RILEY V. CALIFORNIA: CAN YOU HEAR THE EQUILIBRIUM NOW?

Maya Ziv[†]

In 2011, noted Fourth Amendment scholar Orin Kerr hypothesized that the Supreme Court decides Fourth Amendment cases with an eye to maintaining a balance between police power and individual rights initially established by the Framers.[1] Kerr claimed that "judges respond to new facts in Fourth Amendment law in a specific way: judges adjust Fourth Amendment protection to restore the preexisting level of police power."[2] As technology evolves, the tools used by both criminals and law enforcement officers change the equilibrium of power. When this occurs, courts address questions regarding the constitutionality of using new technologies to either increase expectations of privacy or to give law enforcement a new tool. Recently, the Court in *Riley v. California* addressed the issue of "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[3]

At first glance, Kerr's theory seems to hold up as applied through *Riley*. The Court denied police the ability to search through phones without a warrant in order to restore a balance between privacy rights and police power that existed before cell phones became ubiquitous. A closer examination of the application of Kerr's theory ("Equilibrium-Adjustment") in *Riley*, however, reveals several flaws in the theory. By thoroughly applying Kerr's theory to *Riley*, this Note illustrates three limitations to Kerr's claim that the Equilibrium-Adjustment theory can explain "a great deal of the overall shape and substance of Fourth Amendment doctrine."[4]

Part I of this Note reviews Fourth Amendment jurisprudence and introduces the relevant caselaw that has shaped the intersection between

† J.D. Candidate, 2016 University of California, Berkeley, School of Law.

1. Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

2. *Id.* at 487.

3. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

4. Kerr, *supra* note 1, at 481.

digital technology and the Fourth Amendment leading up to *Riley*. Part II investigates *Riley*, illustrating interesting aspects of the Court's analysis and how lower courts are dealing with its rule. Part III examines Kerr's Equilibrium-Adjustment theory and explains how it can be used to analyze *Riley*. Lastly, Part IV applies Kerr's theory to *Riley* in order to illustrate three main limitations on his theory: (1) the application of the theory varies based on the analyst and thus the theory is too broad to provide much insight, (2) the current balance between police power and individual rights that the Court attempts to restore is difficult to define; one jurisdiction's equilibrium may be another's imbalance, and (3) the theory fails to account for profit-minded third parties that may cause a sudden shift in societal norms in a way that neither introduces a new crime nor a new practice yet still upsets the equilibrium.

I. THE FOURTH AMENDMENT AND THE WARRANT CLAUSE

To assess how the theory of Equilibrium-Adjustment can apply to recent Fourth Amendment cases, it will be helpful to briefly review the warrant requirement and how law enforcement may comply with it. The Fourth Amendment establishes:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[5]

The Framers said little about how to define key terms within the Fourth Amendment, so courts have interpreted the Amendment through several seminal cases.[6] A search is considered an infringement of "an expectation of privacy that society is prepared to consider reasonable."[7] A seizure of property is a "meaningful interference with an individual's possessory interest in that property."[8]

Courts have adopted Justice Harlan's definition of a reasonable search in his *Katz v. United States* concurrence: "[T]here is a twofold

5. U.S. CONST. amend. IV.

6. *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING, 602-1791 770–72 (Oxford University Press, Inc., 2009).

7. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

8. *Id.*

requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[9] Yet the Amendment's text, including the warrant clause and the definition of probable cause, and the parameters of Harlan's test remain relatively vague.[10] Historically, judges deemed that a search without a warrant was per se unreasonable unless the search fell into one of many categories of exceptions.[11] But this per se unreasonable rule has been eroded by the adoption of many exceptions to the warrant requirement. More recently, the Court has recognized this shift, commenting that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[12] Generally, a court determines whether to exempt a type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[13]

A. EXCEPTIONS TO THE WARRANT REQUIREMENT

While searches without a warrant may be presumptively unreasonable, the Supreme Court has established dozens of exceptions that make warrantless searches reasonable. A review of these exceptions helps to illustrate the complexity of Fourth Amendment law. The exceptions discussed below display the balance of power between the government and individuals that could come into play in a case dealing with digital information like *Riley v. California*, and thus give context to the debate around the significance of the case.

---

9. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Justice Harlan understood the majority to want protection for an individual's subjective expectation of privacy, if and only if society is prepared to regard the expectation of privacy reasonable.

10. See CUDDIHY, *supra* note 6.

11. This reflected the Founders' fear of warrants. *See* Riley v. California, 134 S. Ct. 2473, 2494 (2014) ("Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1333 (2002) ("According to conventional wisdom, the Fourth Amendment embodies the Founders' concerns over general warrants and writs of assistance . . . because of two connecting themes: concern about the privacy of an individual's home and papers against the government and fear of unbridled official power and discretion.").

12. *Riley*, 134 S. Ct. at 2482.

13. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

First, police do not require a warrant in cases of searches "incident to arrest."[14] In *Chimel v. California*, the Court held that it was unreasonable for police to search beyond the area "within [a suspect's] immediate control," or the area from which a suspect "might gain possession of a weapon or destructible evidence."[15] Thus, a search of Chimel's entire house was beyond the scope of the search incident to arrest warrant exception because it was not necessary to protect the officers or prevent the destruction of evidence.[16] The Court in *United States v. Robinson* held that a search of a cigarette package found on an arrestee was reasonable, though the arresting officer had no concerns regarding the loss of evidence or that Robinson had a weapon.[17] The Court later clarified that this exception was limited to "personal property . . . immediately associated with the person of the arrestee."[18] Finally, in *Arizona v. Gant* the Court noted that cars are treated differently than individuals within the search incident to arrest exception.[19] After an arrest of an individual within their car, police may justify a warrantless search of a vehicle's passenger compartment when it would be "reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."[20] The Court noted that this evidence-based exception was "unique to the vehicle context," limiting the police from searching a car without a warrant unless there is probable cause to search the whole car or if the compartment is within reaching distance of the arrestee.[21]

Another exception to the warrant requirement exists if police obtain information from a third party. Individuals rarely have an absolute "reasonable expectation of privacy" when they share information with someone else because parties to the conversation can later freely share that information with law enforcement. For example, while police may not be able to use wiretapping technology to overhear a conversation, nothing stops a friend from sharing information with the police on his own.

14. *See* Weeks v. United States, 232 U.S. 383, 392 (1914) (acknowledging in dictum "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime").

15. Chimel v. California, 395 U.S. 752, 762–63 (1969).

16. *Id.* at 768.

17. 414 U.S. 218, 236 (1973).

18. United States v. Chadwick, 433 U.S. 1, 15 (1977) (finding that a 200-pound locked footlocker could not be searched incident to arrest).

19. *See* Arizona v. Gant. 556 U. S. 332, 343 (2009).

20. *Id.* at 333 (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)).

21. *See id.*

Applying the exception to people seems reasonable, but the Court also applies it to businesses. In *United States v. Miller*,[22] the Court held that an individual who voluntarily provided financial documents to a bank lacked a Fourth Amendment interest in his banking records that were in the custody of the bank. *Miller* informed the Court's holding in *Smith v. Maryland*, in which police used a pen register to record the numbers dialed from an individual's phone.[23] The Court held that individuals lack a "reasonable expectation of privacy" in the phone numbers they dial, even from a private residence, because the numbers were necessarily communicated to the phone company.[24] The Fifth Circuit extended this concept to uphold the Stored Communications Act[25] ("SCA"), permitting the third-party phone carriers to collect historical cell site data.[26]

Third, consent frequently justifies a warrantless search, especially in cases like *Riley*. If an individual voluntarily gives the police permission to search a cell phone without a warrant, the subsequent search of the phone does not violate the Fourth Amendment.[27] Issues may arise with regards to the scope of consent, but consent will nonetheless play a significant role in dealing with police searches of digital information on mobile devices.

Another sensible exception arises in cases of exigency. The *Riley* Court noted that this exception in particular might justify a warrantless search of a cell phone.[28] Sometimes "'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment."[29] Such exigencies could include the need to prevent the imminent destruction of evidence,[30] to pursue

22. 425 U.S. 435 (1976).

23. Smith v. Maryland, 442 U.S. 735, 737 (1979).

24. *Id.* at 746.

