Volume 1, No. 5 | September–October 2018

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 1, No. 5 | September–October 2018

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Everything Is Not *Terminator*

The Search and Seizure of AI Devices and Programs Under the Fourth Amendment

John Frank Weaver*

The movie *Minority Report* is nominally a science fiction story about "precogs," human psychics who assist police to stop crimes before they happen. In one scene, the film shows "precrime" cops arresting a man *before* he actually harms his spouse. Although I was barely out of college and several years from law school when I first saw it, at the time, I couldn't help but wonder, "Is that arrest Constitutional?" More recently, I've been wondering the same thing about how law enforcement may start to use artificial intelligence. Although researchers are exploring using AI algorithms to predict the future in controlled settings,[1] no one is suggesting *Minority Report* style future crime reports. Rather, I wonder how law enforcement and courts will apply the Fourth Amendment to AI when AI programs and AI-enabled devices are searched. Many forms of AI rely on extensive personal data and on tracking our preferences and actions. Depending on how courts and law enforcement apply the Fourth Amendment's search and seizure requirements, it could become very easy to gain access to that data and analysis. To properly address AI, courts will need to expand societal expectations of privacy and areas where warrants are required before searching.

Very Briefly, Searches and Seizures Under the Fourth Amendment

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

Robotics, Artificial Intelligence & Law / September–October 2018, Vol. 1, No. 5, pp. 341–347.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Amendment was included in the Bill of Rights in 1791, proponents were primarily concerned with ensuring that police and government searches and arrests would be reasonable and limited to instances when a specific warrant was obtained.[2]

Technological developments in the last 50 years have forced courts to consider searches and seizures in the context of devices never envisioned by the Founding Fathers: a thermal imaging device that can detect heat associated with lights for growing marijuana;[3] a GPS device attached to a car that can track the suspect's movements;[4] a device that can search and download all of the stored data in a cell phone;[5] etc. Traditionally, courts use a two-part test to determine if law enforcement officers have actually conducted a search and seizure under the Fourth Amendment: (1) has the person exhibited an actual expectation of privacy in the area or thing searched; and (2) would society find that expectation reasonable.[6]

If the police search the contents of your bag after you have dumped them in the middle of the sidewalk, that is not a search for the purposes of the Fourth Amendment because you did not act like the contents of the bag were private. Conversely, if you placed the bag in your car and locked the doors, a police search of the bag would qualify as a search under the Fourth Amendment because you acted like it was private and that was a reasonable assumption. Once you have established that the police actually conducted a search and seizure under the Fourth Amendment, then you can attempt to prove that the police violated your Fourth Amendment rights.

New Areas and Expectations of Privacy from Developing Technologies

In considering new technologies, courts have begun to establish new spaces within the terms "persons, houses, papers, and effects" of the Fourth Amendment where people have a reasonable expectation of privacy. For example, Chief Justice John Roberts, writing for the U.S. Supreme Court in *Riley v. California*, found that "cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life' … The fact that technology now allows an individual to carry such information in his hand does not make the

information any less worth of the protection for which the Founders fought."[7] In other words, cell phones are a new space where people have a reasonable expectation of privacy and the government must obtain a warrant to search a cell phone.[8]

Similarly, new technologies are prompting a reconsideration of privacy expectations. Historically, when people have done anything in public, they had little reasonable expectation of privacy. However, courts are rethinking this. While considering GPS devices and how they can aggregate public movements in *United States v. Jones*, Justice Sonia Sotomayor wondered about "the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[9] Her point is that few people consider what the sum total of their public activities and movements reveal about themselves. Up to this point, it was not an issue, as it was very difficult for the government or anyone else to track you that way, even in public. With GPS, everywhere you go can easily be data for the Government or another party to analyze and from which to draw conclusions. Unless we are comfortable with how those conclusions can affect us without our knowledge or consent, we should rethink our expectation of privacy.

In that decision, Justice Sotomayor also discussed reconsidering the principle that sharing information with other people eliminates someone's expectation of privacy. "More fundamentally," she notes, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[10] Again, her message is that emerging technologies change how we should conceive of reasonable expectations of privacy. That is particularly true when considering how AI will affect our privacy and the spaces we use for privacy.

