# WHEN ROBOT EYES ARE WATCHING YOU: THE LAW & POLICY OF AUTOMATED COMMUNICATIONS SURVEILLANCE

Kevin S. Bankston & Amie Stepanovich[1]

## ABSTRACT

*Robots are reading your email. Right now.*

*Whether it's the National Security Agency scanning for suspicious keywords, Google trying to divine your interests so that it can serve better ads, or your ISP scanning for viruses and spam, computers are routinely scanning the content of your private messages, along with those of millions of other Internet users. Sometimes with your knowledge and consent. Sometimes without.*

*Many civil libertarians argue that having robots read your email is just as bad as having a human do it—perhaps even worse, considering robots can work at a much greater scale and speed, and have perfect memories. Others, like Judge Richard Posner, have argued that there is no privacy violation at all unless a sentient being has committed the violation, and that automated filtering for relevant communications actually protects privacy by preventing humans from looking at the wrong messages. Both Google and the NSA routinely defend the practice of scanning millions of people's private communications by saying that there are strict limits on which emails people can actually look at. Is that enough?*

*This paper explores what the growing trend toward the automated analysis of masses of private communications means for the law and policy of privacy and surveillance, and will ask the question: when, if at all, does it "count", from a privacy policy and privacy law perspective, if a robot is reading your email? Does a government robot's reading of your email constitute a search or seizure of that email under the Fourth Amendment? And does robotic scanning of your email count as an "intercept" that is regulated by the federal wiretapping statute? This paper examines both questions, looking to statutory and constitutional case law to conclude that, from a privacy perspective, having a robot read your email is just as bad—and may be even worse—than its being read by a human.*



[1] Kevin S. Bankston is the Policy Director of the Open Technology Institute at the New America Foundation. Amie Stepanovich is Senior Policy Counsel at Access. The views expressed here are their own. Special thanks to Jadzia Butler for her extensive research and editorial assistance, and to Drew Mitnick for additional research assistance.

## I. The Question: Does It "Count" When Robots Read Your Email?

Robots are reading your email. Right now.

Right now, copies of your emails are being diverted into massive computers controlled by the National Security Agency (NSA). Emails that appear to be directed to or from a person outside of the United States are automatically scanned for key words and identifiers that are of foreign intelligence interest. If these computers—robots, if you will—discover that your email contains what the NSA is looking for, the email will be stored for potential future review or use; if they discover that your email doesn't contain any of the keywords or identifiers, the email is immediately discarded. Does this automated scanning of email constitute a massive wiretap of all of our international communications, under federal wiretap law? A search and seizure, under the Fourth Amendment? A violation of privacy, however defined?

Although this article focuses on the example of NSA surveillance, these questions reach far beyond the present NSA controversy. Courts are currently considering the extent to which e-mail providers can employ email-scanning robots to detect spam or serve targeted advertisements.[2] In addition, there is an ongoing conversation about the legal and privacy implications of Internet service providers' (ISPs) automatedly monitoring Internet traffic for any number of reasons, whether for advertising purposes, or to block or throttle the bandwidth used by particular applications, services or content.[3]

In all of these cases, as in case of the NSA, a singular question pervades: is an individual's privacy violated if no human eyes ever see any personal information or

[2] *See, e.g.*, In re: Google, Inc. Gmail Litigation, No. 13–MD–02430–LHK, 2013 WL 5423918 (September 26, 2013).
[3] *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417; Daniel J. Weitzner, "The Neutral Internet: An Information Architecture for Open Societies," MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY (May 1, 2007), http://dig.csail.mit.edu/2006/06/neutralnet.html.

communications from that individual? Essentially, can a robot alone violate privacy? More specifically, does automated scanning of an email, which is then discarded, constitute an interception of that communication under federal wiretapping law, or a search or seizure under the Fourth Amendment? Some would argue that a robot's "eyes", alone, could never violate a person's privacy.[4] This article argues otherwise. After reviewing in Part II the facts of the NSA wiretapping that serve as our testing ground for this question, we proceed to consider in Part III the statutory wiretapping question, and in Part IV the constitutional question. Under both statutory and constitutional law we conclude that a robot is, in essence, a proxy for and an agent of the humans that instruct it. We conclude in Part V that the mere fact that the act of reading the emails is automated does not decrease the invasiveness of that act, but instead intensifies the privacy invasion by exponentially increasing the accuracy, speed, and scope of surveillance. When human eyes are watching us, there are practical limits on how many of us and our communications can be spied upon. But when robot eyes are watching us, they can spy on *all* of us, *all* of the time.



## *INTERLUDE I: THE ROBOT IN ROOM 641A*

***The robot doesn't have arms or legs, eyes or ears. But it has a brain. And it's always working.***

***The robot, with its massive computational power, sits quietly in Room 641A, a secure and mysterious corner of AT&T's Folsom Street Facility in San Francisco. That***

[4] *See*, *e.g.*, Richard A. Posner, *Privacy, Surveillance, and The Law,* 75 U. CHI. L. REV. 245, 254 (2008) ("Computer searches do not invade privacy because search programs are not sentient beings. Only the human search should raise constitutional or other legal issues."); Bruce E. Boyden, *Can A Computer Intercept Your Email?,* 34 CARDOZO L. REV. 669 (2012) (arguing that automated review without human review is not an interception under federal wiretap law); and Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2010-2011) (arguing that automated review alone does not violate a reasonable expectation of privacy under the Fourth Amendment).

***facility is home to a key Internet exchange point that passes millions of emails per day between the various networks that comprise the Internet's backbone. A fiber optic splitter device has been inserted into the exchange point such that a copy of every Internet communication that passes through the facility is also copied and sent down another fiber optic cable…leading to the robot in Room 641A.***

***There the robot sits, feeding off the cable, reviewing the content of every email and instant message, looking for key "selectors"—names, addresses, phone numbers—that its human masters have instructed it to look for. The communications that do not contain a targeted selector pass through the robot's memory and are lost forever. Those that do contain a target selector are sent on by the robot to another, secret network, leading to a government database at the National Security Agency Headquarters at Fort Meade, or its massive new data center in the Utah desert or….***

***The robot is not alone. There are dozens of other robots just like it, sitting on top of Internet exchange points across the country, connected to the same secret network, fulfilling the same mission for the same masters. They are always reading. They never stop. And they never miss a thing.***

***This story is not science fiction. It is not hypothetical. It is the world we live in now.***

## II. The Facts: NSA's Secret Network of Email-Reading Robots

In June 2013, the world was informed about PRISM, one of the National Security Agency's programs implemented under the authority of Section 702 of the Foreign Intelligence Surveillance Act Amendments Act (FAA).[5] Via a series of slides, PRISM was described as a "downstream" data collection program – a program that gathers information that has been collected and stored by private companies.[6] The slides that revealed the PRISM program also referenced a separate "upstream" collection program.[7] One key slide explained that upstream collection constituted the "collection of

[5] Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; 50 U.S.C. § 1881a *et seq*.
[6] "NSA Prism Program Slides," THE GUARDIAN (November 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document.
[7] Craig Timberg, "The NSA Slide You Haven't Seen," WASHINGTON POST (July 10, 2013), http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.

communications on fiber cables and infrastructure as data flows past."[8] The Foreign Intelligence Surveillance Court, in a heavily redacted footnote in one of its published opinions, defined "upstream collection" as "NSA's interception of Internet communications as they transit [redacted], rather than to acquisitions directly from Internet service providers, such as [redacted]."[9] A detailed description of the upstream program was provided to the Wall Street Journal by government officials:

> The NSA asks telecom companies to send it various streams of Internet traffic it believes most likely to contain foreign intelligence. This is the first cut of the data…The second cut is done by NSA. It briefly copies the traffic and decides which communications to keep based on what it calls 'strong selectors' – say, an email address, or a large block of computer addresses that correspond to an organization it is interested in. In making these decisions, the NSA can look at content of communications as well as information about who is sending the data.[10]

Senator Diane Feinstein, the chairwoman of the Senate Select Committee on Intelligence, later confirmed that this program tapped directly into the "backbone" of the Internet – the fiber lines over which the whole of Internet traffic travels.[11] In a hearing before the Privacy and Civil Liberties Oversight Board (PCLOB) on March 19, 2014, NSA General Counsel Raj De offered a further confirmation, explaining that "there's two types of