25. Stored Communications Act, 18 U.S.C. § 2703 (2012).

26. *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). For a full discussion of this case and its implications, see Mark Daniel Langer, Note, *Rebuilding Bridges: Addressing the Problems of Historic Cell Site Location Information*, 29 BERKELEY TECH. L.J. 955 (2014).

27. *See generally* United States v. Drayton, 536 U.S. 194 (2002) (holding that a warrantless search of a bus passenger comported with the Fourth Amendment because the passenger gave consent to the search). Even the Electronic Frontier Foundation, a digital privacy rights advocacy group, acknowledges that police don't need a warrant if a defendant consented to a search. *See* Hanni Fakoury & Nadia Kayyali, *Know Your Rights!*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/know-your-rights (last visited Feb. 13, 2015).

28. *See* Riley v. California, 134 S. Ct. 2473, 2494 (2014).

29. *Id.* (citing Kentucky v. King, 131 S. Ct. 1849, 1856 (2011)).

30. *See, e.g.*, *King*, 131 S. Ct. at 1849.

fleeing suspects (hot pursuit),[31] or to aid injured people.[32] Critically, unlike other warrant exceptions, "the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case."[33]

Finally, searches of digital information in practice are very broad,[34] because procedures for searching digital devices involve at least a cursory inspection of every file. If, for instance, a search for drug dealing turns up evidence of some unrelated crime, the details of the unrelated crime fall into the "plain view" exception to the Fourth Amendment. A police officer may seize evidence without a warrant if three requirements are met. First, the officer must observe the object from a lawful vantage point.[35] Second, the officer must be in a location to seize the object lawfully.[36] Third, the incriminating character of the object must be immediately apparent.[37] Even if the officer is conducting a legal warrantless search under an exception to the warrant requirement, any information seen during this search may still be seized under the plain view doctrine.[38] With the amount of data available on cell phones, this exception could allow police conducting a search of a phone incident to an arrest for evidence of a specific crime to discover and seize a significant amount of information unrelated to the original crime.

These exceptions just scratch the surface of the complexity of Fourth Amendment law. The intricacies of this area of the law make it difficult to predict the long-term ramifications of cases after they are decided. They also illustrate the general balance of police power and individual rights that may be of particular relevance when considering searches of digital

31. *See, e.g.*, Warden v. Hayden, 387 U.S. 294 (1967).
32. *See, e.g.*, Brigham City, Utah v. Stuart, 547 U.S. 398 (2006).
33. *Riley*, 134 S. Ct. at 2494.
34. For more on the implications of the breadth of digital searches, see *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1004–05 (9th Cir. 2009). Judge Kozinski of the Ninth Circuit wrote:

> This pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. . . . Once a file is examined, however, the government may claim . . . that its contents are in plain view and, if incriminating, the government can keep it.

Id.
35. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971).
36. *See* Horton v. California, 496 U.S. 128, 136–37 (1990).
37. *Id.*
38. *See Coolidge*, 403 U.S. at 465.

information on mobile devices. The next Section narrows the scope of the discussion to cases discussing the warrant requirement leading up to *Riley* in order to better understand how *Riley* affects this balance.

B. THE PRE-*RILEY* LANDSCAPE

In addition to reviewing general Fourth Amendment concepts, it is helpful to consider the legal landscape of Fourth Amendment jurisprudence and digital technology that existed before *Riley*. A few cases help establish that at this time courts were beginning to consider the impact of digital technology on Fourth Amendment issues. In 2012, *United States v. Jones* addressed whether warrantless use of a global positioning system ("GPS") tracking device to track a car without the owner's consent violated the Fourth Amendment.[39] Because *Riley* dealt with the kind of information found on cell phones in particular, it is also useful to briefly explain the SCA and the 2013 Fifth Circuit case that upheld its constitutionality, *In re Application of the United States for Historical Cell Site Data* ("*Historical Cell Site*").[40] Knowledge of these cases will allow for a more complete understanding of the significance of *Riley* itself.

In *Jones*, the majority of the Court held that police placing a GPS tracking device on a car was a trespass and would be an unreasonable search without a warrant.[41] Through *Jones*, the Court essentially denied police a new searching power simply by using new technology.[42] In a concurring opinion, Justice Sotomayor wrote that the net result of allowing the police to use such technologies now available in the digital age "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[43] Although a single opinion, this concurrence was particularly strong. Justice Sotomayor's comments have aged well enough the *Riley* Court found them sufficiently persuasive to

39. 132 S. Ct. 945 (2012).

40. 724 F.3d 600 (5th Cir. 2013).

41. *Jones*, 132 S. Ct. at 954.

42. *See id.*

43. *Id.* at 956 (Sotomayor, J., concurring) (citing United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). Justice Sotomayor noted that GPS monitoring is a way to make "available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track." *Id.* She also predicted that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," holding that the approach is "ill suited to the digital age." *Id.* at 957.

warrant citation for the proposition that the digital age requires new rules for searches.

The SCA[44] is another important aspect of the pre-*Riley* landscape. This federal statute sets forth procedures for access to communications metadata (such as call logs and user location) and content.[45] This statute allows police to access call logs and historical cell site location data on a less than probable cause evidentiary standard.

In *Historical Cell Site*, the government brought applications under the SCA in three separate criminal investigations seeking to compel cell phone service providers to produce cell site information for targeted cell phones by tracking the phones over a two-month period.[46] The Fifth Circuit held that court orders to compel cell phone service providers to produce the historical cell site information of their subscribers authorized by the SCA under a "specific and articulable facts" standard were not a per se violation of the Fourth Amendment.[47] The Fifth Circuit is still the only court of appeals to address this particular issue,[48] and as it stands, has allowed the power to order such disclosure under a less than probable cause standard to remain with the police.

II. *RILEY V. CALIFORNIA*

This Part builds on the previous exploration of Fourth Amendment law to explain *Riley v. California* and how the Court saw that it related to prior cases and general Fourth Amendment concepts. It is also helpful to explore the factual history and Supreme Court's analysis before determining where *Riley* fits on Kerr's equilibrium.

---

44. 18 U.S.C. § 2703 (2012).

45. The statute generally allows government access to "local and long distance telephone connection records, or records of session times and durations," and "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address" of electronic communication service or remote computing service subscribers. 18 U.S.C. § (c)(2)(C).

46. *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013).

47. *Id.* at 615.

48. The Fifth Circuit revisited this case in September 2014 in *United States v. Guerrero*, No. 13-50376, 2014 WL 4476565 (5th Cir. Sept. 11, 2014). *See* Section II.C, *infra*. The Eleventh Circuit is currently hearing a case en banc in *United States v. Davis* where they also address this issue. 754 F.3d 1205, 1209 (11th Cir. 2014) *reh'g en banc granted, opinion vacated*, 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014).

A. FACTUAL HISTORY

The Court consolidated two cases, *Riley v. California* and *United States v. Wurie*, and held that police need a search warrant before looking through the digital information on a cell phone when the phone is seized incident to the arrest of its owner. This Section will review the facts of each case.

1. Riley v. California

A police officer stopped David Riley for driving with expired registration tags.[49] During the stop, the officer learned that Riley had been driving with a suspended license.[50] Pursuant to department policy, the officer impounded Riley's car; another officer conducted an inventory search of the car, finding two handguns under the car's hood.[51] Riley was arrested for possession of concealed and loaded firearms.[52]

An officer searched Riley incident to the arrest and found items associated with the "Bloods" street gang.[53] In addition, the officer seized Riley's smart phone.[54] The officer searched the phone and noticed that some words[55] were preceded by the letters "CK," a label he believed represented "Crip Killers," a slang term for members of the Bloods gang.[56] Later at the station, a detective specializing in street gangs further examined the contents of the phone, looking for evidence of other crimes.[57] The detective found photographs of Riley in front of a car the police suspected had been involved in a shooting a few weeks earlier.[58]

Riley was ultimately charged for crimes in connection with the shooting.[59] The State alleged that Riley had committed the crimes for the benefit of a criminal street gang, an aggravating factor carrying an enhanced sentence.[60] At trial, Riley moved to suppress all evidence

