CHAPTER 5

The Fourth (and First) Amendment: Searches with, and Scrutiny of, Neuroimaging

Abstract The questions raised of Fourth Amendment law by neuroimaging at first seem to have simple answers: The Fourth Amendment covers neuroimaging because probing any part of the body's interior is a "search." The standard level of protection against such a search is the warrant requirement, imposing on government the responsibility of showing probable cause and specifying the place to be searched before conducting such a search. However, matters are not so simple. There is significant gray area in the Fourth Amendment that the court has used to give government flexibility in meeting vital security interests. This chapter shows that some of the answers to these Fourth Amendment problems may unexpectedly have First Amendment solutions.

Keywords First Amendment · Fourth Amendment · Free speech · Neuroimaging · Search · Searches incident to arrest · Special needs searches · Third party doctrine · Warrantless · Warrants

An Overview: Why Neuroimaging Raises Fourth Amendment Problems

In one key respect, the Fourth Amendment questions raised by neuroimaging are far easier to answer than those raised by the Fifth Amendment's self-incrimination clause. Does the self-incrimination clause bar compelled

M.J. Blitz, *Searching Minds by Scanning Brains*,
Palgrave Studies in Law, Neuroscience, and Human Behavior,
DOI 10.1007/978-3-319-50004-1_5

neuroimaging of a criminal defendant? The answer isn't clear because it is not clear if neuroimaging represents the kind of "self-incrimination" covered by that clause. As explained in the previous chapter, it is only incrimination through a witness's testimonial evidence – not through physical evidence – that is covered by the clause. So, we have to determine on which side of this dividing line neuroimaging falls.

By contrast, our task is easier when we ask if the Fourth Amendment constraints compelled neuroimaging. It constrains any police investigatory technique that counts as a "search" or "seizure." Is a brain scan a "search"? As I noted in Chapter 2, the answer is almost certainly "yes." And almost all scholars who have addressed the question agree it is "yes." A government engages in a search when it intrudes upon an area where one has a "reasonable expectation of privacy," (Katz v. United States 1967, 360–361) and the interior of our bodies is one such realm. As Michael Pardo writes, "subjects have a 'reasonable expectation of privacy' in information about their brain states," just as they do about "other information about inner bodily processes such as the contents of one's blood or urine" (Pardo, 2006, 325). Police certainly intrude upon an individual's privacy, as well as his dignity and comfort, when they take a blood test which, as the Court has observed, requires "piercing the skin" with a needle and "extract[ing] a part of the subject's body" (Skinner v. Ry. Labor Executives' Ass'n 1989, 625). Urine tests do not require such surgical "intrusion into the body," but as the Court observed, they are nevertheless searches since they "can reveal a host of private medical facts about an employee" and because "visual or aural monitoring of the act of urination, itself implicates privacy interests." Breath-testing procedures too, said the Court, "implicat[e] similar concerns about bodily integrity and, like [a] blood-alcohol test should also be deemed a search" (Skinner v. Ry. Labor Executives' Ass'n 1989, 616).

Brain scans are, in some respects, less intrusive than all of these other searches of the body, since they do not require the individual to provide authorities with any biological material. Authorities merely observe brain activity – and obtain information from it. Still, even a medical device that simply extracts information from inside the body counts as a search. As noted earlier, courts have consistently held that where the government uses magnetometers or X-ray devices at airports to reveal information about what a traveler is carrying beneath a jacket, or inside a bag, this is a "search" – even if the authorities do not physically examine the traveller's clothing or bag (United States v. Epperson 1972, 770; United States v. Albarado 1974, 803–805). It seems clear that it is likewise a search when

authorities use electrodes, radio waves, near infrared radiation to probe more deeply – and gather information not just from underneath her clothing, but underneath her skin. Indeed, while these X-ray and magnetometer cases have been decided by federal circuit courts, the Supreme Court itself has made it clear that law enforcement personnel cannot use advanced technology that lets them see or listen through walls to violate the home's privacy and integrity, even though police can thus search a home from a public place. They cannot, said the Court, use a radio transmitter to track a person's movements inside his home (United States v. Karo 1984, 714–718). Nor can they use a thermal imaging device to collect details about a home's interior from a public street outside (Kyllo v. United States 2000, 34). As Pardo notes, if, as the Court has made clear, "one has a reasonable expectation of privacy in the details of one's home (even when measured from outside with a thermal-imaging device)... one plainly also has a reasonable expectation of privacy in the details of what is in her head, even though the government doesn't have to invade the body to learn the information" (Pardo 2006, 325). Madison Kilbride and Jason Iuliano similarly argue that "[j]ust as searching a person's house with a thermal-imaging device or eavesdropping upon a person's phone conversations undermines that individual's privacy interests without invading his bodily space, so, too, does neuro lie detection infringe upon a person's right to privacy in a non-physical manner" (Kilbride and Iuliano 2015, 141–42). Amanda Pustilnik likewise argues that compelled neuroimaging should count as a "searc[h] of private information within a space of presumed privacy," and thus receive Fourth Amendment protection (Pustilnik 2013, 121).

The more complex Fourth Amendment issue raised by neuroimaging technology is not whether US citizens are protected from law enforcement use of it (they are), but how much protection they get. This may initially seem like an easy question too. Typically, when a particular investigatory measure is a "search," police cannot carry it out unless they first obtain a warrant from a neutral magistrate. To do so, they have to specify the "place to be searched" and explain why they have "probable cause" to believe they will find evidence of a crime where they wish to search. So, one might assume that if police wish to obtain a brain scan from a person, that is precisely what they will have to do. They will have to specify whose brain it is that they wish to scan. They will then have to explain to a neutral magistrate why they expect that a brain scan will reveal evidence related to criminal activity (for example, by revealing that the person recognizes the

murder weapon or by allow them to infer some other memory about how the crime was committed). If the magistrate is convinced by these arguments that police have "probable cause" to conduct the search, she will issue a warrant permitting them to do so, and defining its scope.

So, in sum, there is a fairly straightforward answer to what many scholars call the "coverage" question raised by neuroimaging: It is a "search" and thus covered by the Fourth Amendment's reasonableness constraints. There is also a fairly straightforward answer to the "protection" or "procedure" question: Police can typically conduct a search only if they have a warrant based upon probable cause and particularly stating where they will search. In fact, in the normal circumstance, a Fourth Amendment search carried out without a warrant is "per se unreasonable" – and thus, unconstitutional (Katz v. United States 1967, 357).

Why then is there any Fourth Amendment puzzle about whether and when police can use neuroimaging? Such puzzles arise from the extraordinary amount of gray area within Fourth Amendment law itself – a gray area that the US Supreme Court has had to wrestle with practically every year during the past decade as it tries to figure out how emerging technologies – raising unprecedented challenges to privacy – fit into Fourth Amendment doctrine, and whether they demand that this doctrine be changed.

Let me preview some of the key uncertainties about neuroimaging's Fourth Amendment status. First, two complications in coverage: The government engages in a Fourth Amendment search when it requires citizens to, say, submit to an EEG test. Would it be doing so, however, if without revealing the law enforcement use they would make of neuroimaging data officials convinced someone into unwittingly providing such data on a brain-computer interface for a video game, or that one uses in surfing the World Wide Web? Or if they obtained such EEG data from a non-governmental hacker (perhaps a professional "brain hacker")? Under the so-called "third party doctrine," one might argue that it wouldn't be. Under that doctrine, when we share our information with a third party, we assume the risk they will pass it on to government (voluntarily or in response to a subpoena). And if that risk materializes, it's still not a Fourth Amendment search. Under existing Fourth Amendment doctrine, we can't claim that government has invaded our private space to obtain such EEG information – when it obtained that information not from a private space but rather from another source to which we willingly provided it.

There is also another development (albeit an unlikely one) that could make Fourth Amendment coverage vanish. Sometimes, even a government probing of a highly-private space is not a "search" – because the constraints the Fourth Amendment is designed to impose are, in effect, already built into the technology. One of the few examples is a "dog sniff" by a police canine trained to alert only to the presence of cocaine or heroin. If police bring the dog near our car or our suitcase, they are in effect exploring the interior of these private realms – something that would normally be a search. But the dog can only provide one piece of information about this private interior realm – and that is whether it contains illegal drugs. And that piece of information about what lies within a private interior space is something, the Court has found, in which we have no legitimate privacy interest. One might ask then: Are there certain kinds of neuroimaging that would reveal only memories or knowledge that a person has no right to keep private – for example, a memory that reveals the person responsible for a murder or a kidnapping? If so, could that make such use of neuroimaging a non-search, especially if the testing technology told law enforcement nothing else about the brain activity of the person being tested. For reasons I will explain, this argument is unlikely to work: Even a breathalyzer test that tells a police officer nothing but a person's blood alcohol level still involves an intrusion into bodily privacy of a sort that a dog sniff of luggage or a car does not. And the same is likely to be true of neuroimaging. Still, it is useful to raise this question, both because it helps us think a little bit more about the Fourth Amendment interests at stake when someone is subject to neuroimaging, and also because it helps lay the groundwork for certain questions that arise when we turn to Fourth Amendment protection.

And neuroimaging also raises questions about such protection. Indeed, most of the Fourth Amendment gray area that is relevant to neuroimaging concerns the question of "protection." I will say a little bit about these questions here and then look at them more closely later. Consider, first, some of the questions that might arise even if it is clear that a warrant is required. More specifically, imagine that a group of law enforcement investigators wishes to take a brain scan of a person whom they have probable cause to believe is involved in a counterfeiting operation. They also have suspicions that the same person may be involved in a plan to carry out domestic terrorism in the coming months, and that money from the counterfeiting operation may be directed to those plans. On the basis of information suggesting a link between this person and the counterfeiting, they

seek a warrant from a judge to take a brain scan of the suspect so they can run brain scans to gather more detailed information about the operations and his connection to it. One set of questions likely to arise concerns the scope of the warrant: What will such investigators have to tell a judge to "particularly describe the place to be searched"? Is it enough for them specify that they are seeking evidence about a counterfeiting operation and will try to derive it from using an EEG or fMRI to probe the suspect's response to particular stimuli? Or do they have to describe the methods to the judge in more detail, for example, by describing what kind of images, words, or other stimuli they will show the suspect, so it is clear they will not gather more information about his beliefs, thoughts and feelings than what they need? If, in gathering information about the counterfeiting operation, they find evidence which they believe is relevant to the terrorism plans they believe to be associated with it, or evidence of other criminal activity, do they need another warrant to capture and analyze such additional neuroimaging evidence?