[8] *Id.*
[9] [Redacted], 2011 WL 10945618, at *2 n. 3 (FISC Oct. 3, 2011).
[10] Siobhan Gorman and Jennifer Valentino-Devries, "New Details Show Broader NSA Surveillance Reach: Programs Cover 75% of Nation's Traffic, Can Snare Emails," WALL STREET JOURNAL (Aug. 20, 2013), http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470.
[11] Mike Masnick, "Dianne Feinstein Accidentally Confirms That NSA Tapped The Internet Backbone," TECHDIRT (Sep. 27, 2013), https://www.techdirt.com/articles/20130927/13562624678/dianne-feinstein-accidentally-confirms-that-nsa-tapped-Internet-backbone.shtml ("'Upstream collection…occurs when NSA obtains Internet communications, such as e-mails, from certain US companies that operate the Internet background [sic], i.e., the companies that own and operate the domestic telecommunications lines over which Internet traffic flows.'").

collection under Section 702," the second of which "is the shorthand referred to as upstream collection…, collection from the…Internet backbone…."[12]

The technology that facilitates such upstream data collection is described in greater detail in regard to one telecommunications provider in court filings in *Jewel v. NSA*, an ongoing case against the NSA that originally challenged the pre-FAA version of the upstream program:

> To divert the stream of communications to the government, AT&T connected the fiber-optic cables entering its WorldNet Internet room [Room 641A] to a "splitter cabinet." The "splitter cabinet" splits the light signals from the WorldNet Internet service in two, making two identical copies of the data carried on the light signal. The splitter cabinet directs one copy of the light signal through fiber optic cables into a secret room built on AT&T premises, but controlled by the NSA, while allowing the other copy to travel its normal course to its intended destination. The split cables carry both domestic and international communications of AT&T customers, as well as their communications from users of other non-AT&T networks that pass through the Folsom Street Facility.[13]

Essentially, as one government official has put it, "the NSA makes a 'clone of selected communications links' to gather the communications."[14] The court filings explain that the same process is carried out at several facilities across the country.[15] Subsequent revelations demonstrate that through such facilities, installed at key Internet exchange points belonging to a number of telecommunications providers, the NSA's data-mining equipment is able to capture the vast majority of the Internet traffic being transmitted inside the United States.[16]



---

[12] Privacy and Civil Liberties Oversight Board, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (March 19, 2014), *available at*: http://www.pclob.gov/Documents/19%20March%202014%20PCLOB%20Public%20Hearing_Panel%20I%20Transcript.pdf.

[13] Jewel v. NSA, Summary of Evidence, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/document/summary-evidence (internal citations omitted).

[14] Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.," NEW YORK TIMES (August 8, 2013), http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?smid=tw-share&_r=0.

[15] Jewel v. NSA, Summary of Evidence, *supra* note 13.

[16] Gorman and Valentino-Devries, *supra* note 10.

The process continues after the information has been copied: once the communications have been diverted into NSA-controlled computer equipment, devices that "'comb[] through large volumes of phone and Internet traffic' in a 'large data-mining operation.'"[17] In particular, these robots are looking for international communications that are "to, from, or about a tasked selector, or otherwise contain[] foreign intelligence information."[18] A "selector" is "a specific communications identifier or facility tasked to acquire information that is to, from, or about a target."[19] Communications "about" a tasked selector include those that are neither addressed to or from a target of surveillance,[20] but that "contain[] a reference to that selector."[21] Thus, if the NSA's robots detect a selector in the addresses *or* in the content of a communication, that

[17] Jewel v. NSA, Summary of Evidence, *supra* note 13.
[18] Minimization Procedures Used by the National Security Agency in Connection with Acquisition of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 5(b) (Oct. 31, 2011) *available at*: http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. However, the government has not always been able to ensure that the communications that are acquired fit within this broad scope. *See* [Redacted], 2011 WL 10945618, at *2 ("According to the May 2 Letter, such transactions may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection. [] The letter noted that NSA uses … to ensure that 'the person from whom it seeks to obtain foreign intelligence information is located overseas,' but suggested that the government might lack confidence in the effectiveness of such measures as applied to Internet transactions.").
[19] Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: June 1, 2012-November 30, 2012, A-2 (August 2013), *available at*: http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.
[20] "Procedures used by NSA to Target non-US Persons: Exhibit A-full document," THE GUARDIAN, at 1-2 (June 20, 2013), http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.
[21] *See* [Redacted], 2011 WL 10945618, at *5.

communication is stored for later human review, and if it does detect such a selector the communication is deleted; the process takes only a matter of seconds.[22]

The surprising fact that the NSA is not only targeting communications "to" or "from" its foreign intelligence targets, but is also scanning the contents of every email that crosses the border for information *about* its targets raises serious legal questions. The preliminary questions, which this article addresses, are: does such "about" searching of the content of emails count as an "intercept" of those communications under the federal wiretap statute, or as a search or seizure under the Fourth Amendment?[23] We address both of those questions in turn, and answer both in the affirmative.

### *INTERLUDE II: THE MAN IN ROOM 641A*

***Imagine that the robot in Room 641A has been replaced with a man, sitting at a monitor. The man is presented with an email passing by. He reviews it for keywords. If he sees one, he presses a button that saves the email. If he doesn't, he presses a button that deletes it. This is all he does, ever. For days, weeks, years at a stretch. He has seen so many emails that he can't remember the details of any except the very last one he looked at; he has seen so many emails that he no longer has or can maintain any personal or prurient interest, much like a doctor who has seen it all. All he does, all he can do, is decide whether the emails contain the keywords, and decide to keep them if they do and discard them if they don't. He can't read everything—there are far too many emails passing by. And he will occasionally miss a keyword—he is only human, after all. But as the years pass, he reads millions of emails from millions of people.***

***By any conception of the law, this would be counted as statutory interception, and as a Fourth Amendment search and seizure, of the emails being read. Is it more or less invasive than what the robot was doing? Why, if at all, should the law treat them differently?***



[22] *See* Savage, *supra* note 14.

[23] The questions of whether or not the FAA properly authorizes such "about" searching even if the general wiretapping statute forbids it, or whether—assuming the Fourth Amendment does apply—such "about" searching satisfies that amendment's requirements, are beyond the scope of this article. We only address the threshold question of whether such automated scanning implicates the privacy rights that the statute and the Constitution protect.

## III. Can Robots Intercept Your Email? Automated Content Scanning and The Wiretap Act

Under the federal wiretapping statute, "'intercept' means the aural or other *acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[24] Such interceptions are broadly prohibited as a matter of both civil and criminal law, except under specific exceptions or as authorized by a court.[25] Therefore, when considering whether a robot can intercept an "electronic communication," like your email, the critical question becomes: what counts as "acquisition" of the contents of a communication? Is it the moment the electrical signals that comprise the communication reach the robot in question? When the content is examined by that robot? When it is stored by that robot? When it is prepared for—or actually subject to—human review?

The NSA has its own peculiar answer to the question of how to define "acquire". "[A]cquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party."[26] "Collection," the NSA says, occurs only when information "has been received for use by an employee of a [Department of Defense] intelligence component in the course of his[/her] official duties…data acquired by electronic means is 'collected' only when it has been processed into intelligible form."[27] In sum, the NSA does not believe it has acquired a communication until it has not only entered and been stored by one of its devices but has also been rendered into a human-intelligible form and delivered to a human being for use in his (or her) job.



---

[24] 18 U.S.C. § 2510(4) (2006) (emphasis added). The "contents" of a communication are broadly defined as "include[ing] any information concerning the substance, purport, or meaning of that communication." *Id*. at § 2510(8).
[25] *See id*. at §§ 2511 (prohibiting interceptions except under certain exceptions, including authorization under foreign intelligence statutes), § 2518 (outlining procedures for obtaining court authorization in criminal investigations).
[26] Minimization Procedures Used by the National Security Agency, *supra* note 18.
[27] *Id*.