49. Riley v. California, 134 S. Ct. 2473, 2480 (2014).
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*
55. The Court presumed these words were found in text messages or a contact list.
56. *Riley*, 134 S. Ct. at 2480.
57. *Id.* at 2480–81.
58. *Id.*
59. *Id.*
60. *Id.*

obtained by the police off his cell phone, contending that the searches of his phone violated the Fourth Amendment.[61]

The trial court rejected the argument.[62] At trial, police officers testified about the content found on the phone, and some of the photographs were admitted into evidence.[63] Riley was convicted on all counts and received an enhanced sentence of fifteen years to life in prison. The California Court of Appeals affirmed, relying on the California Supreme Court's decision in *People v. Diaz*,[64] which held that the Fourth Amendment permits a warrantless search of cell phone data incident to arrest if the cell phone was immediately associated with the arrestee's person.[65] The California Supreme Court denied Riley's petition for review, and the Supreme Court granted certiorari in this case in conjunction with another case, *United States v. Wurie*.[66]

2. United States v. Wurie

During routine surveillance, a police officer observed Brima Wurie make an apparent drug sale from a car.[67] Officers arrested Wurie, and seized two cell phones from Wurie's person.[68] Five to ten minutes after arriving at the station, the officers noticed that one of the cell phones, a flip phone, was receiving calls from a source identified as "my house" on the phone's external screen.[69] Officers opened the phone, pressed one button to access the call log, and one button to determine the phone number associated with the label.[70] The officers used an online phone directory to trace the number, which led to an apartment building.[71]

When the officers went to the building, they saw Wurie's name on a mailbox and observed through a window a female resembling a figure in a photograph set as the background on Wurie's phone.[72] Based on this information, the police obtained a search warrant and found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm,

61. *Id.*
62. *Id.*
63. *Id.*
64. 244 P.3d 501, 511 (Cal. 2011).
65. *Riley*, 134 S. Ct. at 2480.
66. *Id.* at 2481.
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*

ammunition, and cash.[73] Wurie was charged with distributing crack cocaine, possessing crack cocaine with the intent to distribute, and being a felon in possession of a firearm and ammunition.[74] At trial, Wurie moved to suppress the evidence obtained from the search of his apartment, claiming it was fruit from the unconstitutional search of his cell phone.[75]

The trial court denied the motion, and Wurie was convicted on all three counts.[76] A divided First Circuit panel reversed the denial of Wurie's motion and vacated Wurie's convictions for possession with intent to distribute and possession of a firearm as a felon.[77] In doing so, the First Circuit held that cell phones are distinct from other physical possessions that could be searched incident to an arrest because of the amount of data stored on cell phones and the negligible threat they pose to law enforcement's interests.[78] The Supreme Court granted certiorari in conjunction with *Riley v. California*.[79]

B. SUPREME COURT'S REASONING

In *Riley*, the Court established a Fourth Amendment rule that differentiated digital property from physical property.[80] Specifically, the Court declined to extend the search incident to arrest exception to allow police to search the vast quantities of data available on both smartphones and flip phones, holding that police needed a warrant to search the contents of a phone found on the body of the arrestee.[81] The Court analyzed this issue along with previous cases that established the "search incident to arrest" warrant exception.[82]

The *Riley* Court first considered the importance of officer safety and loss of evidence, otherwise known as the *Chimel* factors, in determining if

73. *Id.*
74. *Id.* at 2482.
75. *Id.*
76. United States v. Wurie, 612 F. Supp. 2d 104, 111 (D. Mass. 2009).
77. *See* United States v. Wurie, 728 F.3d 1, 1 (1st Cir. 2013).
78. *Id.* at 7–10.
79. United States v. Wurie, 134 S. Ct. 999 (2014).
80. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014); *see also* Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California*, a Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSBLOG (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age.
81. *See Riley*, 134 S. Ct. at 2480.
82. *See id.; see also* Weeks v. United States, 232 U.S. 383, 392 (1914) (acknowledging in dictum "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime").

the *Riley* officers were justified in their actions.[83] The Court reasoned that these justifications did not apply because a cell phone did not present the risks of harm to officers or destruction of evidence necessary to justify a search.[84] There is clearly no physical threat to police from the data stored on cell phones. Additionally, once law enforcement officers seize a phone, the Court saw no risk of the arrestee deleting incriminating data from the phone.[85] Though the State claimed that the risk of loss of evidence was strong due to the power of remote-wiping technologies, the Court was not persuaded by the anecdotal examples of remote wiping triggered by an arrest included in the briefing.[86] The Court noted that in cases that police are confronted with an emergency situation, such as recognizing a defendant's phone will be the target of a remote-wipe attempt, police may be able to rely on the exigent circumstances warrant exception to search the phone immediately.[87]

Furthermore, though *Robinson* established that people under arrest have a reduced expectation of privacy, the Court considered a search of the massive quantities of data on a cell phone as beyond the scope of *Robinson*'s holding.[88] The Court believed that the storage capacity of cell phones, inherent pervasiveness of cell phone data, and qualitative difference of data available on cell phones as compared to physical records allowed for too high of a level of intrusion on privacy.[89] The Court noted that to carry around the same amount of information in physical form, a person would need a truck[90] rather than a cigarette package as in *Robinson*.[91] Finally, the fact that some data accessed through a cell phone might actually be stored on the "cloud" raises additional privacy concerns such that "the privacy interests here dwarf those in *Robinson*."[92] The Court also rejected the argument that officers should be able to search a phone's

83. *Riley*, 134 S. Ct. at 2484.
84. *Id.* at 2484–85.
85. *Id.* at 2486.
86. *Id.*
87. *Id.* at 2487.
88. *Id.* at 2484 ("while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones"); *id.* at 2488 ("The fact that an arrestee has diminished privacy interests does not mean the Fourth Amendment falls out of the picture entirely.").
89. *Riley*, 134 S. Ct. at 2489.
90. The Court noted that such a truck would require a search warrant under *United States v. Chadwick*, 433 U.S. 1 (1977).
91. *Riley*, 134 S. Ct. at 2489.
92. *Id.* at 2491.

call log as done in Wurie's case because of the amount of information that exists in a call log.[93] Combined, these rationales hint that other digital devices in possession of an individual, such as laptops, would be protected based on the volume of data stored on their hard drives.

While the Court emphasized that this holding applies to the search incident to arrest exception, they hinted at other issues they would consider in the future. In particular, the Court disagreed with the United States's assertion that a search of data on a cell phone was "materially indistinguishable" from searches of physical items like the *Chimel* house or the *Robinson* cigarette package.[94] The Court instead asserted that "[c]ell phones differ in both a quantitative and qualitative sense from other objects that may be kept on arrestee's person."[95] The quantitative differences come in the form of storage capacity and pervasiveness of data.[96] The qualitative differences exist mainly in the kind of information stored on a cell phone, which can reveal where the owner's prior locations, website searches, and interests.[97]

Citing *Kerr*, the Court added that before cell phones, "a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy."[98] Because of the amount and kind of information now stored on cell phones,

> a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously not found in the home; it also contained a broad array of private information never found in a home in any form—unless the phone is.[99]

In addition, the prevalence of cloud computing means that "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or

93. *Id.* The United States argued that *Smith v. Maryland*, 442 U.S. 735 (1979), which held that no warrant was required to use a pen register at a telephone company premises to identify numbers dialed by a caller, allows for a warrantless search of a cellphone call log. However, the Court in that case concluded the use of the pen register was not a Fourth Amendment search at all. *Id.* at 745–46.

94. *Riley*, 134 S. Ct. at 2488.

95. *Id.* at 2489.

96. *Id.* at 2489–90.

97. *See id.* at 2490–91.

98. *Id.* at 2489. (citing Orin Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404–05 (2013)).

