconstitutional?*, (http://www.nationalreview.com/article/418207/nsa-data-collection-necessary-or-unconstitutional-fred-fleitz) (noting in response to the argument that the Founders would be "appalled" at the NSA's metadata collection program that "the Founding Fathers lived in the era of wooden ships and simple firearms and had no notion of modern warfare and weapons of mass destruction.")

Once that information is reported, British officers review it to determine whether the purchasing habits of certain colonists are indicative of revolutionary activity. The officers review information provided by printers regarding individuals who have purchased column space advocating individual liberty, as well as information provided by the blacksmiths regarding individuals who have purchased large quantities of arms, knives, and horseshoes. These columns and items, British officers have determined, are indicative of revolutionary activity, the tactics of which the British view to be terroristic.

On this information, British soldiers are dispatched to enter the homes of those colonists suspected of revolutionary activity. The colonists' homes are ransacked and their effects are searched and, where deemed appropriate, they are seized. Those colonists who are considered sufficiently suspect are arrested, questioned, and often imprisoned.

The type of systematic invasion of citizens' persons, houses, papers, and effects described in the above hypothetical was, *at a minimum*, the type of government conduct the Founders sought to guard against when drafting the Fourth Amendment. [96] Indeed, the Supreme Court has acknowledged that it is "perfectly clear that the evil the [Fourth] Amendment was designed to prevent was [even] broader than the abuse of a general warrant."[97]

Nearly 200 years later, the Supreme Court decided *Korematsu v. United States*, which involved internment of American citizens under Executive Order 9066, a trespass to a protected category under the Fourth Amendment, the person.[98] We are faced now, the better part of 100 years

---

96. *See* Stanford v. State of Texas, 379 U.S. 476, 481-82 (1965)

> Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws. They were denounced by James Otis as 'the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book,' because they placed 'the liberty of every man in the hands of every petty officer.' The historic occasion of that denunciation, in 1761 at Boston, has been characterized as 'perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."'

Id. (quoting Boyd v. United States, 116 U.S. 616, 625 (1886)).

97. Payton v. New York, 445 U.S. 573, 585 (1980).

98. Korematsu v. United States, 323 U.S. 214, 223–24 (1944).

> It is said that we are dealing here with the case of imprisonment of a citizen in a concentration camp solely because of his ancestry, without evidence or inquiry concerning his loyalty and good disposition towards the United States. Our task would be simple, our duty clear, were this a case involving the imprisonment of a loyal citizen in a concentration camp because of racial prejudice. Regardless of the true nature of the assembly and relocation centers—and we deem it unjustifiable to call them concentration camps with all the ugly connotations that term implies—we are

later, with another internment, this time, a trespass to a different protected category under the Fourth Amendment, citizens' effects. It remains to be seen whether, under the guise of military necessity, the Supreme Court blesses the NSA's metadata collection and storage program like it did with Executive Order 9066. Until then, like Toyosoburo Korematsu, we wait.

IV. CONCLUSION

These authors have endeavored to address whether the government, through its NSA metadata collection and storage program, has engaged in a trespass to citizens' effects, their metadata, in order to obtain information, part of the second prong of the four-pronged analysis outlined above. In so doing, we have shown (1) that citizens' metadata, that is, their information about information, is an effect under the Fourth-Amendment analysis outlined in *Riley v. California*, and (2) that the government's NSA data collection and storage program, according to the holding in *United States v. Jones*, implicates the Fourth Amendment because that program takes control of, through collection and storage, citizens' effects for the purpose of obtaining information.

In so doing, we do not opine as to whether the government's NSA metadata collection and storage program is ultimately lawful. As previously explained, a separate thorough analysis under the third and fourth prongs of the approach that we have outlined may show that the government's action is justified. The government, may, for example, present convincing evidence that citizens' contracts with cell phone companies provide sufficient consent to authorize the trespass, or that the FISA Court orders are an adequate substitute for a traditional warrant. This analysis lies outside the scope of this article, but consideration of these elements is vital to a full analysis of NSA surveillance as it applies to the Fourth Amendment.

> dealing specifically with nothing but an exclusion order. To cast this case into outlines of racial prejudice, without reference to the real military dangers which were presented, merely confuses the issue. Korematsu was not excluded from the Military Area because of hostility to him or his race. He was excluded because we are at war with the Japanese Empire, because the properly constituted military authorities feared an invasion of our West Coast and felt constrained to take proper security measures, because they decided that the military urgency of the situation demanded that all citizens of Japanese ancestry be segregated from the West Coast temporarily, and finally, because Congress, reposing its confidence in this time of war in our military leaders—as inevitably it must—determined that they should have the power to do just this. There was evidence of disloyalty on the part of some, the military authorities considered that the need for action was great, and time was short. We cannot—by availing ourselves of the calm perspective of hindsight—now say that at that time these actions were unjustified.

Id.

Nevertheless, we caution that exceptions to Constitutional trespasses should not be recognized simply as a means to deter danger, both foreign and domestic, however great. This, of course, was the rationale utilized by the majority in *Korematsu* to justify internment camps—or, as the government put it, "Assembly Centers"[99]—for American citizens:

> [W]e are not unmindful of the hardships imposed by it upon a large group of American citizens. But hardships are part of war, and war is an aggregation of hardships. All citizens alike, both in and out of uniform, feel the impact of war in greater or lesser measure. Citizenship has its responsibilities as well as its privileges, and in time of war the burden is always heavier. Compulsory exclusion of large groups of citizens from their homes, except under circumstances of direst emergency and peril, is inconsistent with our basic governmental institutions. But when under conditions of modern warfare our shores are threatened by hostile forces, the power to protect must be commensurate with the threatened danger.[100]

When a court, in whatever jurisdiction in this Republic, places its imprimatur on a program like the NSA's metadata collection and storage program *only* because it saves lives by furthering a strategic military objective, that court cedes its Constitutional imperative to the executive branch's military leadership. And that, to the detriment of this Republic, undermines the sacrifices of our founding and contemporary patriots by rendering the judicial branch a mere "instrument[ality] of military policy."[101]

---

99. *Id.* at 220–21.

100. *Id.* at 219–20 (citations omitted).

101. *Id.* at 247 (Jackson, J., dissenting)

> I should hold that a civil court cannot be made to enforce an order which violates constitutional limitations even if it is a reasonable exercise of military authority. The courts can exercise only the judicial power, can apply only law, and must abide by the Constitution, or they cease to be civil courts and become instruments of military policy.

Id.