This very narrow interpretation of "acquire"—resulting in a very narrow interpretation of "intercept"—has rightly and repeatedly been pilloried by privacy advocates and security experts.[28] It also has no basis in the case law, which demonstrates that the NSA has intercepted our emails as soon as copies of those emails have been diverted to the robot used to scan them.

### A. If Recorders are "Agents of the Ear", Then Robots are Agents of the Brain: *United States v. Turk* and its Progeny

There are two relevant categories of cases addressing the question of exactly what constitutes an "intercept" under the federal wiretapping statute. The first category of cases considers *when* an interception has occurred, whether at the time the intercepted communication is acquired using a device or at the time that the communication is apprehended by human eyes or ears. The second category of cases considers *where* the interception has occurred, whether at the point where the communication was first captured or diverted, or in the place it was recorded or perceived by humans. The first and most influential court opinion in the first category, which is also oft cited in cases in the second category, is the Fifth Circuit's decision in *United States v. Turk*.[29] Although that decision does not clearly and immediately dispose of the question at issue—does acquisition and review by a robot constitute an interception?—it does establish that the locus of an intercept is the point at which a device captures the communication, not the point at which a human perceives it.



---

[28] *See, e.g.*, Trevor Timm, "A Guide to the Deceptions, Misinformation, and Word Games Officials Use to Mislead the Public About NSA Surveillance," ELECTRONIC FRONTIER FOUNDATION (August 14, 2013), https://www.eff.org/deeplinks/2013/08/guide-deceptions-word-games-obfuscations-officials-use-mislead-public-about-nsa; Jameel Jaffer and Brett Max Kaufman, "How to Decode the True Meaning of What NSA Officials Say," SLATE (July 31, 2013), http://www.slate.com/articles/news_and_politics/politics/2013/07/nsa_lexicon_how_james_clapper_and_other_u_s_officials_mislead_the_american.html; Bruce Schneier, "Surveillance by Algorithm," SCHNEIER ON SECURITY (March 15, 2014), https://www.schneier.com/blog/archives/2014/03/surveillance_by.html.

[29] United States v. Turk, 526 F.2d 654 (5th Cir. 1976).

The *Turk* court considered the original definition of "intercept", which did not apply to electronic communications but only to electronic eavesdropping on oral communications or wiretapping of telephone conversations: "'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[30] The police had seized an audio recording from drug trafficker Charles Kabbaby's car of a conversation between him and defendant Frederick Turk, and the Court had to determine if the subsequent act of listening to that recording qualified as an "intercept" of the telephone call.[31]

The court answered that question in the negative, holding that interception doesn't occur at the point of listening but at the point of acquisition by a device, in this case, a recorder: "If a person secrets a recorder in a room and thereby records a conversation between two others, an 'acquisition' occurs at the time the recording is made."[32] Both the statute's text and the legislative history, said the court, "indicate[] that the act of surveillance and not the literal 'aural acquisition' (i.e., the hearing), which might be contemporaneous with the surveillance, or might follow therefrom, was at the center of congressional concern."[33] Refashioning its holding in the form of an old riddle, the court asked:

> In a forest devoid of living listeners, a tree falls. Is there a sound? The answer is yes, if an active tape recorder is present, and the sound might be thought of as 'aurally acquired' at (almost) the instant the action causing it occurred. For § 2510(4) purposes, *the recorder can be the agent of the ear*."[34]

The concept of an intercepting device as an "agent" of the humans using it is a fruitful concept to which we will return in future sections—if a recorder can be the agent of the ear, an automated system that examines communications and judges whether the contents

[30] 18 U.S.C. § 2510(4) (1982).
[31] Turk, 526 F.2d at 657.
[32] *Id*. at 658.
[33] *Id.* at 659.
[34] *Id*. at 658, n. 2 (emphasis added).

are relevant to its human masters could just as easily be considered the agent of those humans. Meanwhile, the *Turk* decision highlights a foundational concept in wiretapping law: the "acquisition" that is the core component of an interception is accomplished by devices, not by humans.

The basic holding of *Turk*—that the act of listening to a previously recorded conversation is not an interception of that conversation—has been widely and consistently followed by the circuit courts in the decades since.[35] However, it still doesn't answer the question at issue here: what if the communication is never recorded at all? Can a communication be acquired by a device, and therefore intercepted, absent a recording?

***INTERLUDE III: THE MAN OUTSIDE OF ROOM 641A***

***The Man has left Room 641A, perhaps for lunch perhaps to sleep. The monitor screen that the Man once observed shows the content of all the emails that he would have reviewed, passing by, scrolling down the screen before they disappear forever. If the Man were in the room, he would see them. But he is not in the room to see them; no one is. Have they been intercepted? Have they been searched or seized?***

### B. If "Redirection Presupposes Interception", So Too Does Robotic Review: *United States v. Rodriguez*, *Halkin v. Helms*, and *People v. Bialostok*

An intercept occurs "when the contents of a wire communication are captured or redirected *in any way*," declared the Second Circuit in *United States v. Rodriguez*, the most influential decision in the second relevant category of intercept cases—those cases considering *where* the intercept took place.[36] *Rodriguez* and its progeny reiterate and expand on the lesson of *Turk*, making clear that the key moment for interception is the

[35] *See, e.g.,* Jacobson v. Rose, 592 F.2d 515, 522 (9th Cir. 1978) (act of listening is unnecessary to establish interception); U.S. v. Lewis, 406 F.3d 11, 18 n.5 (1st Cir. 2005) (same); Sanders v. Robert Bosch Corp., 38 F.3d 736, 740 (4th Cir. 1994) (same).
[36] United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (emphasis added).

moment of acquisition by a device, not the moment of apprehension by (or recording for) a human's eyes or ears.[37]

In that case, the issue was: where did the interception take place, for purposes of identifying which court had authority to authorize it? The Drug Enforcement Agency (DEA), under the authority of a wiretap order issued by the Southern District of New York, had the telephone company install a second line at a restaurant in New Jersey that would divert calls for recording at the DEA's Manhattan Office. The statute authorizes courts to issue wiretaps only within their own territorial jurisdiction,[38] so the answer to the question of where the interception took place would determine whether the wiretap was properly authorized. The court concluded, looking at the original definition of 'intercept':

> The statute does not specify precisely where an interception is deemed to occur. It seems clear that when the contents of a wire communication are *captured or redirected in any way*, an interception occurs at that time. Such an interception plainly occurs at or near the situs of the telephone itself, for the contents of the conversation, whether bilateral as is usually the case, or multilateral as is the case with a conference call, are transmitted in one additional direction. *Redirection presupposes interception.* Accordingly, a federal court sitting in the jurisdiction in which the to-be-tapped telephone is located would have the authority, under § 2518(3), to authorize a wiretap.[39]

The *Rodriguez* court's conclusion that a communication is intercepted whenever it has been redirected has been widely and approvingly cited,[40] and stands to reason when you look closely at the statement that "redirection presupposes interception." The word

---

[37] *Id.*
[38] 18 U.S.C. § 2518(3).
[39] Rodriguez, 968 F.2d at 136 (emphasis added).
[40] *See, e.g.,* Noel v. Hall, 568 F.3d 743, 749 (9th Cir. 2009) (favorably citing the *Rodriguez* holding that interception occurs when a communication's "contents…are captured or redirected in any way" when concluding that listening to a recording does not count as an interception); George v. Carusone, 849 F. Supp. 159, 163 (D. Conn. 1994) (same); In re State Police Litigation, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (citing to *Rodriguez* when considering the *Turk* issue of whether listening counts as an interception, and holding that "it is the act of *diverting*, and not the act of listening, that constitutes an 'interception.'").

"presupposes" means to "require as a precondition."[41] Therefore, the court is not saying that redirection equals interception; rather, it is saying that if a communication has been redirected, a device necessarily must have acquired it first; otherwise, there would be no communication to redirect. Put another way, a device cannot redirect a communication until it has been acquired, hence, "redirection presupposes interception."