99. *Id.* at 2491.

has been pulled from the cloud."[100] The possibility that a search could reach information not actually available on the body of the arrestee is, again, "yet another reason that the privacy interests here dwarf those in *Robinson*."[101] Thus, the Court created a new rule for the digital age, preventing warrantless searches of items that contain too much information.[102]

C. *RILEY* IN THE COURTS

State and federal courts are beginning to hear cases that fall within *Riley*'s "grey area," or cases regarding searches that occurred before *Riley*'s decision but that are being litigated now. In 2011, the Supreme Court ruled that the good faith exception to the exclusionary rule applies when a defendant successfully persuades a court to overturn precedent in favor of expanded Fourth Amendment rights.[103] Trial courts have begun to apply the good faith exception to cases dealing with pre-*Riley* surveillance that relied on *Diaz*, and it is likely that this trend will continue at the appellate level.[104]

The Fifth Circuit, however, recently held that *Riley* does not provide rights to the individual that counter the government's search abilities under the SCA. On September 11, 2014, the Fifth Circuit published its opinion in *United States v. Guerrero*.[105] Guerrero had been charged with various counts related to his membership in the Mexican Mafia.[106] As part

100. *Id.*

101. *Id.*

102. In a separate concurrence, Justice Alito added that the Court should not "mechanically apply the rule used in the pre-digital era to the search of a cell phone," and called for a "new balancing of law enforcement and privacy interests." *Id.* at 2496–97. Second, Justice Alito called on Congress to enact legislation that distinguished privacy interests in different types of data, concluding "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment." *Id.* at 2497.

103. *See* Davis v. United States, 131 S. Ct. 2419 (2011).

104. *See, e.g.*, United States v. Garcia, No. 13-CR-00601-JST-1, 2014 WL 4543163, at *6 (N.D. Cal. Sept. 12, 2014) ("*Diaz* provides sufficient 'binding appellate precedent' that 'specifically authorized' the actions the officers took in this case."). *But see* United States v. Martinez, No. CR 13-00794 WHA, 2014 WL 3956677, at *5 (N.D. Cal. Aug. 12, 2014) (declining to apply the good faith exception based on *Diaz* because "a cell-phone search occurring one to two hours after an arrest was not incident to that arrest"). *See also* Nebraska v. Henderson, 854 N.W.2d 616 (Neb. 2014). Here a warrant was issued before the search, but it was faulty. Thus the court had to consider if the warrantless search was reasonable. The application of the "good faith" exception was different here than in *Davis*.

105. No. 13-50376, 2014 WL 4476565 (5th Cir. Sept. 11, 2014).

106. *Id.* at *1.

of the investigation, police had received "historical cell site location data that roughly indicated where he was, or at least where his cell phone was, on the afternoon that [a victim] was killed," from third party communications providers.[107] Guerrero moved to suppress the evidence of the cell site location data, arguing it had been obtained in violation of the Fourth Amendment.[108] Guerrero relied on *Riley*, seeking to overturn the effects of *Historical Cell Site*.[109] The Fifth Circuit held that because *Historical Cell Site* relied on the third-party doctrine and not the search incident to arrest warrant exception, *Riley* did not apply to the case at hand.[110]

The court cited various sources debating the effect of *Riley* on the third-party doctrine, but noted that "the mere existence of that spirited academic debate, however, resolves our limited inquiry. In determining the effect of Supreme Court developments on our precedents, we . . . only decide whether an issued Supreme Court decision has 'unequivocally' overruled our precedent."[111] Because *Riley* did not explicitly overrule *Historical Cell Site* and the impact of *Riley* on the third-party doctrine was unclear, the court rejected Guerrero's argument.[112] As it stands, the police can only receive access to data known to be shared with a network provider through a process involving further investigation than simply digging through a cell phone's records. The balance between government interests and Guerrero's privacy rights are maintained, if not slightly tipped towards police power. It seems as if this slight tip in favor of the government is the current status quo.

From *Jones* to *Riley*, in Kerrian terms, the Court seems to have been correcting the balance between government powers and privacy rights. Commentators should anticipate that the Court will continue to engage in equilibrium-adjustment. If cases like *Guerrero* wind up in front of the Supreme Court, Fourth Amendment scholars applying Kerr's theory should believe that the Court will establish rules that skew towards upholding individual privacy rights.[113]

---

107. *Id.* at *5.
108. *Id.*
109. *Id.* at *6.
110. *Id.* at *7.
111. *Id.* at *8.
112. *Id.*
113. On a related issue, the Eleventh Circuit recently granted en banc review of *United States v. Davis*, a case that addresses the issue of the constitutionality of the SCA. 754 F.3d at 1209, *reh'g en banc granted, opinion vacated*, 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). Davis had moved to suppress electronic location evidence that

III. ORIN KERR'S EQUILIBRIUM-ADJUSTMENT THEORY

Some scholars theorize that the plethora of warrant exceptions and the generally unclear definition of the warrant clause in the Fourth Amendment itself have led to "messy" Fourth Amendment jurisprudence with inconsistent rules.[114] Through his Equilibrium-Adjustment theory, Kerr attempts to make sense of Fourth Amendment jurisprudence and draw a connection between the potentially difficult to reconcile rules.

Kerr's article proposes the idea that generally the Supreme Court adjusts the boundaries of Fourth Amendment protection in response to changing technologies to maintain the status quo level of protection of individual rights from government power.[115] Kerr claims that this theory explains various seemingly odd holdings that have created exceptions to the warrant requirement, and further exceptions to those exceptions, based on new technologies.[116] For example, the Court has held that use of a beeper to follow a car on public highways does not amount to a search, but as soon as the beeper enters a location in which the driver has a reasonable expectation of privacy and the police can tell where it is, a search has occurred.[117] The location where the beeper was used changed the determination that a search had occurred, despite the same technology being used in both cases. In another example, police may solicit information regarding cell phone positioning data from a third party (the carrier), but cannot receive the same information from the cell phone itself.[118] In other words, one exception to the warrant requirement justifies the search while another does not.

---

the government obtained without a warrant under the SCA, claiming that the obtainment of that evidence violated his Fourth Amendment rights. *Id.* The Court of Appeals held that "cell site location information is within the subscriber's reasonable expectation of privacy. The obtainment of that data without a warrant is a Fourth Amendment violation." *Id.* at 1217. This holding, however, has already been vacated, as the judges will review the case en banc. Such a controversial issue is virtually guaranteed to find its way to the Supreme Court, where we may anticipate that a Court with an eye for equilibrium-adjustment will seek to restore the status quo.

114. *See, e.g.*, Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149 (1998) (noting that many commentators have expressed that the Fourth Amendment is a "mess"); Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 (1985). *See* CUDDIHY, *supra* note 6.

115. Kerr, *supra* note 1, at 481.

116. *Id.*

117. *Id.* at 499–500, contrasting *United States v. Karo*, 468 U.S. 705 (1984), with *United States v. Knotts*, 460 U.S. 276 (1983).

118. *Compare In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (allowing police to request historical cell site data from a

A. KERR'S SCENARIOS AND YEAR ZERO

Kerr argues that courts decide Fourth Amendment cases with an eye to restoring the equilibrium to a time he calls "Year Zero."[119] Year Zero "represents an imaginary time, a sort of beginning of the universe for criminal investigations. . . . By starting with a hypothetical world with no tools, we can see how the introduction of new tools poses a constant challenge to any legal system that seeks to regulate police investigations."[120] Furthermore, Year Zero operates with a few basic rules; Kerr posits these are the rules the Framers had in mind when crafting the Fourth Amendment.[121] First, "the police are always free to watch suspects in public."[122] However, if police seek to make an arrest, "they need probable cause to believe the suspect has committed a crime."[123] If the police wish to enter a suspect's home, they need a warrant based on probable cause.[124] These rules have established "a certain level of police power to enforce the law . . . [T]he rules give the police the powers needed to investigate crime successfully in many cases."[125] Yet these rules also limit police power to avoid abuses through the probable cause and warrant requirements.[126]

Kerr establishes this balance as the original equilibrium, claiming that even if the balance is not perfect, it is stable.[127] New facts and tools, however, "render the balance of police power struck by Year Zero inherently unstable."[128] The critical question that Kerr attempts to answer is how Fourth Amendment doctrine should respond when these changes do occur.[129] To do so, Kerr explores six scenarios in which the balance is upset.[130] First, where "the government uses a new tool to find evidence," perhaps involving the use of a new surveillance device to obtain

carrier on a standard less than probable cause), *with* Riley v. California, 134 S. Ct. 2473, 2495 (2014) (ordering police to secure a warrant before searching a cell phone incident to arrest).