Moreover, one might ask, should a warrant that authorizes a brain scan require nothing more than probable cause and satisfaction of the particularity requirements? Or when mental privacy is at stake in this way, should the government be required to meet a higher threshold? Should it, for example, be required to show (as it is when it seeks a warrant to conduct surreptitious video surveillance in a private area) that other less intrusive measures of obtaining the same information won't work?

Other Fourth Amendment questions will arise if the government wants to use neuroimaging technology in circumstances that have, in the past, normally made it "reasonable" and thus permissible for government to use a warrantless – or even suspicionless – search. The government, for example, does not need a warrant to search you as you enter the United States. It doesn't even need reason to suspect you. There is a "border search" exception to the warrant requirement. The same is true at airports. No matter how unlikely it is that you are a threat to airline safety, if you are a traveler planning to board a flight, you need to go through a magnetometer or other screening device, and submit your luggage to similar screening (and to any physical searches the government deems necessary). Government may also conduct warrantless searches "incident to arrest": it can, for example, require individuals arrested for drunk driving to submit to breathalyzer tests to determine the level of alcohol in their bodies.

How, one might ask, might neuroimaging fit into each of circumstances? Would a permissible warrantless search remain permissible if the government

decided to add brain scanning to its use of magnetometers or breathalyzers? Or would that kind of evidence-gathering about brain operations and mental activity bring it to a Fourth Amendment red line which – even at a border station, an airport, or a police station processing an arrest – it can't permissibly cross without careful judicial oversight? May police, for example, subject an arrestee to a brain scan shortly after arresting him in order to see if any of his accomplices are nearby? May they try to gain some access to knowledge of his accomplices' whereabouts before it becomes stale, or he begins to forget? Might school officials worried about the threat of school violence, or airport officials worried about terrorism, add neuroimaging to the set of tools they use to detect and thwart violent threats?

Fourth Amendment Coverage – and Kyllo v. United States

As Orin Kerr writes, Fourth Amendment doctrine, and its rules of coverage, effectively divide up government evidence gathering into two parts: There are "less invasive steps the government can take at any time, and more invasive steps the government can only take when it has already collected enough evidence to demonstrate special conditions such as probable cause" (Kerr 2009, 574). For example, when police monitor events in public space – for example, a "park or on open fields" – they are conducting surveillance that is unlikely to interfere with our private lives and which they can therefore undertake whenever they like. By contrast, when police want to look into a "home or private packages" – they *are* conducting a Fourth Amendment search and therefore need to obtain a warrant or otherwise show their investigation is constitutionally reasonable. This line between "less invasive" steps in public space and "more invasive steps" into homes or other private spaces is essentially the line that marks the boundaries of Fourth Amendment coverage: The private spaces are covered by the Amendment, the public spaces are not.

This framework provides yet another way to reaffirm the scholarly consensus on neuroimaging: It gathers evidence from inside our bodies, so it is among the "more invasive" steps that law enforcement officials can only conduct if they satisfy Fourth Amendment reasonable requirements, typically by first obtaining a warrant. But before we treat that as the full story on Fourth Amendment coverage for brain imaging, it is useful to say more about this framework – and it is useful to use a 2001

case called Kyllo v. United States to better understand how the Fourth Amendment divides up the world into (1) spaces where the government has free reign to gather evidence, and (2) spaces where we can generally exclude it, and prevent evidence-gathering, unless and until government has good justification for entering.

Kyllo is a case that receives mention from neuroscience and law scholars for a number of reasons. Pardo, as noted earlier, cites it to show that one can conduct a search of the body (as of the home) even when standing outside it and using technology to peer in (Pardo 2006, 325). Amanda Pustilnik cites it both for that reason – and also to argue that, just as the Court in Kyllo was protecting the privacy of the life within the home, and not simply the home as a structure, so Fourth Amendment protection for neuroimaging might protect not just the privacy of our brain physiology, but the interior mental experience that it generates (Pustilnik, 2013, 131–134).

Kyllo essentially held that when police use a thermal imager to gain information about a home's interior, they are conducting a Fourth Amendment search – and need a search warrant to do so. An agent of the US Department of Interior, William Elliott, suspected that an individual by the name of Danny Kyllo was growing marijuana inside his home. Such in-home marijuana cultivation required use of a "high intensity lamp," such as a halide light, and Elliott and a colleague realized that, if Kyllo were using such a lamp, it would – because of its heat, emit plenty of infrared radiation – radiation they could detect from outside of Kyllo's home with a thermal imaging device. They therefore pointed such a device at Kyllo's home, while sitting in their car across the street from it, and found that an area over the garage of the home emitted considerably more infrared radiation than the rest of the home, and considerably more than was emitted from the homes of Kyllo's neighbors (Kyllo v. United States 2000, 30). On the basis of this information, as well as information in utility bills (to provide more evidence that an energy-intensive lamp was being used inside) and tips from informants, the agents obtained a warrant to enter and search Kyllo's house – where they found the lamp and "in indoor growing operation involving more than 100 plants" (Kyllo v. United States 2000, 30).

Kyllo, however, argued that the agents needed to obtain a warrant – based upon probable cause – not only to enter and search his home, in the later stage of their investigation, but also before they pointed the thermal imager at his house, and recorded the infrared radiation that could give them clues as to Kyllo's private activities. Pointing the thermal imager at the home, he argued, was itself a Fourth Amendment search (Kyllo v. United States 2000, 37).

The Supreme Court agreed. Agents could, it acknowledged, look at a home from the street outside – and such visual surveillance by itself would not constitute a search (Kyllo v. United States 2000, 32). So, for example, had Elliott and his colleague stood across the street from Kyllo's home, stared at it, and seen bright light from the halide lamp through a large open window, they would not have been engaged in a search. Nor would they have engaged in a search if they conducted such visual surveillance, and noticed drug paraphernalia lying in a garbage can in the street outside Kyllo's home. In fact, the Court had previously ruled that even if agents hovered over a greenhouse in a helicopter, and noticed marijuana being grown through a crack in the greenhouse roof, such visual surveillance from an aerial perspective wouldn't be a search either (Florida v. Riley 1989, 450–452). But the investigation of Kyllo's house with a thermal imaging device, said the Court, involved "more than naked-eye surveillance of a home" (Kyllo v. United States 2000, 33). The device allowed police to perceive activities within the home's interior not through an open window, or a crack in its structure, but through a solid wall. That insider's perspective on the home, reasoned the court, would previously have been impossible without entering the home itself. And when "sense enhancing technology" is in this way a functional substitute for "physical intrusion into a constitutionally protected area," then use of it by law enforcement should be subject to the Fourth Amendment, and subject to its privacy safeguards (Kyllo v. United States 2000, 34).

Pustilnik offers Kyllo as a good model for explaining Fourth Amendment coverage for an EEG measurement: Just like "thermal signatures from a home," she explains, "electrical brain waves are automatically and continuously produced," and so one might argue that they are – in some sense – there for the taking for anyone who can unobtrusively gather such information from outside (of a private home, or of person's body) (Pustilnik 2013, 133). But both of them are not only "invisible and undetectable absent technology" – they can also both be "decod[ed]" to reveal information that people typically consider to be at the core of their privacy: The home life people are able to shield from public view and thoughts they avoid sharing (sometimes even with family or others in their home) (Pustilnik 2013, 133). Moreover, the Court also took a position that is instructive for analysis of brain scan technology by focusing not only on the crude capacities of thermal imaging existing in the late 1990s (when Kyllo's home was searched) but also on the "imaging technology" that might develop in the future and might "discern all human activity in

the home" (Kyllo v. United States 2000, 35). In applying Fourth Amendment law to brain scanning, courts might likewise take account not just of brain scanning as it exists today, but also as it is likely to evolve over the coming decades.

Kyllo's template for covering new surveillance technologies is certainly an attractive and useful one. But we need to say more about it – and how brain scan technology might be analogized to it – in order to understand whether it provides the basis for an approach to Fourth Amendment coverage that takes sufficient account of the value of intellectual privacy. More specifically, it is helpful to understand Kyllo not only by looking at the Court's conclusion and the core reasons it gives – but at the other side of the debate that occurred between different Justices in that case. While Justice Antonin Scalia held, supported by a majority of the Court, that police engage in a search when they use a thermal imager to gather information from the home's interior, Justice John Paul Stevens vigorously argued that it was not a search – and the Fourth Amendment should thus leave such police use of thermal imaging unconstrained. This was not because Stevens believed that the privacy of the home was unimportant. On the contrary, he emphasized in his dissenting opinion that "the homeowner has a reasonable expectation of privacy concerning what takes place within the home, and the Fourth Amendment's protection against physical invasions of the home should apply to their functional equivalent" (Kyllo v. United States 2000, 44). But this, he said, could not shield from police view, what was visible on the outside of the home's walls. The home's exterior walls and the environments outside of the walls were part of the "public domain," that – in a free society – can be viewed by citizens other than the property owner (including police officers). Thus, he noted, "any member of the public" on the street outside the house "might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces" (Kyllo v. United States 2000, 43). Or he might make inferences about what a person is cooking inside a kitchen by smelling the aromas that float outside (Kyllo v. United States 2000, 43). The thermal imager, said Stevens, simply took as its raw material, and then refined, such physical occurrences in the home's exterior – in this case, the heat that leaked outside of its walls.