Based on the holding from *Rodriguez*, repeatedly echoed in the years since the statute was updated to cover electronic communications, a redirected communication is an intercepted communication—*whether or not it is recorded or viewed by a human afterward*. This conclusion was bolstered by another circuit court decision, *Sanders v. Robert Bosch Corp*., decided two years after *Rodriguez*.[42] In *Sanders*, the defendant corporation had installed a "voice logger" device to continuously record all of the phone calls on certain telephone lines its plant, including telephone lines in the plant's security office that were used by plaintiff Sanders, a security guard at the plant. [43] The company eventually stopped using the voice logger, which was installed in a separate security control room called "the penthouse," to record conversations. However, and unknown to the company, sound from the telephone microphones in the security office was still being redirected to the voice logger in the penthouse, even thought the voice logger had been set to "off" and was no longer loaded with tapes for recording. Therefore, if someone were to turn the volume upon the voice logger in the penthouse, one would be able to hear conversations occurring near the microphone in the security office.[44]

Sanders sued Bosch over the interception of his conversations—both his phone conversations while the voice logger was in operation, and the interception of his conversations in the security office after the voice logger was turned off. Consistent with

---

[41] *Presuppose*, OXFORDDICTIONARIES.COM, http://www.oxforddictionaries.com/us/definition/american_english/presuppose.
[42] Sanders, 38 F.3d 736 (4th Cir. 1994)
[43] *Id.* at 737-39.
[44] *Id*.

the logic of *Turk* and its progeny, the Fourth Circuit held that the phone conversations that were recorded by the voice logger were intercepted, regardless of whether they were listened to: "The recording of a telephone conversation alone constitutes an aural acquisition of that conversation."[45] However, the court also concluded that the conversations that occurred after the voice logger was turned off were not intercepted.[46] Some commentators have taken this conclusion to mean that redirection of a conversation without recording or human review does not constitute an interception.[47] However, this is an over-reading of the decision.

*Sanders v. Robert Bosch Corp*. supports, rather than undermines, the conclusion that mere redirection without recording or listening constitutes in interception. The court specified two reasons for its holding, neither of which turn on the lack of recording or listening. First, the court noted that there was no evidence that the *content* of any conversation was acquired after the deactivation of the voice logger, as opposed to content-less "ambient noise" from the security office.[48] Second and more importantly, the defendants did not mean to leave the microphone on and were unaware that it was transmitting, and therefore did not *intentionally* intercept any conversations that were acquired by the open microphone.[49] However, and consistent with *Rodriguez*'s maxim, it was clearly the microphone that captured and redirected—i.e., intercepted—the communications that were recorded by the voice logger. If it were otherwise, the court would have needed no reason other than the fact that the voice logger was turned off to conclude that no interception occurred at that time, rather than relying on the content



[45] *Id*. at 740.
[46] *Id*. at 742-43.
[47] *See* Boyden, *supra* note 4, at 693 n.106; Brief for Verizon Communications, Inc. at 9-10, In re: National Security Agency Telecommunications Records Litigation, 564 F.Supp.2d 1109 (N.D.Cal. 2008) (No. 06-1791 VRW), *available at*: https://www.eff.org/files/filenode/att/verizonmemmtd.pdf.
[48] Sanders, 38 F.3d at 742.
[49] *Id*. at 742-43.

issue or the intent issue. A telephone call cannot be redirected—or recorded—without first being acquired.

Similarly, a robot cannot analyze a communication until it has first been acquired, as *Halkin v. Helms* demonstrates.[50] In that case, the D.C. Circuit made clear that automated scanning of a communication by computers is necessarily preceded by an acquisition, or, as the *Rodriguez* court might have phrased it, "scanning presupposes interception". In *Halkin*, former Vietnam war protesters sued the NSA for allegedly intercepting their communications, based on the presence of their names on certain NSA watchlists. In its discussion of those watchlists, the court repeatedly refers to the communications being scanned by NSA computers as having previously been "acquired". For example:

> Using "watchlists"[—]lists of words and phrases designed to identify communications of intelligence interest[—]NSA computers scan the mass of *acquired* communications to select those which may be of specific foreign intelligence interest. Only those likely to be of interest are printed out for further analysis, the remainder being discarded without reading or review.[51]

In other words, the NSA did not (and practically, could not) scan a communication until the communication's "signals" were first "*acquired* by [the NSA's] many techniques."[52]

The *Halkin* court ultimately concluded that the "mere existence" of plaintiffs' names on the NSA's watchlists or intelligence reports could not support the presumption that their communications were among the mass of communications that were actually acquired.[53] But in reaching that conclusion, the court made clear that any communications examined by the NSA's computers were indeed "acquired", regardless of which ones were selected by the computers for storage or review and which were discarded. Or, to put it another way: even if acquisition without recording doesn't count

[50] Halkin v. Helms, 598 F.2d 1 (D.C. Cir. 1978).
[51] *Id*. at 4 (emphasis added).
[52] *Id* (emphasis added).
[53] *Id*. at 10-11.

as an interception, any communication that has been scanned by a computer necessarily *was recorded*, if only briefly, so that it could be acted on. At that moment, there was the potential for human review—and the actuality of human agency through the proxy of the robot.

This conception of "acquisition" as the point at which someone other than the sender or recipient gains control over the disposition of a communications contents—in addition to foreshadowing our Fourth Amendment argument in Part IV—is supported by the reasoning of a state wiretapping case, *the People v. Bialostok*.[54] In *Bialostok*, police installed pen register devices on several phone lines being used by a gambling operation in order to monitor the phone numbers being dialed on those lines.[55] The police later obtained a warrant to wiretap the conversations going over those lines, but they did not need to install a new device to accomplish that wiretap. It turned out that the pen register device was also capable of wiretapping, because the calls were already passing through it: by merely attaching an audio cable to an output on the device, it would pass the audio signal from those calls to an attached recording device.

Because that audio signal—the communications content—from the phone conversations had entered the police device, the New York Court of Appeals in *Bialostok*, using logic that would extend to the federal law, concluded that the device had "acquired" those communications for purposes of New York's wiretapping law. "The device," the court reasoned, "acquired the contents of communications from the moment it was installed.[56] The addition of the audio cord and the tape recorder after the warrant was issued merely made accessible what was *already being acquired*."[57] The locus of the

[54] People v. Bialostok, 610 N.E.2d 374 (N.Y. 1993).
[55] *Id*. at 376. Such pen register surveillance did not require a warrant under state law or under the Fourth Amendment as interpreted by the Supreme Court in *Smith v. Maryland*, 442 U.S. 735 (1979).
[56] Bialostok, 610 N.E.2d at 377.
[57] *Id.* (emphasis added).

wiretap and the conduct that comprised it was not in the listening, or in the recording, nor even in the redirection of the communication—it was in the police's *taking control* of the communication using a device that could divert it, or could be used to allow recording or listening.

In sum, the weight of authority regarding telephone wiretapping makes clear that regardless of whether a human apprehends the communication in question, and regardless of whether it is recorded, at a minimum a communication is "intercepted" at the point where the content is redirected by a device, and probably even when that content is made accessible to someone other than the intended recipient, whether it is redirected or not. More recent case law regarding electronic communications, as opposed to voice (or "wire") communications, has not disturbed this conclusion.

### C. Digital Diversions and Modern Wiretapping: Redirection Presupposes Interception for Electronic Communications, Too

Redirection presupposes interception in the digital realm as well as the telephonic realm, as demonstrated in the influential email interception case *United States v. Councilman*.[58] In that case, bookdealer Bradford Councilman offered his customers email service—but allegedly instructed his employees to intercept any incoming email to his customers from rival bookseller Amazon.com, in hopes of gaining commercial advantage by monitoring his customers' book purchasing habits.[59] His employees did so by reconfiguring "procmail", the MTA or "Mail Transfer Agent" software on Councilman's email server that handled incoming emails, such that before incoming emails from Amazon.com were deposited into the recipients' email boxes, copies would be made and diverted into an email box that Councilman could access.[60]

The main controversy in *Councilman* was whether or not copying of emails that were in temporary storage on the email server, as opposed to copying of emails off of the

[58] United States v. Councilman, 418 F.3d 67 (3d Cir. 2005) (en banc).
[59] *Id*. at 70-71.
[60] *Id*.