The line of case law developing around cell phones is helpful in identifying how AI will challenge Fourth Amendment jurisprudence. In *Riley*, the Supreme Court properly recognized cell phones as a space where people have a reasonable expectation of privacy, requiring a warrant to search them. However, the Court did not address natural follow-up questions: How specific does a warrant

have to be? What evidence is required to obtain a warrant? The high Court will almost certainly be called to address those questions, but in the meantime, lower courts are trying to do so.[11]

Unfortunately, early results suggest that courts do not understand how most people generate and store personal data in their phones, a misunderstanding that has serious implications for AI-based devices. For example, in *Commonwealth v. Dorelas*, the Massachusetts Supreme Judicial Court considered how specific a warrant must be before police can search an iPhone.[12] Defendant Denis Dorelas was arrested following a shooting. While investigating the shooting, witnesses told police that Dorelas had received threatening phone calls and text messages from the other individual involved in the shooting. Based on this evidence, police applied for and received a warrant to search Dorelas' iPhone for his:

> name and telephone number, contact list, address book, calendar, date book entries, group list, speed dial list, phone configuration information and settings, incoming and outgoing draft sent, deleted text messages, saved, opened, unopened draft sent and deleted electronic mail messages, mobile instant message chat logs and contact information mobile Internet browser and saved and deleted photographs… [as well as] information from the networks and carriers such as subscribers information, call history information, call history containing use times and numbers dialed, called, received and missed.[13]

In other words, because two guys said that Dorelas received text messages and calls that might be relevant, the police were permitted to search *almost every kind of data* the phone contained. Some of the photographs showed Dorelas holding a gun, resulting in him getting charged with several firearm-related offenses. The Massachusetts Supreme Judicial Court ruled that the search and seizure of the phone was reasonable, noting that electronic communications "can come in many forms" and the issuing judge "could conclude that the evidence sought might reasonably be located in the photograph file," despite the fact that the only evidence supporting the search of the iPhone was testimony that referenced phone calls and texts.[14] Equating texts and phone calls with all electronic communications is a huge expansion of those forms of evidence and grants broad discretion to police to search *all* the data on a

phone as long as there is evidence suggesting that *any* data on the phone could be related to criminal activity.

AI's New Private Areas and Expectations of Privacy

This poses real problems for AI-enabled devices and programs, which potentially have similar data caches. For example, each Amazon Alexa keeps a record of all of the inquiries it receives.[15] A human user can review a list of his or her inquiries in reverse chronological order through the Alexa app. The different types of personal data are easily distinguished: music selections, purchase orders, informational inquiries, personal communications, etc. Following the logic of *Dorelas*, law enforcement officers who receive testimony that a suspect purchased an object found at a crime scene could receive a warrant to search *all* the data stored with Alexa.

Further, AI programs and devices like Alexa can collect personal data even when we do not consciously provide that data. "Alexa does listen to every word it can hear," Amazon warns users.[16] Although the company goes on to note that most of that verbal input is not stored in the local Alexa unit or sent to the cloud,[17] the possibility exists that anything you say in the presence of an Echo (which operates the Alexa program) could be collected, stored, and ultimately seized by law enforcement.

Where do cases like *Riley*, *Jones*, and *Dorelas* leave AI products under the Fourth Amendment? First, similar to Justice Sotomayor's observation in *Jones*, there should be a reasonable societal expectation of privacy in the sum of one's mundane movements, statements, actions, etc., that are recorded and analyzed by AI, particularly because such recordings can happen without our knowledge. If the government were to have access to such aggregation of an individual's personal data, law enforcement could gain a great deal of knowledge about any individual. Requiring a warrant before searching any AI program or device is a reasonable safeguard against that.