We might elaborate and sharpen Justice Stevens's objection here by connecting it with an observation the Supreme Court made in an earlier case where it found that police could gather certain information outside of

the home from a public vantage point: In Ciraolo v. California, the Court held that police did not conduct a Fourth Amendment search when, in following up an anonymous tip that a home owner was growing marijuana in a backyard garden, they flew a plane 1000 feet over the garden and identified the marijuana plants below (Ciraolo v. California 1986, 209). In explaining why it was not a Fourth Amendment search for police to conduct such a fly-over, the Court emphasized that this kind of observation from a public vantage point is "precisely" the kind of information that "a judicial officer needs to provide a basis for a warrant" (Ciraolo v. California 1986, 213). In other words, our homes can remain constitutionally insulated from police investigation only because there is some *other* place – namely, the public domain – where police can vigorously gather evidence of possible criminal activity before taking the more extraordinary and intrusive step of entering the home. If even the large swathes of public domain become off-limits to warrantless police observations then they will have nowhere to begin their investigations. To obtain a warrant allowing them to search the inside of a home for marijuana operations, they need to first get some information from somewhere outside of a home to show that such an inside search is justified. If the law then tells them they need a warrant to scrutinize the outside of the home (with, for example, aerial surveillance or a thermal imaging analysis of heat emissions), then it may be hard to see how (and where) police can begin to build a case for focusing on a particular target. Justice Stevens's dissent then, can be read as an argument that while a just balance between crime fighting and privacy can bar police from closely examining the details of the home's interior – it cannot also reasonably demand that police ignore clues about this interior activity that they find in the public domain. By preventing police from learning anything about a home's interior, even from evidence available in the street outside, one will be making it impossible to tell when the home is being used not simply as a refuge in which people can find privacy from the world, but also as a site for hiding criminal operations.

Stevens's dissent also contains another important challenge to the majority decision in Kyllo. That decision had emphasized that when law enforcement aims to, and succeeds, in extracting information from the home's interior, it does not matter how personal or sensitive that information. Even information that seems so mundane as to be non-private is still staunchly protected from police observation when it is inside the home: as the Court says, entry into the home constitutes a Fourth Amendment search requiring a warrant even if an officer "barely cracks open the front

door and sees nothing but the nonintimate rug on the vestibule floor . . . in the home . . . all details are intimate details, because the entire area is held safe from prying government eyes" (Kyllo v. United States 2000, 37). But if one is prevented from learning non-intimate details, even with technology employed outside the home and focused only on the home's exterior or its environment, then – Stevens worries – law enforcement may be barred even from common-sense strategies for "detect[ing] the odor of deadly bacteria or chemicals for making a new type of high explosive" (Kyllo v. United States 2000, 48). Even where a technology is – "like [] dog sniffs" designed to detect only drugs or explosives – or to detect nothing more than contraband or dangerous weapons – the majority's rule in Kyllo, worries Stevens, may still make it impermissible for police to use it without a warrant. In other words, not only do police have a right to investigation (without any warrants) outside the home. They also have a right, on Justice Stevens's view, to try to gather information even from inside the home, when the only information they are trying to gather is information of the kind a person has no right to keep private – such as the presence of "chemicals for making a new type of explosive" (Kyllo v. United States 2000, 48).

None of this is to say that Justice Stevens or any other Supreme Court justice would have excluded brain-based mind reading from the Fourth Amendment's coverage – or ignored the privacy interests that may be at stake in it. On the contrary, Stevens made it clear that while he believed that it is not a search for police to use a thermal imager to detect heat emanations on the exterior, it *would* be a search if they used what, in his view, was the electronic "functional equivalent" of a "physical invasion of the home." The agents who viewed Kyllo's home, for example, would have conducted a search, argued Stevens, had they been able to use something more like "an x-ray scan, or other possible 'through-the-wall' technique" (Kyllo v. United States 2000, 43). An fMRI or fNIR brain scan derives evidence of brain processes by gathering information from blood flow inside the body. It does not, like the reading of micro-facial gestures, seek to detect dishonesty or other internal mental states from observations of a person's visible behavior. And Stevens would also probably be amenable to the argument that what makes our invisible brain processes so private is not simply that they are inside the body, but that they can be used to infer evidence of our thoughts.

Still, Stevens's dissent in Kyllo – and the similar arguments the Court has made over the years for assuring that police are left with some space in

which they can find the necessary evidence to lay the groundwork for successful crime-solving work – raise important questions about the basis, and extent, of Fourth Amendment coverage for brain scanning. In short, Stevens's arguments emphasize that there are at least two situations where Fourth Amendment coverage that is normally present – say for activities in the interior of a house – vanishes: (1) where police do not collect evidence from inside the house, but collect information from the public world outside of the home – either because they can observe it there, or because they can obtain it from someone who shares it with them, or (2) where instead of remaining outside the home, police use a technique that penetrates into the interior but tells them only about activities that the individual has no right to conduct – such as possessing illegal drugs or manufacturing explosive materials. Each of these highlight two possible exceptions to the general rule that brain imaging would almost certainly be a Fourth Amendment search and it is worth considering each of them a little more closely.

Fourth Amendment Coverage – and Third Party Doctrine and Abandonment

There are certain activities we take that we do not leave entirely open to observation, but which the Supreme Court has long said are public enough to be fair game for government to investigate without a warrant, and indeed, without any Fourth Amendment limits. This happens, for example, when we abandon items, leaving them to be examined by any one who recovers it (including police). For example, when we dispose of garbage, we often enclose it a sealed bag: We do not leave it open to observation by the rest of the world. But because we are disclaiming any property interest in it and leaving it to be picked up by a trash service, we lose the right to treat it as a private space under our control.

This abandonment doctrine was central to the Court's ruling in the 1988 case Greenwood v. California. In that case, police had received tips that a man named Greenwood was engaged in drug trafficking. So, they contacted the trash collector for the neighborhood, and asked him to preserve Greenwood's trash for police to look at, making sure that it wasn't mixed with those of others in the neighborhood. When police then examined the bags they received from the trash collected, they found items indicative of drug use – and used them to obtain a warrant to search Greenwood's house. Greenwood claimed (as Kyllo would later do)

that they needed a warrant not only to search the house, but even earlier in their investigation – in this case, when they wanted to search his trash. The Court, however, held that he lacked a reasonable expectation of privacy in its content: Once left on "a public street" where it was accessible to "animals, children, scavengers, snoops, and other members of the public," he could retain no further interest in it. Having abandoned the items in the garbage, Greenwood could not expect to control who examined them (Greenwood v. California 1988, 40–42). This was true, even though there are many things people dispose of that they might be uncomfortable sharing: As the dissenting opinion pointed out, "A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it. A search of trash, like a search of the bedroom, can relate intimate details about sexual practices, health, and personal hygiene" (Greenwood v. California 1988, 50).

As Elizabeth Joh points out, courts analyzing "abandoned DNA" have followed Greenwood's analysis and have concluded that "there is no objective expectation of privacy in saliva – and the DNA contained within it – that is left behind on a coffee cup or on a smoked cigarette." Indeed, in some circumstances, suspects have been tricked into providing DNA samples. Police have sometimes "act[ed] as passive collectors, waiting for a suspect to discard a smoked cigarette or to spit on the floor" (Joh, 2006, 868–872). In one notable use of a similar DNA-collection technique in a Washington murder investigation, "Seattle Police Department detectives, posing as a fictitious law firm, induced [the suspect,] Athan to mail a letter to the firm, from which Athan's DNA sample was extracted." Following the pattern described by Joh, the Washington State Court found in that case that, because "obtaining the saliva sample in this case did not involve an invasive or involuntary procedure," Athan retained no privacy interest in the saliva he voluntarily used to seal the envelope (State v. Athan, 2007, 31, 33).This abandonment doctrine has been subject to scholarly criticism, by Joh and others. For example, in analyzing Canada's equivalent of Fourth Amendment protection, Ian Kerr and Jena McGill explain that if it is constitutionally problematic for police to learn about the interior of our homes from heat "emanations" released from it into the outside world, it should be similarly problematic for police to learn about a person's interior through use of the information "our bodies emanate" in "DNA from flaking skin cells and shedding hair" and "electrical activity from brains and hearts" (Kerr and McGill, 2007, 393). But Fourth Amendment law continues to treat the latter type of information sources as unprotected.

There is also another circumstance where information is treated as open to police observation even when it is public: When we convey information to a third party, that party can then share it with government (whether voluntarily or in response to a subpoena), without that sharing counting as a Fourth Amendment search. This doctrine first originated in cases involving government informants: In On Lee v. United States, the government recruited a friend of a suspect drug dealer to act as an informant and surreptitiously record the suspect with a hidden microphone (On Lee 1952, 748–751). Similarly, in Hoffa v. United States, Jimmy Hoffa made the mistake of confiding in a friend who was secretly working with the police (United States v. Hoffa 1966, 294–302). In these and other cases, the Court made clear that the government's use of an informant was not the kind of invasive technique that counted as a Fourth Amendment search: The Fourth Amendment, said the Court in Hoffa, does not protect individuals against misplaced trust.

The Court then extended this logic to make clear that other kinds of sharing of information we undertake are also taken at our own risk. Even if we are dealing not with friends (who we might or might not decide to continue trusting), but rather with companies we have little choice but to deal with if we want to participate in modern life – companies such as banks or telephone companies – we still lose the right to prevent these third parties from, in turn, sharing it with government. Thus, in Smith v. Maryland, the Court held that it is not a Fourth Amendment search for law enforcement to obtain, from the phone company, records of the phone numbers dialed from a customer's home (Smith v, Maryland 1979, 741–743). In United States v. Miller, it likewise held that it is not a Fourth Amendment search for law enforcement to obtain, from a bank, copies of checks an individual has deposited. While we may hope and expect that these businesses will maintain the privacy of our calling or financial records, our sharing of this information nonetheless places it into the realm of information where police's access to it is considered a "less invasive" investigative step, not subject to Fourth Amendment limits (United States v. Miller 1976, 441–443).

One question we might ask about brain imaging data then is whether there might be circumstances where it too is treated as abandoned or shared in a way that takes it outside of the Fourth Amendment's ambit. This is certainly not the scenario most writers imagine when they imagine law enforcement use of brain imaging: They imagine a government agent asking questions of a subject undergoing a brain scan, or presenting him

with images or other stimuli and assessing his brain responses. But there are three scenarios – further removed from existing technology – where third-party doctrine would be more relevant.

First, as Stacey Tovino observes, insurance companies, for example, could conceivably want "individuals' neuroimaging information . . . to predict future illness, a propensity to violence, or other conditions or characteristics relevant to underwriting decisions" (Tovino 2005, 847–848). Employers may also have an interest in collecting neuroimaging information about their employees. As Tovino notes "the federal Employee Polygraph Protection Act ('EPPA') prohibits employers from requiring employees to submit to lie-detector tests, defined to include polygraphs, deceptographs, voice stress analyzers, psychological stress evaluators, and 'any other similar device'" and this would likely cover use of brain imaging to assess an employee's honesty. But this leaves open the possibility that neuroimaging information would be used for other purposes. And it is conceivable that individuals seeking certain types of psychiatric or other medical treatment would undergo brain imaging, leaving records that might be claimed by government.