119. *Id.* at 482.
120. *Id.* at 483.
121. *Id.* at 484.
122. *Id.*
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.* at 485
128. *Id.* at 486.
129. *Id.* at 487.
130. *Id.* at 489.

information that was previously unobtainable.[131] Second, where "criminals use a new tool to evade detection," which makes it harder for the government to observe the crime.[132] Third, "new crimes and new practices," where new social or political developments emerge, but crime occurs using the same technologies.[133] Fourth, where "both criminals and the police use a new tool," where criminals use a new technology to commit crime and police use a method of surveillance to detect the crimes using the same technology.[134] Fifth, "the status quo," in which the facts remain the same as they were in Year Zero.[135] Finally, "defeating countermeasures," where both the police and criminals try to use new advances in technology to gain an advantage over the other.[136]

Kerr claims his theory is defensive, that it is a "theory of interpretation seeking guidance from prior historical moment—rather than a theory of legal evolution."[137] Kerr contrasts his theory with the trend he views in right to privacy and Commerce Clause caselaw.[138] In the right to privacy cases, Kerr claims the Court attempts to apply principles informed by a sense of current societal values and the broader role of the Supreme Court in American society.[139] In the Commerce Clause cases, the Court has expanded the federal government's authority dramatically, which Kerr believes is hardly the goal of the Framers.[140] While these cases have evolved in standard common law fashion, Fourth Amendment jurisprudence "has been guided by the restorative principles of equilibrium-adjustment."[141]

B. JUDICIAL DELAY AS A LIMITATION ON EQUILIBRIUM-ADJUSTMENT

Kerr also provides some ideas for how judges can maximize their impact that holdings in such cases will have in balancing police power and privacy rights. One of these concepts is "Judicial Delay," or waiting for the best time to determine if a technology is disruptive enough to deserve a

131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.*
137. *Id.* at 493.
138. *Id.* at 493–94.
139. *Id.*
140. *Id.*
141. *Id.* at 494.

holding.[142] Essentially, if a court intervenes too soon, "it may wrongly assess the need for adjustment because either the technology hasn't evolved to a reasonably stable state or else social practices relating to the use of the technology continue to evolve."[143] Kerr points to 1928's *Olmstead v. United States*[144] decision as an example of early judicial intervention, ultimately triggering its reversal by *Katz* in 1967.[145] Resolution of the reasonable expectation of privacy test ultimately depends on the stability of society's notion of what is reasonable; deciding a case too early would undermine this part of the *Katz* test. Courts can solve this problem by either putting off deciding how the Fourth Amendment applies to a new technology until the use of the technology has stabilized, or stepping in earlier while recognizing the decision must remain tentative while the technology is in flux.

The Supreme Court recently addressed this notion in *City of Ontario v. Quon*.[146] While Justice Kennedy expressed a preference to avoid ruling on how the Fourth Amendment applies to changing technology "before its role in society has become clear,"[147] Justice Scalia wrote otherwise in his concurring opinion:

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.[148]

142. *Id.* at 539.

143. *Id.*

144. 277 U.S. 438 (1928).

145. Katz v. United States, 389 U.S. 347, 353 (1967). *Olmstead* focused on the text of the amendment, explaining there was no search without physical intrusion on a person, house, paper, or effect. *Id.* Thus, the Fourth Amendment did not cover eavesdropping from beyond the boundaries of a house. *Id. Katz* shifted the focus to expectations of privacy generally, holding "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." *Id.*

146. 130 S. Ct. 2619 (2010).

147. *Id.* at 2629.

148. *Id.* at 2635 (Scalia, J., concurring in part and concurring in the judgment) (citation omitted).

Yet Kerr believes that judicial delay will "tend to resolve the issues more quickly, and with greater interim assistance from legislative privacy protection, than will efforts to address the Fourth Amendment issues early on while the risk of error is high."[149] This concept will become especially useful in discussions of the practical effects of *Riley* after the private sector's reaction to government surveillance of digital data.[150]

C. WHAT COULD SHIFT THE EQUILIBRIUM?

Before diving into an analysis of where *Riley* and related cases fall along this equilibrium, it is useful to consider what kind of case could actually disprove Kerr's theory. In other words, what would trigger a "shift" of the equilibrium as opposed to a court's attempt to restore Year Zero's balance of power?

A shift might come in the form of consecutive holdings that either expand or contract the interpretation of the Fourth Amendment. Expansion or contraction of the law may not appear in the exact same form. A restriction could come in the form of expanding the definition of a "search" or by refusing to apply an exception to the warrant clause. An expansion could occur by holding that a search was reasonable or by creating a new exception to the warrant requirement. Consecutive holdings that similarly change the interpretation of the Fourth Amendment would indicate a significant shift towards either privacy rights or police power.

Though a perfect balance is impossible as the world changes, Kerr argues that the Court's holdings historically seem to oscillate over an ideal center, the Kerrian Year Zero equilibrium.[151] Yet factors beyond the legal system's control mean that the Court may not continue to follow its historic pattern. Because the Court has been frequently dealing with technology in the last three years, now is an opportune time to revisit Kerr's thesis by applying it to the cases decided since he published the theory in 2011.

D. *JONES*, THE STORED COMMUNICATIONS ACT, *RILEY*, AND EQUILIBRIUM-ADJUSTMENT

Kerr's theory can be tested by analyzing cases that were decided after he published his article. *Jones*, *Historical Cell Site*, and *Riley* provide the

149. Kerr, *supra* note 1, at 539.
150. *See* Section IV.C, *infra*.
151. See Kerr, *supra* note 1, at 481–82.

perfect starting point to determine if the Court acted in compliance with a desire to maintain an equilibrium as Kerr suggests. The first case used here to analyze the theory is the 2012 case *Jones*, which held that the police could not use a GPS tracker without a warrant to track the movements of a car.[152] The second case is 2013's *Historical Cell Site*, which held that the SCA allows police to access via subpoena historic cell site location data (which can also be found on the phone itself).[153] Third, *Riley* held in 2014 that police could not search a cell phone found on the person of an arrestee without a warrant.[154] This Section will plot each of these issues on the spectrum between privacy rights and police power to determine if Kerr's theory holds along these technological changes.

The *Jones* majority held that warrantlessly tracking a suspect using a GPS device was unconstitutional because the police had to trespass on the defendant's property in order to engage in the search. A strong concurrence by Justice Sotomayor added that securing GPS data without a warrant was an unreasonable search because such a search was too intrusive due to the amount of data easily collected through such little effort by police.[155] *Jones* thus tilts the balance towards more individual privacy rights because it held that the police must show probable cause before attaching a GPS device to a suspect's car.

Yet in 2013, *Historical Cell Site* employed the third-party doctrine to hold that police may obtain cell phone user information under the SCA,[156] which allows the government to access call logs and historical cell site location data with less than a warrant. While *Jones* held that police need a warrant to use a GPS device to track a defendant's location, police can now gain historical cell site information on a standard lower than probable cause.[157] Given operator retention policies, this search could turn up years of location data.[158] Such a conclusion tilted the balance towards more police power in certain situations. If Kerr's theory were valid, in order to counteract this grant of police power given by the *Historical Cell Site* court, the Supreme Court would be expected to limit police power through *Riley*.

152. United States v. Jones, 132 S. Ct. 945, 954 (2012).

153. *In re* United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

154. Riley v. California, 134 S. Ct. 2473, 2495 (2014).

155. *Jones*, 132 S. Ct. at 954.

156. *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 600 (5th Cir. 2013).

157. *See id.*

158. David Kravets, *Which Telecoms Store Your Data the Longest? Secret Memo Tells All*, WIRED (Sept. 28, 2011, 6:30 AM), http://www.wired.com/2011/09/cellular-customer-data.

Because the *Riley* Court mentioned both Justice Sotomayor's "digital age" concurrence in *Jones* and historic cell site location data in their analysis of *Riley*, the Court seemed to analogize the large amount of data available for low cost to police by using a GPS tracking device or through requests to a cell phone provider as to the amount of data available on a smartphone found on an arrestee's person. However, GPS trackers or a request for cell site location information from a third party only reveal historical metadata, while data available on cell phones is typically much more detailed.

In Kerrian terms, the *Riley* Court recognized that that the information available in a comprehensive cell phone search give police too much surveillance power and sought to restore a balance of this power and privacy rights that existed in the pre-digital era.[159] Allowing police the power to examine every aspect of a cell phone user's life because there was probable cause to arrest him for one crime shifts the balance so far that the Court could not stand for it.[160] Thus, by declining to give police this tool, the Court provided more robust privacy rights to the arrestee. Because the Court adjusted the balance back towards individual's privacy rights after Congress enacted the SCA, *Riley* seems to validate Kerr's theory.