"wire", could constitute an interception at all.[61] What was not controversial, assuming that an interception had occurred,[62] was when and where it had occurred. As the court described:

> [The] systems administrator modified the server's procmail recipe so that, before delivering any message from Amazon.com to the recipient's mailbox, procmail would copy the message and place the copy in a separate mailbox that Councilman could access. Thus, procmail would *intercept and copy* all incoming messages from Amazon.com before they were delivered to the recipient's mailbox, and therefore, before the intended recipient could read the message.[63]

The court's description makes clear not only that the reconfigured procmail software was the interception device in question, but also that the moment of acquisition was the moment when the reconfigured procmail software *received* the communication, before it was copied. "Acquisition" by the device did not equal the creation and diversion of a copy to Councilman's email box by the device; rather, "acquisition" by the device occurred when the device gained control of the disposition of the communication such that it *could* divert a copy. Or, put another way: copying presupposes interception.

Later electronic wiretapping cases not only do not disturb this reasoning, but indeed support our conclusion. In particular, the arguments made by Internet giant Google in a couple of recent interception cases—or, more to the point, the arguments not made—highlight how automated capture or review of communications content, even without any human perception of the content, constitutes an interception. In *Joffe v. Google, Inc.*,[64] Google was sued for intercepting and storing masses of personal Internet communications transmitted over home and business Wi-Fi networks.[65] Those interceptions occurred when Google vans, which drive around cities to take pictures for



[61] That controversy does not apply to our fact pattern, which clearly does involve splitting copies directly from the wire.
[62] The *en banc* Third Circuit Court of Appeals ultimately answered that question in the affirmative. Councilman, 418 F.3d. at 79.
[63] Councilman, 418 F.3d. at 70.
[64] Joffe v. Google, Inc., No. 11–17483, 2013 WL 6905957 (9th Cir. 2013).
[65] *Id.* at *1-2.

the company's "Street View" mapping product, also attempted to map the location of Wi-Fi networks in order to enhance Google's various location-based services.[66] In addition to capturing the non-content information needed for mapping, Google's equipment also captured unencrypted communications information passing over open Wi-Fi networks, including password information and e-mail content.[67]

Separately, while the *Joffe* case has progressed, Google has also been sued in relation to its "Gmail" email service by individuals who argue that the automated scanning of the content of their emails in order to serve ads relevant to the subject matter of those emails constitutes an interception of those emails.[68]

Google often promotes the fact, when addressing privacy concerns about its Gmail service, that automated scanning for advertising purposes involves no human review: "Ad targeting in Gmail is fully automated, and no humans read your email or Google Account information in order to show you advertisements or related information," says the company.[69] Nor did humans review the mass of Wi-Fi-derived data.[70]

However, in neither case did Google even attempt to argue that it had not acquired with a device the communications in question, based on the fact that humans had not reviewed or made use of the data. Rather, Google argued that it was not liable based on various exceptions in the wiretapping statute. In *Joffe*, Google only argued that the statute did not cover the unencrypted Wi-Fi communications it had intercepted because they fell into an exception for interception of communications that are "readily



---

[66] *Id*. at *1.
[67] *Id.*
[68] In re: Google Inc. Gmail Litigation, 2013 WL 5423918.
[69] *See, e.g.*, *How Gmail Ads Work*, GOOGLE, https://support.google.com/mail/answer/6603?hl=en (last visited Mar. 22, 2014).
[70] *See* Alan Eustice, "WiFi data collection: an update," GOOGLE OFFICIAL BLOG, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (last visited Mar. 22, 2014). According to Google, this information was segregated and made inaccessible when it was discovered, and much of it was eventually deleted.

accessible to the general public."[71] In the Gmail litigation, Google only argued that acquisition of communications by the content-scanning software was not an actionable interception because that software was used in the ordinary course of business, and because Gmail users had consented to the interception.[72] The one argument Google never put forward? "It didn't count because it was just robots."

In sum, and looking at the weight of case law both in regard to telephonic and electronic communications, it is clear that the emails being reviewed by the NSA's robots are intercepted as soon as copies of those emails are diverted to those robots. Or, to analogize to an interception in the game of football[73]—the emails were "caught" at the moment of diversion. That was the interception. Whether the intercepting player is then tackled, fumbles, takes a knee, or makes it all the way to the end zone, the initial interception happened, and the opposing team lost control of the ball. Similarly, what the government chooses to do after intercepting an email doesn't change the fact that it was intercepted, and to essentially leave the disposition of that email to the government's discretion would undermine the purpose of the wiretapping statute—and as we'll discuss in Part IV, the Fourth Amendment.

## IV. Can Robots Search or Seize Your Email? Automated Content Scanning and The Fourth Amendment

It has been clear for nearly half a century that electronic eavesdropping on or wiretapping of the contents of telephone calls is both a search and a seizure of those

[71] *See* Joffe, 2013 WL 6905957 at *2-3; *see also* 18 U.S.C. § 2511(2)(g)(i) (excepting readily accessible communications).
[72] *See* In re: Google Inc. Gmail Litigation, 2013 WL 5423918, at *12-13 (September 26, 2013); *see also* 18 U.S.C. § 2510(4) (defining intercept as acquisition of communications content "through the use of any electronic, mechanical, or other device"); § 2510(5)(a)(i) (excepting from the definition of "electronic, mechanical, or other device" any device that is used by a communications provider in the ordinary course of business); 2511(2)(c) (excepting interceptions done with prior consent of one of the parties to a communication).
[73] United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010) (analogizing to football interception but questioning application to email).

communications under the Fourth Amendment.[74] Less clear is how the Fourth Amendment applies to electronic communications, and whether the actions of a robot—automatedly reviewing the content of electronic communications, alone and without human intervention—can trigger that application. Is such scanning a search? Is it a seizure?

The answer to both questions is "yes".

### A. Can Robots Search Your Email?

To answer the question of whether a robot can "search" your email for Fourth Amendment purposes, a threshold question is whether we have a "reasonable expectation of privacy" in our email, such an expectation being a key requirement for Fourth Amendment protection.[75] Although not yet settled by the Supreme Court, appellate courts have so far uniformly concluded that the contents of electronic communications, such as email, are protected against unreasonable search by the Fourth Amendment,[76] such that

---

[74] *See* Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); United States v. United States Dist. Ct. for E. Dist. Of Mich., Southern Division, 407 U.S. 297 (1972).

[75] The Supreme Court has recently been inclined to find a Fourth Amendment violation even in cases where no reasonable expectation of privacy exists. It is unclear to what extent these cases are an aberration or enunciate a new, alternate rule for determining search. *See* United States v. Jones, 132 S. Ct. 945 (2012); United States v. Jardines, 569 U.S. __ (2013).

[76] *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (in context of email pen register, distinguishing between "unprotected addressing information" such as "the to/from addresses of a person's e-mails or the IP addresses of websites visited," and "protected content information" such as "the contents of the [email] messages or…the particular pages on the websites the person viewed"); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008), *cert. granted sub nom.* City of Ontario v. Quon, No. 08-1332, 2009 WL 1146443 (U.S. Dec. 14, 2009) (finding that pager text messages are protected by a Fourth Amendment reasonable expectation of privacy, concluding that there is "no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here. Both are sent from user to user via a service provider that stores the messages on its servers."); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP.") (internal quotations omitted). The only contrary circuit ruling was ultimately vacated, and its reasoning only applied to emails that have completed transmission, not to

even academics who were previously skeptical of an expectation of privacy in email have now concluded that there is such an expectation.[77]

### 1. *Smith v. Maryland* and "The Automation Rationale"

Assuming a reasonable expectation of privacy in our emails, the question then becomes: does an automated search of those emails, without a human in the loop, violate that expectation? In answering that question in the affirmative, we can look for support in *Smith v. Maryland*, a case more often used to argue against the existence of a privacy expectation. In that case, the Supreme Court distinguished its previous holdings that eavesdropping on phone conversations' content violates a reasonable expectation of privacy and therefore constitutes a search, holding that using a pen register device to monitor non-content dialing information about phone conversations on a single phone line over a 24-hour period did not violate an expectation of privacy and was therefore not a search.[78] The Court so held based on its conclusion that by providing phone numbers to the phone company for the purpose of connecting his calls, the caller had voluntarily exposed that information to the phone company and had assumed the risk that the information would be shared with the government.[79] A critical part of the court's reasoning was that, for Fourth Amendment purposes, *there is no distinction between exposure of information to a human and exposure of information to automated equipment controlled by humans*:

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he

---

communications that are still in transit like those being captured by the NSA. *See* Rehberg v. Paulk, 598 F.3d 1268, 1261 (11th Cir. 2010) ("A person [has no] reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."), *vacated*, 611 F.3d 828 (11th Cir. 2010).