Of course, if neuroimaging measures only individuals' responses to specific stimuli, then it is unlikely it will include information of precisely the kind law enforcement is looking for in solving a specific crime. An insurance company seeking to assess an individual's tendency to take unwise risks will not typically have reason to ask whether a client is familiar with aspects of a particular crime under investigation.

Second, apart from situations where companies collect neuroimaging information from individuals, and then share it with law enforcement, it is conceivable that we will collect neuroimaging information about ourselves – or leave a data trail about it as we play video games we control with EEG technology or with other kinds of brain-computer interfaces. As noted earlier, companies such as Emotiv and Neurosky have marketed video games that use a variation of EEG technology to allow gamers to control video-game play (Childers 2013). In 2012, Ivan Martinovic and his colleagues conducted experiments demonstrating "the feasibility of using a cheap consumer-level BCI gaming device to partially reveal private and secret information of the users." They attempted to use evidence – from EEG-based gaming systems – of P300 reactions to infer information about banks and credit cards (Martinovic et al. 2012). They also noted that while their own experiment was fairly simple, it was easy to conceive of "more sophisticated attacks" – for example, attacks in which "an uninformed user could be easily engaged into 'mind-games' that camouflage the interrogation of

the user and make them more cooperative." Martinovic and his colleagues were primarily concerned about how mental privacy could be compromised in identity theft or other crime. But techniques that "camouflouge the interrogation of a user" could also, of course, be used by a government informant, like those in On Lee and Hoffa. Tamara Bonaci and Howard J. Chizek also analyze the privacy concerns that arise as individuals use brain-computer interfaces – and note that "several marketing companies . . . have shown interest in the usage of BCI devices for marketing research" and that "if BCI devices become widespread we might see private information extracted from individuals without their permission" (Bonaci & Chizek 2013).

As a number of writers point out, intellectual privacy has already been compromised by the migration of numerous activities – including those involved in intellectual exploration – to the Internet. Julie Cohen, for example, pointed out in 1996 that individuals' reading habits, which had been a traditionally private activity, were increasingly subject to being monitored as people switched from reading physical books to digital books on the Web (Cohen 1996, 1004–1019). The spread of Kindle and other electronic reading services makes it easier to track reading habits. More recently, Neil Richards has pointed out that an "your ISP has records of every website you've visited – transcript of your intellectual explorations, of your reading and thinking" (Richards 2015, 5). To the extent that brain computer interface (BCI) interactions merge with on-line gaming or other interactions, we may add to this trail of data about our reading and Web-searching choices, data that might reveal some of the feelings or other internal reactions we have as we interact with Web-based content.

Third and finally, there is one more scenario that might make it relatively simple, and common, for parties other than government to obtain information that they can share with government agents. Nita Farahany notes that "police may soon be able to monitor suspicious brain activity from afar" and that "various government agencies are funding the development of technology to detect brain activity remotely and are hoping to eventually decode what someone is thinking" (Farahany 2008). Of course, even if government can monitor the brain from a distance, it would likely be just as engaged in a Fourth Amendment search as it is when it detects a home's infrared radiation from a decent distance. But if technology arises that allows government to monitor a "suspicious brain from afar," the same technology will allow others to conduct such monitoring – and then share such information with government, free of Fourth Amendment restraints.

Indeed, if such technology for remote brain imaging became sufficiently widespread – use of it may lose its status as a Fourth Amendment search for another reason. In Kyllo, even Justice Scalia, in noting that the Fourth Amendment should protect individuals from future as well as present technology, implied that the thermal imaging that was a search in that case might not be in the future. If and when thermal imagers ceased to be an uncommon and relatively unknown tool police could use to see into places where individuals expected to remain unseen – if they instead became a technology in "general public use" that Americans knew were in others' hands, and understood might affect their privacy – then police, he hinted, might be as free to use them as anyone else (Kyllo v. United States 2000, 34). Other scholars have pointed out that it is unclear how the court would determine when an investigatory technology is in "general public use" (Slobogin 2007, 57–58, 62–65, Adkins 2002, 262). However, it is at least possible that if neuroimaging devices become perhaps as pervasive as SmartPhones are today, and individuals can (legally) use them not only to gather information about their own minds, but also those of their neighbors, then use of such technology may no longer count as a Fourth Amendment search – even when it gathers information from within a person's body (Federspiel, 2008, 881–882).

In short, while the third-party doctrine is unlikely to leave police with free access to any kind of brain imaging data in the near future, it may be a part of the Fourth Amendment analysis in future technological landscapes if the technology both migrates out of the laboratory, and is used by individuals and private companies. This does not mean, however, that the Fourth Amendment doctrine of the future will necessarily leave government with access to such data.

Third-party doctrine has long been harshly criticized by Fourth Amendment scholars. Daniel Solove for example, argues that "[g]overnment access to records held by third parties should be covered by the Fourth Amendment" (Solove 2010, 1533). Stephen Henderson, writes that "the doctrine was controversial when adopted, has been the target of sustained criticism, and is the predominant reason that" in the view of many scholars Fourth Amendment law still offers far too little protection in the face of technological change (Henderson 2007, 1976). He notes, in a more recent article, that the third-party doctrine left the Fourth Amendment ill-equipped to protect us against automatic sharing of information and that courts seemed to recognize this: "Fourth Amendment Third Party Doctrine – which holds that a person retains no expectation of

privacy in information conveyed to another – has at least taken ill, and it can be hoped it is an illness from which it will never recover," and he proposes a four factor test that could offer Fourth Amendment protection to at least some kinds of third-party records – one factor of which protects transfer of records linked to First Amendment freedoms (Henderson 2011, 39–40, 48). Jane Bambauer similarly argues that "[t]he third-party doctrine may be dismantled soon, and for good reason. It always strained the logic and common sense of search and seizure law" (Bambauer 2015, 208). One reason for these predictions that third-party doctrine may not survive coming years of technological change is the opinion of Justice Sotomayor in United States v. Jones, which – although focused on the question central to the case about whether and when police can permissibly use GPS technology to track a car's movements in public – added that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (United States v. Jones 2012, 975).

However, as Henderson writes, it is one thing to reject the doctrine and urge that "some third-party information should be protected, and quite another to articulate how and when different information should be accessible to police" (Henderson 2007, 976). Whether brain imaging information is protected, even when we let it be captured in computer interactions or kept by third parties, would depend on what specific criteria courts adopted to decide what third-party records merit Fourth Amendment protection. What, in other words, might place certain third-party records back within the realm of the Fourth Amendment – on the private side of the private-public distinction, such that law enforcement access to and use of those records would be a "more invasive" method constrained by the Fourth Amendment rather than a "less invasive" one free of its restraints?

One argument, which I will elaborate upon in the next section, is that the relationship of a record to our intellectual privacy makes a difference here. Solove already makes an argument like this: Where third-party records have First Amendment value, at least some constitutional provision (the First Amendment if not the Fourth) should safeguard them: Such records would include "bookstore records" which "clearly fall within the boundaries of the First Amendment because they concern the consumption of ideas." "Internet search queries," he argues "are very similar to book records in that they involve a person's reading habits and intellectual pursuits" (Solove 2007, 286).

Data that allows authorities to draw inferences about our thoughts should similarly be among the kind of records that receive heightened protection against government monitoring. Even fragmentary evidence about our thoughts – the fact that we recognize an image, or feel anxious in response to it – should not be evidence government can help itself to when our response is manifested not in a visible observation (like a facial expression) but rather in the data generated by our use of a neurofeedback device, for example, which we use to produce information for our own medical needs, or our own entertainment or self-understanding, and not for government to use in the manner of its choice.

Fourth Amendment Coverage – and Perfectly Efficient Search Technology

There is another possible argument that some neuroimaging data will fall outside Fourth Amendment coverage. Recall, again, Justice Stevens's argument in Kyllo that police should be able to freely gather evidence even about what happens inside a home when the methods they use reveal only something dangerous or illegal – such as "the odor of deadly bacteria or chemicals for making a new type of high explosive" (Kyllo v. United States 2000, 48).

This is a search doctrine that Supreme Court had previously made the centerpiece of two cases. United States v. Place dealt with the question of whether the government engaged in a Fourth Amendment search when using a dog – trained to alert when it smelled illegal narcotics – to sniff the air around the luggage of a traveler whom the Drugs Enforcement Administration (DEA) had come to suspect might be carrying drugs. The Court held that the DEA agent's detention of the traveler's luggage was a Fourth Amendment "seizure," and that the length of its detention was unreasonable under the circumstances. The Court, however, also addressed, in the course of its decision, whether the government engages in a Fourth Amendment search when it uses a trained dog to sniff the package for drugs. The Court decided it did not: The dog sniff, said the Court, "does not require opening the luggage" and "does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage." Indeed, said the Court, the dog sniff reveals absolutely nothing except "the presence or absence of narcotics, a contraband

item" (United States v. Place 1983). This intrusion was so limited, said the Court that it did not even count as a Fourth Amendment search.

A year later, the Court applied the same analysis to a chemical test a government agent conducted on white powder that Federal Express employees had noticed in a damaged package and called the DEA to report. The DEA agent "removed a trace of the white powder" and administered a field test "on the spot" which "identified the substance as cocaine" (United States v. Jacobsen 1984, 112). As it had in Place, the Court found that the chemical test was not a Fourth Amendment search: "A chemical test that merely discloses whether or not a particular substance is cocaine," it said "does not compromise any legitimate interest in privacy" (United States v. Jacobsen 1984, 123). In fact, said the Court, "even if the results are negative – merely disclosing that the substance is something other than cocaine – such a result reveals nothing of special interest. Congress has decided – and there is no question about its power to do so – to treat the interest in 'privately' possessing cocaine as illegitimate" (United States v. Jacobsen 1984, 123).