Together, these cases and statutes do not signal the significant shift that one looks for to disprove Equilibrium-Adjustment. Kerr's theory thus seems to hold through *Riley*, and can arguably assist in predicting the outcome of cases currently pending in various federal courts.[161] Upon closer examination, however, this analysis also shows a few flaws in Kerr's

159. *See Riley*, 134 S. Ct. at 2495. The Court specifically wrote:

> The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Id.

160. *See id.*

161. As an interesting thought experiment, applying Kerr's theory may allow attorneys and law enforcement officers to predict what the court will do in upcoming cases such as *United States v. Davis*. *See Davis*, 754 F.3d at 1209, *reh'g en banc granted, opinion vacated*, 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). Assuming the en banc panel holds as expected, that the SCA comports with the Constitution, Kerr's theory predicts that the Supreme Court will uphold the statute. As it stands, *Riley* has demanded that police secure a warrant before collecting digital data from a cell phone. To maintain the equilibrium, the Supreme Court will likely not also demand that police obtain a warrant to gain access to historical cell phone location data from a third party. While the Court has hinted that it may be time to revisit the third party doctrine, Kerr's theory predicts that it will unlikely do so through an appeal of *Davis*.

claim that Equilibrium-Adjustment can draw connections among the large body of Fourth Amendment jurisprudence. The next Part of this Note uses the above analysis to illustrate and explain three limitations on Kerr's claim that his theory can explain a variety of results of Fourth Amendment cases: (1) the application of the theory can vary between analysts, (2) it does not specify what information should be used to determine the equilibrium that ought to be restored, and (3) it fails to account for actions of private actors that don't fit in to any of Kerr's categories.

IV. ISSUES WITH EQUILIBRIUM-ADJUSTMENT

The previous application of Kerr's theory to *Riley* illustrates some tensions with the theory. Kerr's claim that his theory can explain a variety of Fourth Amendment cases should thus be taken with a grain of salt. First, the theory is inherently analyst-dependent and overbroad. Second, it does not explain if lower court decisions, previously unaddressed technologies, or the state of technology that exists when the Court is actually deciding a case should be used to determine the equilibrium sought to be restored. Finally, the theory fails to account for actions of private actors that change the status quo but do not introduce new crimes or practices.[162]

A. RESOLUTION OF EQUILIBRIUM-ADJUSTMENT VARIES WITH THE ANALYST

One of the main critiques of Kerr's thesis is that it closely resembles an already existing theory: originalism.[163] Thus, the argument goes, the theory suffers from the same problems as originalism. Specifically, a given case is analyst-dependent (as the way people define Year Zero may vary) and therefore the theory lacks predictive power.[164]

Kerr has already responded to this criticism by illustrating how equilibrium-adjustment occurred in *Jones*:

162. A primary counterargument may be that the *Jones*-SCA-*Riley* setup was not the only way to apply Equilibrium-Adjustment to *Riley*. Yet this application was the best way to establish the state of technology that existed before *Riley* that the Court also considered. The Court relied on the state of the balance between police power and privacy rights set up above to reach its conclusion. Thus, Kerr would likely hold that those cases were the ones that factored into the Court's equilibrium which they sought to restore through its holding.

163. *See generally* Christopher Slobogin, *An Original Take on Originalism*, 125 HARV. L. REV. F. 14 (2011).

164. *Id.*

> The three opinions in *Jones* proceed from different premises. One is originalist; two are not. . . . The majority opinion seeks to preserve the privacy protections that existed in 1791; the concurring opinions seek to preserve the privacy protections that existed in the "pre-computer age" (in Justice Alito's words) or before "the digital age" (in Justice Sotomayor's). But all three opinions interpret the Fourth Amendment to restore a prior level of government power. All three opinions engage in equilibrium-adjustment.[165]

This argument, however, illustrates an inherent problem with the theory. Kerr argues that each opinion in *Jones* created a different Year Zero for the purpose of their analysis, but that only the majority opinion is "originalist." Each opinion, however, created its own "original" balance of power it sought to restore. Just because a Justice can define Year Zero as some time after the 1700s does not exempt the theory from the same criticisms levied at originalism: application of the theory to a case inherently depends on the analyst and the theory lacks predictive power.

First, the application of equilibrium-adjustment in *Riley* was analyst-dependent. The majority of the *Riley* Court quoted Sotomayor's "digital age" approach in *Jones*, implying that the *Riley* Court's Year Zero was a time before the digital age, even though none of the other Justices had concurred with her in the context of *Jones*.[166] In fact, the *Riley* Court had the benefit of selecting from three different kinds of analyses done in *Jones*, and could possibly have selected any of them. The fact that the Court chose to focus on Justice Sotomayor's concurrence implies that they selected which equilibrium they choose to restore. Yet if another commentator believed that the true equilibrium to focus on should be something other than the balance of power that existed in the pre-digital age, that commentator would claim that the Court did not actually engage in equilibrium-adjustment.

Second, the theory lacks predictive power. Moving forward, how is a Court to analyze related issues? Are all issues dealing with digital technology now under the *Riley* umbrella, or may a future Court ignore *Riley's* proscription of a new rule for digital technology and return to Scalia's trespass theory in *Jones* or the even more generic "reasonable

165. Orin S. Kerr, *Defending Equilibrium-Adjustment*, 125 HARV. L. REV. F. 84, 89 (2011).

166. Note that the concurrence agrees with the need for a new rule in the digital era. Justice Alito wrote only to disagree with the need to limit the search incident to arrest exception to the *Chimel* factors. This issue is irrelevant to Kerr's equilibrium-adjustment analysis.

expectation of privacy" theory in *Katz*? Kerr's theory fails to explain how this might play out. If a Court adopts Scalia's trespass theory, police would have to physically place tracking technologies on a suspect themselves; using a remote technique would not create liability, regardless of how invasive the search actually might be. A "reasonable expectation of privacy" approach would cover more activities than the trespass approach, as society may have expectations of privacy that remote police activities would violate. For example, a Court adopting the Alito approach would find an activity like remotely hacking into the hard drive of a suspect's mobile device without a warrant to be an unconstitutional search, while the Scalia approach would not because it does not involve any physical trespass onto a suspect's property. The Alito approach might also differ from the Sotomayor approach in that it may find a warrantless search of a cell phone incident to arrest reasonable because suspects could have the contents of their pockets searched incident to arrest in the pre-computer age. It may thus be reasonable to believe that society is not willing to protect an expectation of privacy in an arrestee's pocket contents. Finally, a Court that adopts Sotomayor's emphasis on needing new rules for the digital age would find that searching a cell phone found incident to arrest is a constitutional violation; this is what occurred in *Riley*. Thus, given which opinion a Court decides to apply in the future, the result can be very different. Because Kerr gives no guidance on which opinion should be most influential in this situation, the theory creates a circular argument with regards to how a Court defines the equilibrium: the equilibrium is that which the Court sought to restore because that is the balance of power the Court selected as their Year Zero.

Kerr's defense of his theory through his illustration of how equilibrium-adjustment is achieved in *Jones* exposes another inherent flaw. The theory is so broad that Kerr can argue that the three very different kinds of analysis in *Jones* fit within it. Is a court engaging in equilibrium-adjustment every time they consider the balance of police power and privacy rights within the context of the Fourth Amendment? If yes, then Kerr is simply giving *Katz's* "reasonable expectation of privacy" test a new name and it becomes unclear that the theory encompasses cases that diverge from this analysis. If no, then Equilibrium-Adjustment fails in the same way as originalism fails: it is inherently analyst-dependent and lacks predictive power.