Those expectations are almost certainly established, or well on their way, after *Riley* required warrants for searches and seizures of cell phones. But the proper treatment of AI under the Fourth Amendment also requires a refutation of *Dorelas*. Like iPhones, AI-enabled programs and devices sort and save different types of data—photos, texts, internet history, etc.—in different directories,

which function as distinct virtual locations. In other words, for Fourth Amendment purposes, AI is creating new areas to store information that was once stored exclusively in "persons, houses, papers, and effects." Police will need to submit an application supported by evidence describing each data area with particularity before receiving a warrant to search each one.[18]

The Fourth Amendment was drafted and adopted at a time when information was not stored in the cloud, collected autonomously, or analyzed by aggregating the sum of many individual actions or statements. All recorded, private information took up *tangible space.* AI-enabled programs and devices can store abundant information and conduct analysis about each of us in negligibly small spaces, which, in some cases, can be accessed in locations worldwide. As AI applications become more widely used, those spaces should be recognized and receive full Fourth Amendment protection.

Notes

* John Frank Weaver, an associate at McLane Middleton and a member of the firm's corporate and real estate practice groups, is the "Everything Is Not *Terminator*" columnist for *The Journal of Robotics, Artificial Intelligence & Law.* Mr. Weaver, who may be contacted at john.weaver@mclane.com, has a diverse practice that focuses on land use, real estate, telecommunications, and emerging technologies, including artificial intelligence, self-driving vehicles, and drones.

1. *See* Théophane Weber, "Imagination-Augmented Agents for Deep Reinforcement Learning," February 14, 2018, *arXiv.org,* https://arxiv.org/abs/1707.06203; Razvan Pascanu, et al., "Learning model-based planning from scratch," July 19, 2017, *arXiv.org,* https://arxiv.org/abs/1707.06170.

2. This statement represents a reconciliation of irreconcilable positions taken by Akhil Reed Amar and Thomas Y. Davies. Amar believes that the Framers wanted to ensure "that all government searches and seizures be reasonable." Akhil Reed Amar, *Fourth Amendment and First Principles,* 107 Harv. L. Rev. 757, 759 (1994). Davies believes that the Framers "aimed the Fourth Amendment precisely at banning Congress from authorizing use of general warrants; they did not mean to create any broad reasonable standard for assessing warrantless searches and arrests." Thomas Y. Davies, *Recovering the Original Fourth Amendment,* 98 Mich. L. Rev. 547, 724 (1999-2000). Both present reasonable and compelling arguments. Because the difference is irrelevant to this article, I have chosen to adopt aspects of each.

3. *Kyllo v. United States*, 533 U.S. 27 (2001).

4. *United States v. Jones*, 565 U.S. 400 (2012).

5. *Commonwealth v. Dorelas*, 473 Mass. 496 (2016).

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

7. 134 S. Ct. 2473, 2495 (2014).

8. *See id.,* at 2495. Although this is generally true, the exceptions that exist when "special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impractical" likely remain exceptions for the search of a cell phone and other new spaces made possible by technological advancements. *See Skinner v. Railway Labor Executives Association*, 489 U.S. 602, 619 (1989).

9. 565 U.S. at 416 (Sotomayor, J., concurring).

10. *Id.,* at 417 (Sotomayor, J., concurring).

11. *See* William Clark, *Protecting the Privacies of Digital Life: Riley v. California, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants,* 56 B.C.L. Rev. 1981 (2015).

12. Full disclosure: I helped the American Civil Liberties Union of Massachusetts draft its amicus brief for this case. *Commonwealth of Massachusetts v. Dorelas*, No. SJC-11793 (Commonwealth of Massachusetts Supreme Judicial Court), Brief of *Amicus Curiae,* American Civil Liberties Union of Massachusetts, filed March 27, 2017 ["Dorelas Brief"].

13. *Dorelas*, 473 Mass. at 499.

14. *Id.,* at 503.

15. *See* Amazon, Amazon Alexa: What kind of data does Amazon get from me?, https://www.androidcentral.com/amazon-alexa-what-kind-data-does-amazon-get-me, accessed on May 17, 2018.

16. *Id.*

17. *Id.*

18. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (authorization of search warrant must be limited "to the specific areas and things for which there is probably cause to search, [a] requirement ensur[ing] that the search will be carefully tailored to its justifications"); Dorelas Brief, at 12-18, 22-27.