In short, each of these cases were real-life versions of Loewy's hypothetical "divining rod," (discussed in Chapter 2) which reveals only the presence of criminal activity – without simultaneously revealing any innocent activity or data (Loewy 1983, 1247). Indeed, Loewy even suggested the use of "a marijuana-sniffing dog sniff" was one of the real life search methods closest to a divining rod – although he also noted that he opposed the "carte blanche use of marijuana-sniffing dogs," and that, to the extent that "the dog is less than perfectly accurate, innocent people run the risk of being searched" (Loewy Arnold 1983, 1247).

With these cases as background, one might ask whether this part of Fourth Amendment doctrine provides another rationale by which certain neuroimaging data might be excluded from Fourth Amendment coverage. If the only thing a certain brain imaging design tests is whether someone's brain activity shows that he is familiar with a murder weapon, might that be a non-search on the ground that no person has a legitimate interest in hiding familiarity with the weapon? Of course, it is possible that, if government infers from a person's P300 response, that he recognized a murder weapon, this inference will be mistaken – or, even if correct, will be detecting a sense of familiarity that doesn't arise from any kind of criminal conduct (just because he finds a weapon familiar-looking does not mean he used it in the crime). But the kinds of dog sniff and chemical tests that the Court held to be non-searches can also show false

positives – and this has not dissuaded the Court from excluding them from Fourth Amendment coverage.

Moreover, even when cocaine is genuinely in someone's luggage, this may not be evidence that the person carrying it is engaged in criminal activity: She may have been unaware of its presence, not realizing – for example – that someone else was using her as an unwitting pawn in a delivering the drug. Authorities may still have a powerful interest in detecting the drug. However, in stopping her and searching her suitcase, they are subjecting to government surveillance a space (in her luggage) that she generally has a right to regard as private, and is insulated by the Fourth Amendment from government investigation except when officials have powerful reasons to intrude into it. Why then, one might ask, doesn't the government have an equally good argument that it has a right to use non-intrusive methods that establish only whether someone shows familiarity with key evidence from a crime scene?

There are a few possible answers to this question. One is that a thought or feeling, no matter how closely connected it may seem to criminal activity, cannot itself be a contraband item – in the way that an illegal drug is. When one possesses an illegal drug, one possesses an item one has no right to have. A thought, by contrast, can never be illegal itself. It must always be accompanied by some kind of action to count as criminal. Moreover, tests – like Farwell's brain fingerprinting – do not present only the "probe" stimuli. They also ask the subject to react to other stimuli, and – no matter how mundane these may seem – they can reveal or confirm additional information about the subject's thinking. As a consequence, even if brain imaging is focused only on revealing limited information about a person's familiarity with certain items or images, it is highly unlikely the Court would classify it as so removed from any legitimate privacy interest as to be a non-search.

The fact that it involves probing into a person's brain and mind, and not merely a package or piece of luggage, adds to the case of maintaining Fourth Amendment coverage. And this is strengthened by Michael Adler's net-wide search hypothetical (discussed in Chapter 2). As Adler noted, even a search which – like that in Place or Jacobsen – is perfectly designed to reveal only contraband may seem at odds with a free society when it constantly or frequently brings the government into spaces from which, our society assumes, government must generally be excluded. Adler's example of such an environment is the digital storage space inside of our houses. Even if a particular government search there targets only what is illegal, "a search

that eliminates an individual's control over the boundaries to her most private realms would likely be perceived as a threatening exercise of coercive power." What makes this even more damaging is that, as Adler says (Adler 1996, 1112), such a search need not be limited to evidence of actions (such as murder) that are universally and enduringly recognized as wrong. "[V]irtually any socially disfavored act can be criminalized at the discretion of the majority; the individual would then retain no control over whether or not information relevant to such an act would be revealed" (Adler 1996, 1111). Thus, even the most limited probing of our minds for knowledge of illegal activity might be unjustifiably damaging to our mental privacy, and perhaps to others' sense of privacy – even if it reveals only illegal activity. A brain imaging test that reveals only knowledge of who committed a minor act of vandalism, for example, might do more damage to such a sense of privacy than any benefit it brought in terms of crime control. Still, as I will soon argue, where an EEG, fMRI, or other brain imaging test is very limited in what it reveals, this may not make law enforcement use of the technique a non-search, but it will affect the analysis the Court does to determine if such a search is reasonable.

Fourth Amendment Protection – and the Importance of Balancing

The philosopher Robert Nozick opens his book, *Anarchy, State and Utopia*, with the following characterization of how to think about rights: "Individuals have rights, and there are things no person or group may do to them without violating their rights" (Nozick 1974, xix). American constitutional rights aren't quite so absolute. They apply only against the government, not against private parties. And even the staunchest constitutional protection has exceptions. For example, even though the First Amendment generally protects individuals against ideological censorship, it will permit the government to engage in such censorship on the rare occasion that it has a "compelling interest" in doing so. Still, many constitutional rights are at least approximations of Nozick's ideal. The First Amendment right to freedom of speech and Fifth Amendment privilege against self-incrimination, for example, block government action: When they cover a certain government method, they prevent it (or, the case of the First Amendment, do so most of the time).

By contrast, the Fourth Amendment right against unreasonable search and seizure is somewhat different. While it firmly prohibits unreasonable

search and seizure, the uncertainty about what counts as "unreasonable" in specific circumstances makes its protection give way more easily. Indeed, rather than completely shield a particular private realm of human action (such as speech), it is often described by the Court as balancing the individual's interest in privacy against the state's interest in conducting an investigation. "The essential purpose of the proscriptions in the Fourth Amendment," it has said, is to "impose a standard of 'reasonableness' upon the exercise of discretion by government officials," and "the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests" (Delaware v. Prouse 1979, 654). In the default case, as noted earlier, the warrant requirement constrains how this balancing takes place: Even when law enforcement has very strong interests in searching a home, this typically does not justify police entering on their own discretion. They rather have to make the case to a neutral magistrate that there are "legitimate government interests" in searching the place they have particularly specified, and that they have probable cause to search. Government must, in other words, meet some "objective standard" of reasonableness – such as probable cause or some other level of individualized suspicion – rather than simply argue that its interests outweigh that of the individual (Delaware v. Prouse 1979, 654).

But in many cases, the Court has identified exceptions to the warrant requirement. Sometimes this is because it is impractical to insist on a warrant, or on a showing of probable cause. This is true, for example, where an officer might have to enter a house (or other private area) immediately in "hot pursuit" of a felon, or to deal with exigent circumstances threatening someone's safety, or possibly the destruction of evidence. Those threats – to safety and integrity of evidence – might also arise when police arrest a suspect, who could be carrying arms and has strong incentive to destroy evidence before it can be used against him. In other cases, it is impractical to expect police to know, beforehand, where to find the dangers they are looking for – so it is not only a warrant, but even individualized suspicion, that is impractical. At an airport, for example, the danger feared is extraordinary and is very difficult to pinpoint ahead of time. The same is true, the Court has said, when police try to find drunk drivers or schools try to find students using drugs during school activities. Moreover, a warrant is not only impractical in such environments, it is less necessary because the expectations of privacy people have in the heavily

regulated confines of airports or schools, for example, are much lower – and the regulation they face is not first and foremost designed to thwart and prosecute crime, but to advance a "special need" different from ordinary crime control (like assuring school – or transportation – safety).

With the warrant requirement out of the picture, the Court is often thrown back in these cases on fundamental Fourth Amendment purposes – which, on the view it has often taken, require it to carefully weigh the investigation method's "intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."

Fourth Amendment Protection – Warrantless Searches, and Problems with Balancing

Use of such a balancing approach, however, is problematic for administrative and special-needs searches, and many other types of warrantless searches. In the first place, under a balancing regime, when security or safety concerns become powerful enough, as they are in the wake of terrorism attacks, Fourth Amendment interests in privacy or autonomy become more and more likely to find themselves in an unwinnable contest. Not surprisingly, when balancing has been applied in the context of special-needs and administrative search cases, for example, the government almost always wins. Moreover, the balancing has also frequently favored police when they conduct a search incident to arrest and, for example, administer a breathalyzer to obtain evidence of drunk driving. Recall Kerr's explanation of how the Fourth Amendment divides law enforcement investigation into "less invasive steps" free of constitutional oversight, and "more invasive steps," that count as "searches" and are subject to warrant requirements or other constitutional limits. We might say that special needs and administrative searches represent a kind of hybrid of the two sides of this division: They are searches, because they implicate realms of privacy covered by the Fourth Amendment, but – thanks to the dangers government needs to combat, the lowered privacy interests at stake, or both – officials often get a level of investigative leeway approaching that which they have when they conduct less invasive steps outside of the Fourth Amendment's coverage.

It is this thumb on the scales in favor of warrantless government searching that has caused some scholars thinking ahead – to Fourth Amendment applications to neuroimaging – to fret, especially since

many of the searches the Supreme Court and other courts permit under such balancing regimes involve searches into the body. For example, in Skinner v. Railway Labor Executives Association (1989), the Court respectively allowed government to administer random drug tests – through blood tests, breathalyzer tests, and urine tests – in the railway industry. In Vernonia School District v. Acton (1995) and Board of Ed. of Independent School Dist. No. 92 of Pottawatomie Cty. v. Earls (2002), it permitted random drug tests of public school students – tests that required collection of urine samples. In airports, as I have said, courts have permitted use of magnetometers, and more recently, powerful millimeter scanning of individuals' persons, to assure passenger safety.

If, as noted earlier, the clearest basis for the Fourth Amendment to cover neuroimaging is that it is, like a search into urine or breath, and intrusion into our bodies, or that it is like an X-ray, then – the template of the warrantless search cases above indicates we might be subjected to compelled neuroimaging in a number of circumstances where police wouldn't need a warrant use this technology. It is worth looking more closely at two of these circumstances: (1) special-needs and administrative searches, and (2) searches incident to arrest and other cases where exigency might justify a search that would otherwise require a warrant.