[77] *See, e.g.,* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 at 1029 (2010).

[78] Smith, 442 U.S. at 743-45.

[79] *Id*.

> dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[80]

This logic used in *Smith* to undermine a claim of privacy—"the Automation Rationale", as described by one commentator[81]—here helps to preserve it. What is good for the goose is good for the gander, and if voluntary exposure to the phone company's automated switching equipment in *Smith* eliminated any expectation of privacy in the caller's dialing information, then the involuntary exposure of protected email content to the government's email-scanning robots similarly violates the expectation of privacy in that email. We are not inclined to conclude that a different constitutional result is required because the government has decided to automate its surveillance of Americans' emails.

### 2. Email-Scanning Robots as Automated Agents of the Government

Looking beyond *Smith* and other wiretapping and pen register precedents to the realm of physical searches, a strong analogy can be made between the automated email-reading equipment employed by the NSA and those private actors who engage in searches as agents of the government.[82] A search by a private party without the instigation or involvement of the government does not implicate the Fourth Amendment, but if the government instructs or otherwise participates in the search, the Fourth Amendment kicks in. And in such cases, it is the search done by the private party as an agent of the government, not the moment at which the private party hands over the evidence, that implicates the Fourth Amendment—and it is the involvement of the

[80] *Id*. at 744-45 (internal citation omitted).
[81] *See* Tokson, *supra* note 4, at 586.
[82] One need not limit the concept of robot "agency" to the Fourth Amendment context. *See generally* SAMIR CHOPRA AND LAURENCE F. WHITE, A LEGAL THEORY FOR AUTONOMOUS ARTIFICIAL AGENTS (2011) (articulating a broad and general theory of robots as legal agents); *see also id.* at 98-105, 107-118 (specifically discussing robot agency in the context of automated communications content scanning).

government prior to or during the search, not after, that is relevant to establishing the applicability of the Fourth Amendment. So, for example, if a private party searched another's property at the instruction of the government for a particular piece of evidence but did not find it, that would constitute a search, even if that person never reported back to the police, or only reported back the absence of the evidence. [83] The same is true for a robot.

### 3. Drug-Sniffing Dogs vs. Packet-Sniffing Robots

Some might suggest that the more apt analogy for considering the Fourth Amendment implications of NSA's "packet-sniffing" robots would be drug-sniffing dogs used by the police, which the Supreme Court has repeatedly held do not violate an expectation of privacy. For example, in *U.S. v. Place*,[84] the defendant had raised the suspicion of two DEA agents at La Guardia Airport, and subsequently refused to allow his luggage to be searched. [85] The luggage was then taken to John F. Kennedy Airport in the neighboring borough and was subjected to a "sniff test" by a trained narcotics dog, which reacted to one of the suitcases.[86] The dog's reaction provided the basis for a search warrant, and cocaine was found in the suitcase.[87] In considering the question of whether

[83] Whether a private person is acting as a government agent when conducting a search is determined by reference to government involvement prior to or during the search, without reference to after. *See, e.g.*, WAYNE R. LAFAVE, 1 SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.8(b) (5th ed. 2013) ("it may generally be said that the search [by a private person] is still governmental action if it was instigated by the authorities or the authorities have participated in the search in some way"); United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994) (The two-part test for determining whether a private person acted as an agent of the government for Fourth Amendment purposes is "(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends.").
[85] United States v. Place, 462 U.S. 696 (1983).
[85] United States v. Place, 462 U.S. 696 (1983).
[86] *See id.*
[87] *See id.*

the dog sniff itself was a search requiring a warrant, the Court held dog sniffs stand apart from any "other investigative procedure":

> [T]he sniff discloses *only* the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited…Therefore, we conclude that the particular course of investigation that the agents intended to pursue here – exposure of respondent's luggage, which was located in a public place, to a trained canine – did not constitute a 'search' within the meaning of the Fourth Amendment.[88]

A 2005 Supreme Court Case, *Illinois v. Caballes*, further clarified the Court's reasoning: "[A]ny interest in possessing contraband cannot be deemed 'legitimate,' and thus, governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'"[89] Accordingly, if a search is constructed so as to *only* reveal contraband, it is not considered a search at all under the drug-sniff precedents, because one can have no reasonable expectation of privacy in illegal material.

At least one commentator has considered how this reasoning might apply to certain searches of electronic data. Specifically, Richard Salgado has suggested that scanning computers or networks for known unlawful files, such as child pornography, may not constitute a search under the dog-sniff precedents.[90] Such automated searching could be done using "hashes" associated with the offending files—unique numbers, derived from files and replicated in their duplicates, that could then be scanned for on a seized computer or on a monitored network and that would only reveal images matching the original contraband file.[91] However, the Fourth Amendment analysis around such



[88] *Id.* at 707 (emphasis added).
[89] Illinois v. Caballes, 543 U.S. 405, 408 (2005) (emphasis in original); *see also* Florida v. Jardines, 133 S.Ct. 1409 (2013); Florida v. Harris, 133 S.Ct. 1050 (2013).
[90] *See generally* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38 (2005).
[91] *See id*. at 39-41.

scanning is complicated by the fact that determining whether an image is contraband is much harder than determining whether a substance is contraband:

> The definition of child pornography cannot be set out as a chemical formula, unlike drug contraband, and no legislative body has declared particular images to be contraband, much less blessed a hash set. Instead, the definitions describe the attributes that make an image contraband. It would seem that populating a hash set requires exercise of discretion that is not required when teaching a dog to detect cocaine or developing a chemical test to react to particular narcotics.[92]

Even under Salgado's theory, scanning for files that have not actually been adjudicated to be contraband would challenge the analogy of porn-sniffing robots to drug-sniffing dogs, and raise Fourth Amendment questions that dog sniffs do not. Short of child pornography or obscene images, the contents of a communication will rarely be adjudged "unlawful" in their own right, though they may concern or allude to unlawful activity.[93]

The analogy of packet-sniffing to drug-sniffing breaks down even further in the situation of automated scanning like that done by the NSA, which clearly does not "only reveal the possession of contraband."[94] The foreign intelligence information sought by the NSA is not *per se* illegal contraband, but instead simply information related to its targets. Furthermore, even if that information arguably was contraband, it has not been adjudicated to be so by any court. Rather, as noted by the Wall Street Journal, "NSA has discretion on setting its filters, and the system relies significantly on self-policing. This can result in improper collection that continues for years."[95] Finally, even in the unlikely



---

[92] *Id*. at 46.
[93] *See, e.g.*, Lon A. Berk, *After Jones, the Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud*, 14 J. HIGH TECH. L. 1 (2014) ("That information is tangible property protected by the Fourth Amendment is supported by *Boyd v. United States*, which protected information in an invoice. That case involved seizure of an invoice. By statute the defendant was obligated to produce it. The court held that that was an unreasonable search and seizure, distinguishing between contraband, in which the government had a possessory interest, and the invoice relating to that contraband, to which only the defendant had a possessory interest, and held that the latter could not be seized absent warrant.").
[94] Caballes, 543 U.S. at 408.
[95] Gorman and Valentino-Devries, *supra* note 10.

event a court has previously determined that every identifier sought by NSA's robots is unprotected, contraband speech, the NSA has acknowledged its failures to collect traffic that only includes the foreign intelligence information that it seeks.[96] For all these reasons, packet-sniffing fails to achieve the necessary level of specificity to draw a legal analogy to upheld dog-sniff searches.