Finally, even if Kerr admits that his theory lacks predictive power, there also exist challenges in applying his theory retroactively.[167] *Riley* provides a good example about how one can apply the same theory to come to opposite conclusions: one could argue that the equilibrium in *Riley* was either maintained or ignored. Those arguing that *Riley* validates Kerr's thesis would point out that the case's conclusion, that police may not search a cell phone incident to arrest, did technically adjust the status quo. Yet opponents will note that this holding is potentially limited to the search incident to arrest exception, causing a very minor restoration of the balance that existed in the pre-digital age. The Court even left open the possibility that exigent circumstances that threaten the destruction of evidence may be enough to allow a search as in *Riley*. In addition, as a day-to-day matter, the easy-to-surmount "voluntariness" standard for consent to search a phone may affect the majority of cases with similar facts.[168] By leaving open the possibility that other warrant exceptions may justify a warrantless search of a cell phone, it remains unclear that the Court effectuated a significant restoration of the equilibrium that existed before cell phones were searched for evidence of crimes. Thus, *Riley* illustrates how Kerr's thesis is analyst-dependent, allowing commentators to see what they want to see in the Court's analysis, and cautions against

167. *See* Kerr, *supra* note 165.

168. Mark Eckenwiler, a former deputy chief of the Justice Department's computer crime section[,] . . . said that Chief Justice Roberts's opinion allows searches when the owner of the phone gives consent, and that "police will now, as a routine matter, ask for consent. . . . And an extraordinary number of arrestees will give that consent," Mr. Eckenwiler said, "just as people consent today to all sorts of searches of cars and containers, very much against their personal interest."

John Schwartz, *Cellphone Ruling Could Alter Police Methods, Experts Say*, N.Y. TIMES (June 25, 2014), http://www.nytimes.com/2014/06/26/us/cellphone-ruling-could-alter-police-methods-experts-say.html.

As a brief aside, Kerr's theory also fails to account for how technology may implicate other issues in connection with a Fourth Amendment argument. For example, what would happen if Riley's phone was locked, requiring him to provide a passcode to police? Would the *Riley* court have determined that this functioned as implicit consent to search the phone, or would it still address the issue under the search incident to arrest warrant exception? This situation would implicate Fifth Amendment self-incrimination issues, but it is unclear how Kerr would factor this into the equilibrium analysis. Note that courts are struggling with this question. *See Virginia v. Baust*, No. CR141439, 2014 WL 6709960, at *3 (Va. Cir. Ct. Oct. 28, 2014) (holding that a fingerprint was not testimonial and thus not protected under the Fifth Amendment).

accepting the theory as a broad resolution of the messy state of Fourth Amendment law.

B. THE DEFINITIONS OF THE EQUILIBRIUM ARE UNCLEAR

Another issue arises when trying to determine which "equilibrium" a court is trying to maintain. While Supreme Court holdings apply across the whole country, circuit and district courts make geographically scoped decisions that are sometimes in conflict. This makes it unclear to determine which lower court decisions should factor into the equilibrium analysis, if any. This becomes especially relevant when the Supreme Court does not actually deal with every technology that may upset the balance; how does the existence of those technologies factor into the equilibrium analysis? To further complicate matters, technology develops quickly and may outpace the rate of decision-making at the Court. How does rapidly changing technology factor into the Court's analysis? Kerr's theory does not acknowledge the fact that different balances between police power and individual rights exist in different jurisdictions, and thus the Court's nationwide rulemaking may affect each balance differently.

First, Kerr does not clarify how the Court should treat inferior courts' decisions when attempting to restore the equilibrium. This can be especially problematic for Kerr's theory when there is a split in authority regarding the effect of a certain technology under the Fourth Amendment. It seems like lower court decisions must be factored into the Court's thinking in some way, because they too establish the balance of police power and individual rights in their respective jurisdictions. For example, in *Riley*, the Court mentioned the ability of police to gather historic cell site information from the user's device as a reason for why a search warrant is necessary.[169] Yet *Historical Cell Site* upheld the constitutionality of the SCA, which allows for acquisition of similar information from a third party with just a subpoena.[170] Thus, by emphasizing that a search of a cell phone can reveal historical cell site location as justification for requiring a search warrant, the Court potentially affected the Fifth Circuit more than any other.[171] Kerr's theory fails to acknowledge that the Court's decisions create the same rules in every jurisdiction, even though there may be a

169. Riley v. California, 134 S. Ct. 2473, 2489 (2014).

170. *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 600 (5th Cir. 2013).

171. This is the issue that the Fifth Circuit in *United States v. Guerrero*, No. 13-50376, 2014 WL 4476565 (5th Cir. Sept. 11, 2014), had to tackle. The Fifth Circuit held that *Riley* did not affect police power under the SCA because the *Riley* Court did not explicitly overrule *Historical Cell Site*.

different balance of police power and individual rights in each. The Court could thus restore or upset balances with the same holding based on how the new rules affect different jurisdictions.

One may counter the previous argument by claiming that Kerr's theory only incorporates the equilibrium established by the Court itself, making any lower court decisions irrelevant. Yet this argument is problematic because the Court frequently addresses new technologies without having ever addressed preceding technology. If analysts are only to consider the Court's cases when engaging in equilibrium-adjustment, how does predecessor technology factor into the definition of the equilibrium?

This conundrum becomes clear in cases like *Maryland v. King*, where the Court held that "taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."[172] In his dissent, Justice Scalia argued that this justification was flawed because the Court had never addressed the constitutionality of fingerprinting technology itself and had yet to do so even in this case.[173] Could the Court have decided the case the same way without considering fingerprinting practices? Was fingerprint database technology a part of the equilibrium though it had never been considered by the Court?[174] If previously undiscussed technology could factor into the equilibrium, how is an analyst of Fourth Amendment jurisprudence supposed to anticipate which precedent technology the Court will find meaningful? If Kerr is claiming that the Court is only meant to consider technology that it had previously commented on, then *Maryland v. King* is an important instance where the Court does not engage in equilibrium-adjustment. If the Court does not engage in equilibrium-adjustment in addressing such an important issue, the constitutional validity of warrantless DNA database searches, then perhaps Kerr's theory does not explain as much as he purports it does.[175]

172. Maryland v. King, 133 S. Ct. 1958, 1980 (2013).

173. *Id.* at 1987 (Scalia, J., dissenting) ("It is on the fingerprinting of arrestees, however, that the Court relies most heavily. The Court does not actually say whether it believes that taking a person's fingerprints is a Fourth Amendment search, and our cases provide no ready answer to that question.").

174. These questions just skim the surface. In addition, more can be learned about an individual with DNA than with a photo. In Year Zero, one could not collect physical information from someone and use it to determine that the person was related to the actual offender—the purpose of DNA sweeps.

175. The following further illustrates this dilemma. If the use of a fingerprint database was previously a police power that the Court considers part of the equilibrium, wouldn't the Court have attempted to balance police power and privacy rights and deny police the ability to use an even more intrusive technology? Either they shouldn't be

Finally, it remains unclear how the general change of technology affects how the Court may answer the issues before it. Kerr does not explain if the Court does, or should, consider the current state of technology when deciding cases on the facts before them. Does the Court only define the equilibrium as whatever existed prior to the initiation of the police activity in question, or does the Court factor in the current state of technology when attempting to restore the equilibrium? If the former, then the Court could be making rules about already outdated technologies that may no longer be relevant. If the latter, then the Court could be providing advisory opinions. Either way, even if Kerr's theory indeed can explain previous holdings of the Court, it still does not explain how to determine what effect current technology has on the equilibrium the Court is attempting to restore.

C. THE THEORY IS MISSING A CATEGORY: INTERVENING PRIVATE ACTORS

Finally, Kerr's theory could benefit from considering a seventh category of technological change: the destabilizing effect of private actors. This category is similar to Kerr's "new crimes and new practices," where new social or political developments emerge but crime occurs using the same technologies. Yet "new crimes and new practices" does not call for analysis of the increasing ubiquity of already existing practices.

Because of the rate at which they can act, private actors can cause a sudden shift in the status quo. After *Riley*'s mandate that police obtain a search warrant before searching the phone of an arrestee, actions by private companies may do more to alter the balance than the Court could have anticipated. One of the main examples of this effect comes from top tech companies Apple and Google, which recently announced their new default data encryption software for mobile devices.

On September 17, 2014, Apple CEO Tim Cook announced that the company would be encrypting all data communicated between their servers and the customers in order to prevent Apple's ability to share such information when subpoenaed.[176] A corresponding letter from Mr. Cook

accounted for in the equilibrium sought to be restored because the Court has never spoken on those topics, or the Court isn't actually engaging in equilibrium-adjustment because they continue to uphold police power within certain technological groups (like using biometric data to identify suspects without a warrant). Kerr's theory fails to account for these effects when establishing which equilibrium the Court is considering in each case.