For example, to illustrate why neuroimaging might conceivably, like other searches of our bodies, be something police can do without a warrant, Pustilnik cites Schmerber v. California, where the Court found it was reasonable for police to compel the drawing of Schmerber's blood "incident to [his] arrest." Given that "the percentage of alcohol in the blood begins to diminish shortly after drinking stops, as the body functions to eliminate it from the system," there may have been no time for the officer to obtain a warrant – and the blood draw was not unreasonably intrusive to Schmerber, or damaging of his dignity (Schmerber v. California 1966, 770–771). Lower courts have since often emphasized that the possibility of losing the evidence in that case presented "exigent circumstances." In wondering whether Fourth Amendment protections might be too weak to protect against warrantless neuroimaging without modification of the doctrine, Farahany takes note of Skinner v. Railway Labor Executive Association, and the warrantless blood, urine, and breath tests it permitted as part of a "special-needs" search (Farahany 2012b, Searching Secrets, 1263–1264). She also notes that, when it comes to concerns about bodily intrusion, the court's limits on law enforcement are "certainly not absolute" and the "Court has found such procedures to be reasonable searches so long as the test is routine and minimally physically

invasive" (Farahany 2012b, Searching Secrets, 1284). But neuroimaging tests, as she notes, generally "would not be physically invasive" (Farahany 2012b, Searching Secrets, 1288).

Both Pustilnik and Farahany are understandably concerned about the prospect that – in circumstances like these, where a warrant is not required, and the Court turns to balancing – neuroimaging will be treated in the same way as non-intrusive testing of one's body. Pustilnik, for example, worries about the possibility that courts might treat "thoughts" as equivalent to "fingernail clippings" or other "physical samples" (Pustilnik 2013, 131). In part, the problem stems from a story about Fourth Amendment coverage that relies entirely on brain activity taking place in the interior of the body (like blood flow, air intake, or formation of urine). As she points out, "[l]ooking at our brain emanations as physical samples apart from their informational content and apart from the extent to which mental privacy allows us to constitute our identities" provide us with only a deeply "impoverished" account of the privacy interests at stake (Pustilnik 2013, 131). We seem to be missing a key part of the story when we treat our brain activity as being private only in the same sense as our blood, breath, or urine are private. Farahany similarly argues that courts ignore a crucial privacy interest when they give brain activity Fourth Amendment protection only to the extent that it is (like other physiological processes) secluded within the body (Farahany 2012b, Searching Secrets, 1288–1289). The Fourth Amendment, she argues, should not protect brain activity simply because of the seclusion that characterizes it, but because of the secrecy of the thoughts and memories that could be compromised if government could freely observe such activity. These concerns echo those of scholars who have worried that existing Fourth Amendment law (including both third party doctrine and some warrantless search cases) provide government with too much access to external records of our thinking – and particularly those we leave in digital form (Solove 2007, 112).

What then is to be done if government wishes to conduct neuroimaging at airports or at entrances to a federal building? This example is not entirely fanciful. Government has already used behavioral profiling in airports to try to identify dangerous intentions (and not simply the dangerous items it looks for in electronic airport screening). Justin Florence and Robert Friedman describe the Department of Homeland Security efforts to use behavioral profiling (Florence & Friedman 2010, 425–430). Christopher Rogers writes of efforts to explore supplementing this with

biometric "Future Attribute Screening Technology (or FAST), which can remotely read a person's vital signs and then predict whether that person has the indicators of 'malintent,' the intention to commit a crime" (Rogers 2014, 339–340). Farahany also takes note of an Israeli company, WeCU, marketing a device that presents passengers with subliminal stimuli at airport check-in lines – in order to generate emotional responses because that "emotional response is highly predictive of a passenger's potential security threat" (Farahany 2012a, Incriminating Thoughts, 376). As others have suggested, it is not far-fetched to think government may use technology like this to engage in behavioral profiling by looking at brain activity (Federspiel 2008, 889, 890–91), (Holley 2009, 13), (Moreno 2009, 717–719). Neuroimaging could conceivably allow the government to gather additional information of the kind these profiling systems and technologies are meant to enable.

Fourth Amendment Protection – Two Possible Alternatives to the Status Quo

One possible response to such concerns is to accept the basic Fourth Amendment framework as it is – that is, one where courts balance the intrusion into privacy against the government interests advanced, but then insist that in doing so, courts must accurately assess the privacy intrusion that neuroimaging causes, looking not just at how physically intrusive it is, but also at how mentally intrusive it might be. Moreover, there are at least some hints in the Court's past Fourth Amendment cases that it would be responsive to such arguments. For example, the Court has emphasized that whereas urine analysis does not require the intrusion into the body that occurs in a blood test, it "can reveal a host of private medical facts about an employee" (Skinner 1989, 616). Similarly, it might acknowledge that no matter how minimal the physical intrusion is in neuroimaging (and possibly even less intrusive in neuroimaging of the future), analysis of recorded brain activity can reveal numerous facts about a person's thought. Moreover, in its search incident-to-arrest line of cases, the Court has recently been willing to change the rules to protect private information (in a cellphone). (I say more about this later) Perhaps it will similarly change rules for special-needs and other warrantless searches if and when those searches make use of neuroimaging technology.

However, it is worth considering two other possible responses to such concerns. First courts could hold that while many different investigative techniques may be fair game for authorities in these kinds of searches-incident-to-arrest, special-needs searches, and other warrantless searches, neuroimaging simply isn't. In other words, courts could adopt an across-the-board rule that any kind of search that may intrude into mental privacy requires at least a warrant and probable cause (if not more). And so, schools and workplaces, for example, simply may not use neurotechnology to examine people about whom they have no suspicion. The idea behind this approach is that when a search method is so intrusive that it threatens mental privacy, it needs at least the kind of protection provided by an individualized determination of whether a warrant is justified in a particular case.

In fact, this is precisely what the Court has done in some of its recent search incident to arrest cases. As a general matter, the Court has for decades allowed police to search individuals whom they arrest – immediately and without a warrant – for two reasons: (1) to check the arrestee for weapons to see if he presents a threat to the officer and (2) to prevent the arrestee from destroying evidence. When either of these were a possibility, an officer could search any item or area within the arrestee's control (Chimel v. Califronia, 1969). Moreover, the Court said in United States v. Robinson that officers could search the arrestee's own person even *without* showing that there was a danger to the officer's safety, or of destruction of evidence. In other words, it adopted a categorical rule that searching an arrestee's person without a warrant was permissible (United States v. Robinson, 1973). Thus, even where officers had no valid reason to worry that a cigarette package they had found in Robinson's coat pocket presented a safety risk or had to be opened to preserve evidence related to Robinson's alleged crime, they could warrantlessly open this package (as they did, discovering drugs hidden within it). In 2014, however, the Court modified the rule in Robinson: Instead of assuming that police could *always* search the person of an arrestee, the Court said that – confronted with the question of whether officers could search SmartPhones obtained from the person of an arrestee – judges should not simply apply Robinson's rule "mechanically" but should instead go back to Fourth Amendment first principles. They should determine – if a warrant is necessary by "assessing, on the one hand, the degree to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests"

(Riley v. California, 2014). In the case of a cell phone, the Court said, a warrantless search intruded too deeply into individual privacy interests. "Cell phones," said the Court, "place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in Robinson" (Riley v. California, 2014).

The Court applied the balancing test again to analyze two related search-incident-to-arrest questions in the 2016 case of Birchfield v. North Dakota: the question of whether police need a warrant to search a drunk driving arrestee (1) with a blood test and (2) with a breathalyzer test (Birchfield v. North Dakota 2016). Applying the same balancing test described in Riley v. California and numerous other cases, the Court reached a split decision: blood tests of arrestees require warrants, breathalyzer tests do not. The reason for the different outcomes largely lay in the privacy intrusion inherent in each test: A blood test requires breaking the skin and removing blood. It also potentially reveals any information a chemical test might reveal in the blood. A breathalyzer test uses air that would be released by the body in any case. Moreover, said the Court the breathalyzer test is designed to provide only information about alcohol content, and nothing else: authorities do not retain the breath sample in such a way that they could extract other information from it (Birchfield v. North Dakota 2016).

The result of such analyses is that certain kinds of tests police wish to conduct incident to an arrest – a search of a cellphone, for example, or a blood test, will now typically require a warrant. They are removed from the realm of permissible objects of a warrantless search unless some other exception applies (for example, because there is demonstrable exigent circumstance that requires access to a cell phone that would otherwise require a warrant). In other words, while searches of persons incident to arrest have been treated as akin to "less invasive" steps where police have considerable leeway to search vigorously (even without specific reasons for focusing on a particular item), searches of their cell phone data have now been moved back to the "more invasive" category – in part, because, when it comes to the intangible information in SmartPhones, there is less immediate threat to law enforcement interests from such information, and there is also a significantly stronger privacy interest at stake (Riley, 2014, 2485). Neuroimaging could likewise typically require a warrant or other showing of justification even in many cases where other kinds of police investigations can take place without one (such as in an airport)

for similar reasons: Because mental states are not, by themselves, dangerous in the way that explosives or other weapons are, and because there we have far greater privacy in our thoughts than in our luggage. (For the reasons noted in Chapter 2, the weight of this privacy interest may depend on the nature of the neuroimaging technique used and the specific inferences about thought it makes possible.)

Fourth Amendment Protection and First Amendment Procedures – A Third Alternative to the Status Quo

However, there is still another possible response – and I will argue that it is an advisable one, not instead of an approach that emphasizes the importance of mental privacy, but in addition to such an approach. In short, the Court's framework for permitting special needs and certain other warrantless searches will be better – and better-equipped to deal with technologies such as neuroimaging – if it moves away from unpredictable balancing of privacy and security interests to which it is hard to assign a definite weight (and thus, hard to balance in a principled way).

Such a shift would have benefits for Fourth Amendment law that go beyond its application to neuroimaging. Blanket searches in some respects resemble the kind of "general warrant" the Fourth Amendment was designed to forbid: The Fourth Amendment's text requires officials specify the place to be searched, and have probable cause to search it. It does not permit them to do what officers of the English crown used to do with general warrants, which is to explore numerous papers, places, or other possible sites of criminal evidence – even without any strong reason to focus on them. But in special-needs and administrative searches, this is precisely what the government does. Christopher Slobogin describes searches such as "special needs" and administrative searches as examples of what he calls "panvasive" searches, by which he means "modern government's efforts at keeping tabs on the citizenry [that] routinely and randomly reach across huge numbers of people, most of whom are innocent of any wrongdoing." And he notes there is a tension between the Court's permissive attitude toward such searches and the Fourth Amendment's widely known inconsistency with general searches. As Slobogin recognizes, this presents a problem – and requires some constitutional constraint that can make up for the absence of the warrant requirement, and of particularized suspicion (Slobogin 2014, 1722–1723).