### 4. Email-Scanning Robots and Heat Imaging Devices

To the extent that the NSA's packet-sniffing robots reveal more than just contraband, they are much less analogous to drug-sniffing dogs or to the child porn hash tools that Salgado envisions, and much more like the heat imaging tool used in *Kyllo v. United States*, which Salgado notes "was not discerning enough to reveal only illicit activities."[97] In *Kyllo*, federal agents used a thermal imaging device to scan a house that they suspected was being used to grow marijuana.[98] The agents were looking for high amounts of heat, associated with the heat lamps that are used to grow marijuana indoors. The Supreme Court held that the device had been used to perpetrate a search: "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search."[99]

The NSA isn't yet peering through the walls of our homes with heat imaging equipment (as far as we know!). However, the *Kyllo* decision is especially pertinent to the case of the NSA's email-scanning robots because of the sharp distinction it makes between the act of *scanning* the house, which was a search, and the act of a human

[96] *See* [Redacted], 2011 WL 10945618, at *2. As noted, even a search that returned *only* foreign intelligence information would not be constitutional under the dog sniff rationale, because foreign intelligence information is not *per se* unlawful. However, this case is cited to provide support for the assertion that even an automated search constructed to only return a narrowly-defined category of information will necessarily return a great deal of information outside those perimeters.
[97] Salgado, *supra* note 90, at 45 (citing Kyllo v. United States, 533 U.S. 27 (2001)).
[98] Kyllo, 533 U.S. at 29-30.
[99] *Id.* at 34.

understanding the results of that search, which was not. This distinction arose in an argument between the majority and the dissenting Justices. The Dissent argued that the majority opinion was wrongly treating the investigating officers' inferences about the contents of the home, based on heat signatures emanating from the home, as a Fourth Amendment search.[100] The majority's response makes clear that it is was use of the heat scanner, not the conclusions drawn from that scanning by the police, which constituted the search:

> The issue in this case is not the police's allegedly unlawful inferencing, but their allegedly unlawful thermal-imaging measurement of the emanations from a house. We say such measurement is a search; the dissent says it is not, because an inference is not a search. We took that to mean that, since the technologically enhanced emanations had to be the basis of inferences before anything inside the house could be known, the use of the emanations could not be a search. But the dissent certainly knows better than we what it intends. And if it means only that an inference is not a search, we certainly agree. That has no bearing, however, upon whether hi-tech measurement of emanations from a house is a search.

In other words, using technology to reveal information about the contents of a private home is a search, even if that information is not comprehended or used by a human afterward. The same is true of the contents of a private communication.

This conclusion is made evident by an only slightly science-fictional hypothetical. Imagine a self-driving police car that regularly patrols the streets with a thermal imaging device. That device scans every house that the car passes. If a heat signature from one of the scanned houses might indicate marijuana growth operation, police headquarters is alerted and a copy of the scan's results are transmitted to investigating officers so that they may judge for themselves whether the signature supports a strong inference about the contents of the house. Otherwise, the police are left unaware of the results of the scans, which are immediately discarded. It seems obvious under *Kyllo* that such thermal scanning would constitute a search of every house, independent of whether human beings

[100] *Id*. at 44 (Stevens, J., dissenting).

ultimately viewed or evaluated the results of those scans—as would NSA's analogous scanning of email content.

However, even if all analogies fail and one concludes that the NSA's robots are not searching our email, there is still the separate question: are they *seizing* our email?

### B. Can Robots Seize Your Email?

The Fourth Amendment regulates not only searches, but seizures as well. Whether or not the reader agrees that automated scanning of communications constitutes a search, the Fourth Amendment still regulates such scanning as a seizure of the communications. Although not yet clearly established by the courts, recent scholarship strongly supports the conclusion that not only the scanning, but the mere diversion of communications into the government's control is a seizure, just as mere diversion without more constitutes an interception under the statute. As those scholars explain, the right against seizure is more than just a right to privacy, but a right to prevent "the government's exercise of control over a copy of our property."[101] Therefore, "[f]rom the standpoint of regulating the government's power to collect and use evidence, generating an electronic copy is not substantially different from controlling access to a house or making an arrest…[and] copying Fourth Amendment protected data should ordinarily be considered a Fourth Amendment seizure."[102]

For most of the history of the Internet, the question of diversion of electronic information as a Fourth Amendment seizure of those communications was under-discussed in academia and the court system. At best, Supreme Court precedent on the issue is divided as to whether information is seized when a copy of it is made.[103] Courts

[101] Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Tangible Property*, 2008 STAN. TECH. L. REV. 2, 20.
[102] Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 709 (2009-2010).
[103] Arizona v. Hicks, 480 U.S. 321. Hicks involved the copying of a serial number off of the bottom of a stereo. The Court held that the copying of the serial number was not a

define seizure as "a meaningful interference with a possessory interest."[104] The cases demonstrate that even a short-term interference is enough to qualify.[105] Arguably, both tangible and intangible property may be subject to seizure.[106] The Supreme Court in *Katz v. US*[107] *and US v. Berger*[108] clearly indicated that the electronic recording of a conversation was a seizure, as well as a search. Dicta in later cases, particularly *US v. Jacobsen* and its progeny, placed doubt on if non-physical interferences would still be considered seizures by the Court.[109] However, recently some leading scholars have explored this question, and have concurred that a seizure does occur at the point that information is diverted and cloned, even with no further action.[110]

Relying primarily on one of the post-*Jacobsen* cases, *Arizona v. Hicks*, Professor Orin Kerr reasoned in 2005 that "bitstream copies," or complete bit-by-bit duplications of an entire target (including the metadata) would not constitute seizures of the original file. Kerr conceded that the process could *include* a seizure of the device that holds the target, if it was invaded in the act of copying, but the data itself was never seized.[111] However, a

---

seizure, but did find a search in the movement of the stereo in order to reveal the number. *Cf*. Berger, 388 U.S. 41.

[104] U.S. v. Jacobsen, 466 US 109 (1984) (emphasizing the "possessory interest" required as a pre-requisite for a seizure).

[105] *See* Terry v. Ohio, 392 U.S. 1, 19 (1968) ("We therefore reject the notions that the Fourth Amendment does not come into play at all as a limitation upon police conduct if the officers stop short of something called a "technical arrest" or a "full-blown search.").

[106] Katz, 389 U.S. 347. "We have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any "technical trespass under . . . local property law;" *see also* Silverman v. United States, 365 U.S. 505, 511 (1961).

[107] Katz, 389 U.S. 347.

[108] Berger, 388 U.S. 41.

[109] Ohm, *supra* note 101 at 3 (citing discrepancy between *Berger* and *Katz* and *Jacobsen* and *Hicks*).

[110] Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2005); Paul Ohm, *supra* note 101; Orin Kerr, *Searches and Seizures in a Digital World*, 115 HARV. L. REV. 531 (2005).

[111] Kerr, *supra* note 110.

few years later Kerr changed his mind, and instead decided that the creation of copies of electronically-transmitted information may qualify as a Fourth Amendment seizure.[112] Kerr explains that he believes the key difference is between whether a copy is made in order to preserve that which is previously observed or, conversely, made to "freeze the scene" – that is, to "take some evidence that was beyond the government's control and bring it within the government's control."[113] Such an approach explains how some copies may not interfere with a possessory interest, while others do:

> Writing down information or taking a photograph merely preserves the human observation in a fixed form. In contrast, electronic copying adds to the information in the government's possession by copying that which the government has not observed. The two types of copying should be treated differently; the former should not be treated as a seizure while the latter should.[114]

According to Kerr, the relevant Fourth Amendment moment is at the point that "government action changes the predetermined path of the item by some intentional action."[115] This would encompass the automated diverting and cloning, as Kerr explains:

> Although some cases will prove difficult, many important examples should be clear. If the government wiretaps an email account and generates copies of all of the emails incoming and outgoing from the account for law enforcement use, all of the communications are "seized" for Fourth Amendment purposes at the moment the copies are generated. The usual and expected path of transmission of email includes passage through mail servers across the Internet, but it does not include an effectively compulsory "bcc" to the government. Such copying is outside the usual and expected path of transmission. It therefore constitutes a seizure.[116]

A personal electronic communication, once sent, is intended to travel directly to the party to which it is addressed, adjusting for the de-centralized network of the Internet. When government robots divert that message, it interrupts that path, even for only a brief time.