176. *See* Cyrus Farivar, *Apple Expands Data Encryption Under iOS 8, Making Handover to Cops Moot*, ARS TECHNICA (Sept. 17, 2014, 9:57 PM),

on the privacy section of the Apple website states the following: "I want to be absolutely clear that we have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will."[177] The Apple website goes on to explain exactly what data law enforcement cannot get from Apple:

> On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.[178]

Essentially, "[w]hat is new is *the amount of data* your phone will now encrypt. Apple has extended encryption protections to nearly all the data [users] produce on a daily basis and will also require you to enter the passcode (or fingerprint) each time [users] reboot [their] phone."[179] Top competitor Google has also implemented default encryption with the release of its latest operating system.[180]

---

http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot; Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html.

177. *A Message from Tim Cook About Apple's Commitment to Your Privacy*, APPLE, http://www.apple.com/privacy (last visited Feb. 13, 2015). Note that while technically Apple has not allowed outside parties direct access to their servers, they claim that "0.00358% of customers had data disclosed due to government information requests," and that they received 250 or less of those kinds of requests in the first sixth months of 2014. *See* Apple Privacy Policy, Government Information Requests APPLE, http://www.apple.com/privacy/government-information-requests (last visited Feb. 13, 2015).

178. Apple Privacy Policy, Government Information Requests, APPLE, http://www.apple.com/privacy/government-information-requests (last visited Feb. 13, 2015). Recall that some of the evidence introduced against Riley included photos found on his iPhone.

179. Matthew Green, *Is Apple Picking a Fight With the U.S. Government?*, SLATE (Sept. 23, 2014), http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html (emphasis in original).

180. *See* Andrea Petersen, *Google Officially Announces Android 5.0 'Lollipop' with Default Encryption*, WASH. POST (Oct. 28, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/28/google-officially-announces-android-5-0-lollipop-with-default-encryption.

This change is sudden enough that it has instigated serious debate and an outcry from the law enforcement community. Reporters have already noted that "[i]n June, the Supreme Court ruled that police needed search warrants to gain access to data stored on phones in most circumstances. But that standard is quickly being rendered moot; eventually no form of legal compulsion on service providers will suffice to force the unlocking of most smartphones."[181] FBI Director James Comey has already shared that "he doesn't understand why companies would 'market something expressly to allow people to place themselves beyond the law.'"[182] Comey and others have called on Congress to act to ban default smartphone encryption.[183] Unfortunately for Comey, members of Congress have already expressed that there is "zero chance" of the FBI Director's proposal passing.[184] If Congress does not act, might it fall to the courts once again to handle the matter through the slow and blunt judicial tool that Justice Alito feared in his concurrence in *Riley*?[185]

The fact that law enforcement may not be able to get the information they need through serving warrants on the service providers raises an interesting question: If *Riley* were in front of the Court today, would these announcements change the outcome of the case? It is possible; because the Court left open the potential for exigent circumstances to be a valid exception, it seems likely that an argument claiming that evidence is permanently lost once a phone locks could be persuasive. Thus, if these announcements occurred before the case was decided, it might have been argued as a different warrant exception and the outcome might have

181. *Id.*

182. Brian Naylor, *Apple Says iOS Encryption Protects Privacy; FBI Raises Crime Fears*, NPR (Oct. 18, 2014), http://www.npr.org/blogs/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears. Comey's reaction is still not as extreme as that of others like John Escalante, the chief of detectives in Chicago, who said the iPhone would become "the phone of choice for the pedophile." *Id.*

183. *See* Jason Keobler, *FBI Director: If Apple and Google Won't Decrypt Phones, We'll Force Them To*, MOTHERBOARD (Oct. 16, 2014, 11:20 AM), http://motherboard.vice.com/read/fbi-director-if-apple-and-google-wont-decrypt-phones-well-force-them-to.

184. Jason Keobler, *Congress to the FBI: There's 'Zero Chance' We'll Force Apple to Decrypt Phones*, MOTHERBOARD (Oct. 20, 2014, 9:25 AM), http://motherboard.vice.com/read/congress-to-the-fbi-theres-zero-chance-well-force-apple-to-decrypt-phones.

185. Riley v. California, 134 S. Ct. 2473, 2497 (2014).

different.[186] Whether or not this would have ultimately happened is not important; this thought exercise illustrates that Kerr's theory does not clearly account for the potential of private actors to change the Court's analysis. In this time of fast-paced technological evolution, intervening private actors may be the most important actors in upsetting the balance between police power and individual privacy rights. The failure to acknowledge these kinds of effects shows the theory is underinclusive.

Kerr's discussion of judicial delay highlights one possible way to handle the issue of private action.[187] Because these actors drive changes in technology, the Court could wait until the use of the technology stabilizes before weighing in with a decision. The *Katz* test itself is dependent on stable expectations of privacy, as the second part of the test requires that the expectation of privacy is one which society is ready to recognize. If expectations are shifting along with technology, it may be impossible for the Court to effectively weigh in on the case. After all, Apple has just changed the status quo of who has access to encryption, but the technology itself has not changed. Thus, police can still use the same tools they currently do when they need access to an encrypted phone. Until this movement to default encryption sparks an empirically proven paradigm shift, the Court should delay any decisions that may disturb the naturally forming equilibrium before it has a chance to stabilize.

Yet given the rate at which technology is developing, it is possible that private actors may move quickly enough to prevent a stable equilibrium from ever forming before the Supreme Court considers an issue. Thus, even Kerr's recommendation of Judicial Delay may not suffice to address the legal issues that these actors cause. Because Courts cannot delay dealing with issues forever, Kerr should amend his Equilibrium-Adjustment theory to explain how a Court deals with the actions of third parties that do not introduce a new practice but still lead to a disruption of the balance between police power and individual rights.

186. We may still see this argument appear in the future. In fact, *Riley* might have the effect of encouraging police to find "exigent circumstances" in more cases. Did default encryption counter-intuitively undermine the balance maintenance of *Riley*?

187. *See* Orin Kerr, *Apple's Dangerous Game*, WASH. POST (Sept. 19, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game ("Incidentally, I have long argued that the Supreme Court should wait until a technology stabilizes before applying the Fourth Amendment to it to avoid the problem of announcing a rule that doesn't make sense over time. In light of Apple's new iOS8, *Riley* may be an interesting example.").

V. CONCLUSION

Riley, related cases, and the response from both the courts and private sector raise fascinating questions about how the Fourth Amendment protection against unreasonable searches and seizures will function in an increasingly digital age. The search incident to arrest warrant exception already bars police from searching mobile phones without a warrant; if a phone "locks" before police can obtain a warrant, and police cannot compel a company or the individual to give them the password, will such technology completely stall any investigation? As technology continues to evolve, will the courts' Fourth Amendment holdings continue to be made immediately less relevant by private action? If police have the ability to hack a phone, does *Riley* even significantly change the ultimate outcome of cases; in other words, is the protection of a warrant strong in these cases, or is it just a matter of how long it will take police to get data from a mobile device? If technology evolves too quickly for the courts to establish a stable, long-term equilibrium, could this indicate that society is ready for a shift in the equilibrium away from the Year Zero balance? Does the prevalence of digital data mean that we need to establish a new norm instead of trying to return to the old norm? When only the user knows passcodes or encryption keys, does the use of encrypted technology run afoul of the Fifth Amendment and its proscription against compelling self-incriminating statements?

Kerr's Equilibrium-Adjustment theory does little to answer these important questions. It assumes that the Court's Year Zero is clearly definable. It fails to account for changes from the private sector that may push courts to provide more power to police. The theory is so broad that it can encompass seemingly unlimited different kinds of analyses, raising uncertainties about its utility. It is unclear in how to deal with lower court decisions or the precise way in which the Court reaches a conclusion. These issues are inherent flaws in Kerr's claim that his theory can explain "a great deal of the overall shape and substance of Fourth Amendment doctrine."[188] Applying Kerr's Equilibrium-Adjustment theory to *Riley v. California* illustrates these flaws and cautions against overvaluing Kerr's theory.

188. Kerr, *supra* note 1, at 481.