The Court has hinted at such requirements. In the context of administrative searches, of regulated businesses, it has done more than hint. It has stressed the existence of what it calls "a constitutionally adequate substitute for a warrant." Rather than leaving the inspection and penalizing of regulated business subject "to the unchecked discretion of Government officers," there is a federal statute governing the industry which "establishes a predictable and guided federal regulatory presence" (Dewey v. Donovan, 1981, 604). In the context of special-needs searches, like random drug testing, it has been less clear. But, as I have argued in previous scholarship, (Blitz 2004, 1457–1478), the Court often emphasizes features of the blanket search that it argues, in some sense, make up for the absence of warrant.

For example, the Court typically takes note of whether the government's blanket search is characterized by certain features that effectively minimize the intrusion it makes into an individual's privacy and dignity. They often note, for example, that officials have little control over how a search of this kind will be conducted or what kind of information it will turn up: In drug tests, for example, there is a very specific protocol from which officials cannot easily deviate. Also, such tests will often reveal only the presence or absence of a certain drug in the blood, breath, or urine. And the tests' administration is confined to an environment that, as I have noted above, is heavily regulated. A train worker is tested for alcohol under such a regime not when at home or on vacation, but when she is operating trains – conducting a task where it is in the public interest to assure she is able to concentrate.

These hints suggest another possible response to the possibility that neuroimaging techniques might find their way into special needs, administrative or other warrantless searches. The key problem with balancing, as I noted earlier, is that where security interests are deemed to be very high, as they have been in cases where drug use threatens safety, or where violent attacks or accidents are possible in car or air travel, then it is likely they will be deemed by courts to justify even highly invasive searches – regardless of whether the government could do better in protecting privacy. As a consequence, even where the government can do without neuroimaging, courts may let the government use it anyway if it determines that the balance of interests is heavily in the government's favor (as it typically is in special-needs cases).

An alternative regime modeled on First Amendment law, however, would not give the government such an option. Free speech rights, as I noted, are

closer in nature to Robert Nozick's barrier against government interference that Fourth Amendment rights typically are. And the specific material that barrier is made of – in First Amendment and other constitutional contexts – is "heightened scrutiny" on the part of the judiciary towards any kind of government action that threatens the right in question (Sorrell v. IMS Health, 2011, 2664). More specifically, in order to justify a speech restriction, government has to show (1) it has a very important goal – one which can justify a measure as worrisome and unusual as placing limits on speech – and (2) that something as foreign to a free society as speech restriction is, in this case, necessary to achieve that goal, but that they are taking measures to restrict speech as little as possible (or at least, not significantly more than necessary) to further their goal. Sometimes, this form of heightened scrutiny takes on a form ("strict scrutiny") which is almost impossible for the government to satisfy: When the government wishes to suppress speech on the basis of the message it carries, for example, the Court will almost reject such ideological censorship – allowing it only when the government has an extraordinarily important interest (or the kind a court refers to as a "compelling interest"), and can achieve that interest in no other way (United States v. Playboy Entertainment, 2000, 812–813, 816, 817). Even then, the court will require the government to use the "least [speech] restrictive" measure available to it – so that it avoids doing any more damage than necessary to First Amendment interests. In other First Amendment cases, the court lowers the bar a little bit and applies only "intermediate scrutiny." In these cases government has to cite only a "substantial interest" which need not be as rare or extraordinary as one it would need in other cases where strict scrutiny applies and its restriction, while it need not be a perfect fit with the government's ends, must avoid burdening "substantially more" speech than necessary to achieve these ends (Ward v. Rock Against Racism, 1989, 794–796, 799).

The Fourth Amendment typically does not operate like this: Police can obtain a warrant to investigate any crime. They do not need to show the judge that the particular crime they are investigating is a particularly grave one that gives them a compelling or significant interest in obtaining a warrant. Nor do they need to show, in each case, that they will minimize the intrusion. To be sure, they do have to specify a particular place they will search – so that they will not, as under a general warrant, have access to all of a person's papers, possessions, or private space. But in many cases when a warrantless search is permissible, even this limit is gone, or substantially weakened.

However, when extraordinary privacy interests are at stake in such a balancing situation, the better response is for a court to shift from vague

balancing to a more constrained inquiry that requires government not merely to show that its interest are strong, but also that it is minimizing the harm done to the interests at stake. This is especially appropriate when the interests are not only Fourth Amendment interests, but simultaneously First Amendment interests. Courts should not be indifferent to situations where government does those interests substantially more damage than is necessary to achieve its objectives. Indeed, as noted above, courts have already occasionally emphasized minimization where they see it in a special needs case: They have noted, for example, that drug tests leave little room for government discretion (Vernonia School District v. Acton 1995, 658, National Treasury Employees Union v. Von Raab 1989, 667) and – harkening back to the decisions in Place and Jacobsen on dog sniffs and chemical drug tests – reveal nothing more than the presence of illegal drugs in a person's body (Skinner 1989, 672 n.2).

More specifically, government effectively should have to meet intermediate scrutiny in order to assure that is not doing unnecessary and excessive damage to Fourth and First Amendment interests. Under this regime, government should have to show, for example, that the problems it is addressing with neuroimaging justify such strong law enforcement medicine. The need to detect and thwart terrorism or other violent crime might qualify as such an interest. So too might the need to detect financial crime (such as identity theft) that causes tremendous disruption to society and is difficult to detect with normal law enforcement means. But even so, government should not be permitted to use such methods in special-needs searches where there are other methods of available that are less threatening to individuals' privacy and freedom of thought.

Consequently, even where it can show that neuroimaging is necessary in a special-needs search, for example, it should also have to show that it has built into its general search regime privacy protections that help assure that the invasion created by the search is not far greater than necessary. Solove recommends that such heightened scrutiny be applied to government attempts to obtain and gain external records of our thoughts – in diaries or Web searches, for example (Solove 2007, 151–176). There is an equally strong case for applying it to government access to our unexpressed thoughts. For example, courts should insist if government needs access to mental states, that (where possible) it employ technology that probes only those aspects of a person's thinking it needs knowledge of to serve the significant government interest in question. A variant of this approach to modifying search and seizure doctrine might also be applied when information is collected through use of grand jury

subpoenas rather than in a police search. Pardo and Pustilnik have noted that Fourth Amendment protections are considerably weakened in cases involving such subpoenas. In Dionisio v. United States, a case discussed by Pardo (Pardo, 327, 2006), the Supreme Court observed that the Fourth Amendment provided protection against a "grand jury subpoena duces tecum" – that is a subpoena to produce certain tangible items – "too sweeping in its terms 'to be regarded as reasonable.'" But it went on to find that the defendant did not have the kind of privacy interest that would justify raising a Fourth Amendment shield to prevent subpoena of the voice exemplar demanded of Dionisio (which law enforcement wished to compare with recordings in evidence): The "physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public," said the Court, and therefore unprotected (Dionisio, 1973, 11, 14). Pustilnik likewise discusses cases where non-intrusive gathering of information about biological activity was permitted in a grand jury investigation (Pustilnik, 2013, 132–134). As in warrantless searches, one could argue that a framework for assessing the permissibility of such a subpoena should accord sufficient weight to the full privacy interests at stake in neuroimaging (and not just their physical invasiveness).

Fourth Amendment Protection – Beyond the Warrant Requirement

Having argued that this kind of First Amendment regime should replace the balancing the Court does in some situations where warrantless searches are normally permissible (especially when they are blanket searches), I also argue that such a First Amendment heightened scrutiny structure should, in some cases, be layered over the warrant requirement – even where that requirement does apply – and that there is a particularly compelling case for doing so when the government's search technique involves neuroimaging.

If imaging of someone is a "search," then – unless one of the recognized exceptions apply – police will only be able to use such a technique to gather information from an individual if they first obtain a warrant based upon probable cause. But is that sufficient protection for compelled brain imaging, even in its current limited form? Would it be sufficient protection for brain imaging of the future, that might occur without the subject realizing it is occurring, and may, perhaps, be able to the gather more

detailed information about the person's psychological characteristics or about mental events? The warrant and probable cause requirements certainly provide a safeguard against arbitrary or groundless searches of a person. They require police officials to build a case – before using a certain kind of investigatory method – that shows that that there is a "fair probability" that they will find evidence of criminal activity in the place to be searched.

But one might argue that when police wish to search in certain places, or with certain very intrusive techniques, even more should be required. Michael Pardo and Dennis Patterson note that the Court has imposed "probable cause plus" requirements for a warrant, but that these apply under current Fourth Amendment law only when "a search or seizure poses physical risk to a defendant," not on the basis of the privacy of the information sought (Pardo and Patterson, 213, 154, n. 37).

There is, however, another circumstance in which courts (especially lower courts) demand more of police than a warrant: when police engage in wiretapping or in video-surveillance of the inside of a home or other private space. In New York v Berger, the 1967 case in which the Court first extended the Fourth Amendment to cover wiretapping, the Court insisted that police seeking a warrant need to specify more than "probable cause" and "the place to be searched." Because electronic eavesdropping "involve[s] a privacy violation that is broad in scope," said the Court, it imposes "a heavier responsibility" on a court "in its supervision of the fairness of procedures." Apart from simply describing a target in describing the place to be searched, police had to – in meeting this particularity requirement – describe the "type of conversation sought with particularity, thus indicating the specific objective of the Government." They also had to limit their intrusion to "one limited intrusion, rather than a series or a continuous surveillance." Such safeguards, said the Court, insured that the "danger of an unlawful search and seizure was minimized" (Berger 1967, 57–58).

In the wake of Berger, Congress used the Court's discussion in that case as a template for imposing specific statutory requirements on federal wiretapping. Apart from requiring a judge to assure that (1) that the warrant must contain "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," Congress also imposed other requirements, including that (2) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," (3) that the time during which the surveillance of a conversation is to take place is not

longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days" and (4) that a wiretap interception of a telephone conversation "be conducted in such a way as to minimize the interception of communications" that are not related to criminal activity subject to investigation (18 U.S.C. Sections 2518(3)-(5)).