---

[112] Kerr, *supra* note 102.
[113] *Id.* at 716.
[114] *Id.* at 714.
[115] *Id.* at 721.
[116] *Id.* at 723.

At this point of interruption, coupled with the cloning and scanning, a seizure has occurred, regardless of if it goes through "maximum deletion" afterward.[117]

Other authors that have confronted this idea have similarly found that a seizure occurs in the copying of data, albeit through different tests and for different reasons.[118] For example, Professor Paul Ohm, has proposed two different analytical approaches, both of which lead to the conclusion that electronic diversions constitute seizures. Ohm refers to the first approach as "Dominion and Control," and is derived from language in *Jacobson*:

> While the meaningful interference conception of seizure focuses on the deprivation to the property owner, the dominion and control class focuses on the usurpation by the state of the property. With physical property, these competing emphases are two sides of the same coin: by exerting dominion and control, the police meaningfully interfere with the owner's possessory interest.[119]

Separately, though related to the "Dominion and Control" test, Ohm also looked to a different formulation of the accepted seizure test – deprivation of a possessory interest.



---

[117] *Dr. Who-Rise of the Cybermen-Delete Delete, Delete Delete!* YOUTUBE, http://www.youtube.com/watch?v=4ecWDo-HpbE.

[118] Berk, *supra* note 93, 14 J. HIGH TECH. L. 1 (2014). ("Seen in this context, a search or seizure of information by a government agent should be treated no differently from a search or seizure of any other natural resource acquired from the world through the use of individuals' labor. While it is merely a technological innovation that permits us to acquire information on the scale that we have done through cloud computing, its acquisition is no different from any other acquisition. The information is no different from any other effect of a person's labor and should be treated, for purposes of the Fourth Amendment, exactly as any other property.") *See also* Mark Taticchi, *Redefining Possessory Interests*, 78 GEO. WASH. L. REV. 476, 496 (2010) ("The Supreme Court should hold that perfectly duplicating information seizes the information because it deprives the information's owner of her right to exclude others from it. To achieve this result, the Supreme Court should broaden its definition of possessory interest beyond mere physical possession to include an individual's right to exclude the government from her written or digital information. Under the proposed rule, any duplication process, such as photography or photocopying, that yields a perfect copy of a document in the owner's possession would be a seizure of the document's information because creating the copy would strip the owner of her ability to control the use and disposition of that information.").

[119] Ohm, *supra* note 101, at 13.

Ohm explains that there *is* a possessory interest in intangible property, namely an interest in the "right to delete." The "right to delete," says Ohm, is violated "when an owner loses control of a copy of her data [and therefore] the ability to dispose of or alter that data."[120]

In sum, although not definitively addressed by the courts, a variety of scholars taking a variety of approaches have concluded—and we agree—that the automated copying of digital files constitutes a seizure of those files, in essence because by doing so the government has deprived us of our control over how those files are disposed of. To return to an earlier analogy: how the football is handled after the opposing team intercepts it does not change the fact that it was in fact intercepted—or seized.

***INTERLUDE IV: THE MEN IN ROOM 641A***

***The Man has returned—and he's not alone.***

[120] Ohm, *supra* note 110, at 12; *see also* Ohm, *supra* note 101. In a footnote *to the Fourth Amendment Right to Delete*, Ohm notes that it is arguable that "a computer program that scans Internet traffic for particular text strings" may not have "seized every single packet flowing through the program" due to a *de minimis* interference with a "right to delete" during the short time the information comes into contact with the program. The question, he poses, is whether such a brief possession by the government would constitute a "meaningful interference with the right to delete." Ohm, *supra* note 110, at 16 n.32. Our answer is "yes", for three reasons. First, to conclude otherwise would undermine the basic premise of Ohm's theory: that seizure of a digital file occurs when the owner of that file loses control of how it is disposed of. That loss of control happened as soon as a copy was diverted to the scanning program, and the ultimate decision of whether and when to delete was no longer the owner's but the government's. Second, placing a temporal limit on whether a right to delete has been violated—a particular number of seconds, hours, days or more—would be completely arbitrary, and would essentially mean that whether a seizure had taken place would turn on how quickly the government could scan or make use of the data. Which leads to the third reason why even brief acquisition for scanning purposes is a seizure: as computing power increases, the ability to exploit a piece of data in ever-shrinking numbers of milliseconds also increases. To conclude that the quickly increasing speed with which the government can scan communications content actually affords us less legal protection would lead to both law and technology working in concert to continually erode our privacy rights. Yet as Justice Scalia made clear in *Kyllo*, new technology should not be allowed "to erode the privacy guaranteed by the Fourth Amendment," but rather the protections of the Fourth Amendment must keep pace with new technologies to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." 533 U.S. at 34.

***The room is bigger—much bigger—now with countless monitor stations for countless men and women to read the emails passing by. Dozens…hundreds…millions of people, always reading, in endless shifts. Now with reinforcements, the Man and his fellow readers don't miss a thing: they are able to take the time to read every single email from every single person. In fact, there are now enough readers to ensure that each email is double- and triple-checked.***

***No target is ever missed. Nothing escapes their eyes. Ever.***

## V. Conclusion: Privacy Versus The Robot Army, or Why Robotic Surveillance Is Worse Than Human Surveillance

Robotic review of emails implicates the privacy rights protected by statute and the U.S. Constitution at least as much as human review. More than that, though, robotic review is in many ways *worse* for privacy than human surveillance, since it allows mass surveillance with a scope, speed, and accuracy that even untold thousands of humans working around the clock could never provide. The manner in which automated surveillance facilitates such mass surveillance—unconstrained by the practical difficulties and costs of doing similar surveillance using human investigators—was one of the key concerns of several Justices of the Supreme Court in the recent landmark case of *U.S. v. Jones*, and that case provides an important lens through which to view the issue of robotic surveillance.

In *Jones*, the Supreme Court considered whether the police's attachment of a Global Positioning System (GPS) device to a suspect's car, and the use of that device to monitor the car's movements along public roads for twenty-eight days, constituted a search under the Fourth Amendment.[121] While a majority of the court held that the attachment of the device constituted a search,[122] five justices in two concurring opinions concluded that the tracking itself also was a search.[123] As Justice Alito explained:

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any

[121] 132 S. Ct. at 948.
[122] *Id*. at 949-53.
[123] *Id*. at 954-57 (Sotomayor, J., concurring); 957-64 (Alito, J., concurring).

> extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance…. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[124]

Justice Alito concluded that the prolonged tracking at issue in the case violated an expectation of privacy because "society's expectation has been that law enforcement agents and others would not-—and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period."[125]

Similarly, society's expectation has been that intelligence agencies would not—and indeed, simply could not—monitor the content of every email of every person who communicates internationally, an effort that would be impossible absent an impossibly large and costly army of humans. But now, the NSA has a robot army to accomplish the impossible, a result that presumably would alarm the concurring Justices in *Jones*. Indeed, other commentators have sought to derive Fourth Amendment rules from the *Jones* concurrences that specifically address—and seek to prevent—technology-enabled mass surveillance.[126]

Ultimately, in the case of robotic searches of communications content already protected by an expectation of privacy, such special rules for mass surveillance

---

[124] *Id*. at 963-64 (Alito, J., concurring).
[125] *Id*. at 964 (internal citation omitted).
[126] *See, e.g.,* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71-72 (2013) ("In our view, the threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state…."); *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 356 (2014), http://yalelawjournal.tierradev.com/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones (proposing a Fourth Amendment analysis keyed to the exponentially falling costs of surveillance due to advances technology, concluding that "where technology renders previously impossible surveillance possible on a mass scale, the Fourth Amendment must be applied to restore equilibrium.").

technologies based on *Jones* may not be necessary. Whether individualized or in bulk, such robotic searches already intrude on our privacy, whether as an interception, a search, or a seizure. But the mass surveillance that is enabled—and indeed is being accomplished—by virtue of such robotic searches amplifies the privacy violation beyond measure, and far beyond what would ever have been possible before. As more and more robot eyes watch more and more of what we do, answering the questions posed in this paper will become that much more urgent, or else we will soon find ourselves in a world where nothing and no one is free from the robots' gaze.