These requirements were imposed by Congress, in its wiretap act, not by the Constitution in the Fourth Amendment. But beginning in 1984, a number of federal courts imported these requirements into Fourth Amendment law when the government sought to use surreptitious video-surveillance in a private environment. In United States v. Torres, the Seventh Circuit Court of Appeals found it "unarguable that television surveillance is exceedingly intrusive, especially in combination with audio surveillance, and inherently indiscriminate, and that it could be grossly abused – to eliminate personal privacy as understood in modern Western nations." It thus imposed the same requirements on television surveillance that Congress had imposed on wiretapping in above-cited statutory provisions, finding in the constitutional context, and with respect to such an intrusive surveillance method, they were necessary to "implement the constitutional requirement of particularity" (Torres 1984, 884). Since then, a series of federal courts across the United States applied the same or similar requirements in other video surveillance cases.

Should courts impose similar requirements on technology that is used to gather physiological data from the brain rather than from wiretaps or video surveillance? Susan Freiwald argues the justification for such "heightened procedural hurdles" beyond the ordinary warrant requirement depends on the four features of surreptitious video surveillance and wiretapping: that it is (1) "hidden," (2) "intrusive," (3) "indiscriminate," and (4) "continuous." Hidden surveillance justifies a higher hurdle because "the target is less able to hold government investigators accountable, and therefore needs the court to protect his interests." Intrusive methods do so because they "bring law enforcement further into our private lives, and therefore require judicial intervention to ensure that government makes such intrusions only after satisfying a high level of need." Surveillance is indiscriminate when it "obtains information beyond that which is justified, and thus requires court oversight to ensure unjustified surveillance is minimized." And "continuous surveillance is more likely to be intrusive and indiscriminate because it acquires more information over a longer period of time" (Friewald 2007, 10–11).

The feature of this quartet of characteristics that has been more heavily emphasized by courts applying the Fourth Amendment, and also by many other scholars, is the indiscriminate nature of some searches. This worry about indiscriminate searches flows naturally from the particularity requirement in the Fourth Amendment. In order to obtain a warrant, as I have said, police need to do more than simply show that they have probable cause to believe that their investigation of certain activity will produce evidence of a crime. The Constitution's text itself makes it clear that they must also "particularly describ[e] the place to be searched, and the person of thing to be seized." This "particularity" requirement is intended to forbid – in US enforcement of the law – that practice of using "general warrants," which, as the US Supreme Court said, "allowed royal officials" in eighteenth-century England and the English colonies, "to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown" (Stanford v. Texas 1965, 472).

Armed with a general warrant, officials could enter any house or other private space they have a hunch might aid their investigation, and then search whatever they wished to in a person's home. They could, in other words, engage in what the Supreme Court described as "general, exploratory rummaging in a person's belongings" (Coolidge v. New Hampshire 1971, 443). The particularity requirement shields individuals in a free society from this kind of unconstrained invasion into their personal spaces and possessions: It not only forces police to justify their search of such spaces or possession to a magistrate – and obtain a warrant from that magistrate. It also requires that the warrant itself be limited in scope, so that the search focuses only on that part of a person's space or possession that police reasonably believe is likely to contain evidence of a particular crime.

Yet courts and scholars have argued that some emerging technologies make it hard to prevent "general exploratory rummaging" of people's information. This was, in large part, why courts have insisted on minimization requirements for wiretapping and video surveillance: Such electronic surveillance will likely capture not only conversation, or images, concerning criminal activities, but all other words that are exchanged in a phone call or in front of a hidden video camera.

Thus, David Gray and Danielle Citron argue that the Fourth Amendment should apply not only to protect us in traditionally private areas, but also against technologies that subject us to "broad programs of indiscriminate

surveillance" (Gray and Citron 2013, 73). In recent years, some magistrate judges have also imposed specific limitations on computer searches on the grounds that such searches will otherwise give government access to numerous files that have little to do with the crime it is targeting. In United States v. Comprehensive Drug Testing, for example – a case in which federal agents searched computer files for information about specific major league baseball players' steroid use – the magistrate issued a warrant for a search of computer files, but imposed "significant restrictions on how the seized data were to be handled. These procedures were designed to ensure that data beyond the scope of the warrant would not fall into the hands of the investigating agents" (United States v. Comprehensive Drug Testing 2010, 1166). As Orin Kerr writes, it has become increasingly common for magistrate judges to impose ex ante restrictions in computer searches (Kerr 2010, 1243, 1248–1271). As Paul Ohm explains, the logic of such ex ante restrictions is to prevent something akin to a general warrant from being issued under the guise of one that meets the particularity requirement: "Many government practices have been compared to general warrants, but almost none are close to being as invasive as a months-long trawl through a person's personal computer" (Ohm 2011, 10).

To the extent indiscriminate searches remain the primary candidate for additional constraints on the warrant requirement, it is unlikely that current neuroimaging techniques qualify. Where officials use a test that only reveals how individuals' brain activities respond to specific stimuli (or when making specific statements) related to a particular crime, they will not be as likely to come across entirely unrelated activity, as they will when they are listening in on a phone conversation, videotaping unanticipated activity in a living room, or browsing through hundreds or thousands of computer files stored on a computer they have seized. If, for example, the government asks a researcher trained in neuroimaging techniques to tell them whether or not a tested subject's brain responds to an image of a murder weapon, and does so in a way that past studies have correlated with showing familiarity with that weapon, agents will not easily be able to learn much else about the suspect's thoughts or mental states. Consequently, it is likely that a warrant is all that is required here.

Moreover, existing types of neuroimaging technology also are non-candidates for heightened procedures under two of Freiwald's other criteria. They are not hidden: If, in future years, development of infrared imaging or other technology allows a government to surreptitiously and

remotely gather data about brain activity from an unsuspecting individual, then this would of course significantly strengthen the case for demanding that the government should need more than a warrant – unless, perhaps, even such surreptitious probing is constrained to reveal nothing more than a link to knowledge of a crime under investigation. Similarly, if and when investigators can gather data through brain-computer interfaces by "camoufloug[ing]" the interrogation of a user, in the manner described by Martinovic and his colleagues, this too might be a technique that should be subject to heightened procedural requirement – for example, the requirement that it be used only when other means of obtaining the information needed by police have failed, leaving use of a brain-computer interface as a last resort (Martinovic et al. 2012). But the neuroimaging methods of the present do not raise this problem. Likewise, neuroimaging is not continuous, as is an hours-long wiretap recording or hidden video-surveillance recording. While it may take a long time to obtain the required images, this is sometimes because many fMRI scans are needed to gather reliable information about a particular brain response – not because those using the fMRI are gathering significant information about person's on-going daily routine (whether in her communications, or home activities, or choices about where to drive) over an extended period. If and when future versions of neuroimaging allow researchers to construct something more like a continuous video of a person's internal life from second to second, then this factor might weigh in favor of heightened requirements. The same might be true of surreptitious and portable methods of neurorecording that allow individuals to take multiple measurements of an individual's activity over a long period of time, as that individual performed normal routines (rather than specific tasks dictated by a supervising researcher or tester).

There is, however, one of Freiwald's factors that does weigh in favor of heightened requirements for obtaining a warrant and that is intrusiveness. As noted above, Freiwald suggests that high intrusiveness weighs in favor of additional safeguards because it "bring[s] the law enforcement further into our private lives, and therefore require[s] judicial intervention to ensure that government makes such intrusions only after satisfying a high level of need" (Freiwald 2007, 10). There is a strong case to be made that even relatively brief and fragmentary glimpses of how the brain behaves as it generates our thoughts entail a level of intrusiveness than justify strong safeguards – and requir[ing]

that government first show that it has "a high level of need" before it can observe such brain activity. As I noted in the introduction, our thoughts and feelings have long seemed to made entirely secure against external observation by the natural order of things. One might argue that this should remain the case – even in a world where neuroimaging can reveal solid clues as to unexpressed thoughts – unless police can demonstrate an extraordinary need for access to this realm of our experience.

And the fact that neuroimaging implicates not only Fourth Amendment – but also First Amendment concerns – provides another argument for treating even simple neuroimaging as deeply intrusive – and intrusive enough to impose additional requirement beyond a simple warrant requirement. If, as the Court has said, the First Amendment protects not only freedom of speech, but also "the freedom of thought" underlying that speech – then police intrusion into the realm of our thoughts is a threat to First Amendment interests.

Intellectual Property and Intellectual Privacy

There are alternative proposals for refashioning Fourth Amendment law to provide greater protection for the mental privacy that may be vulnerable in neuroimaging. One such proposal comes from Nita Farahany. She argues that the courts will better appreciate the privacy interests at stake in neuroimaging if they view at least some of our mental content as similar to intellectual property. "Authors," she argues, "can properly claim a 'secrecy interest' in 'their' writings and effects," and this will sometimes give them a right to prevent an examination of their work even when it is accessible (Farahany 2012b, Searching Secrets, 1243). Moreover, she argues, this authorship right should apply not only to what we write on paper or other media in the external world, but also to memories we refrain from writing about: "Two individuals looking across a courtyard, for example, will focus on different aspects of the scene before them. The memories they encode of that moment will be personally created expressions of their own experiences" (Farahany 2012b, Searching Secrets, 1294). Such an authorship interest, where it exists, adds to the privacy interests in brain activity that derive solely from bodily seclusion. With authorship as an additional principle of Fourth Amendment protection – apart from the privacy we derive from concealing ourselves, our papers, or our effects – Farahany then tests, against this standard, each of the four categories in the spectrum of activity she proposed to replace the

testimonial-physical distinction in the Fifth Amendment context: identifying information, automatic processes, memorialized content, and utterances. Her conclusion is that an individual:

> has the strongest claim of authorship in uttered and memorialized evidence and the weakest claim of authorship in automatic or identifying evidence. Because memorialized and potentially recorded utterances are the proper subject of copyright protection, a court must balance the intrusion upon both the seclusion and the secrecy of the individual against the governmental interest in the evidence sought to decide if an unreasonable search or seizure has occurred. (Farahany 2012b, Searching Secrets, 1275)

As was true in her Fifth Amendment analysis of these categories, Farahany finds the Fourth Amendment analysis worrying and counterintuitive in some respects: "If real and intellectual property law are the only sources to which the Court will turn to inform reasonable expectations of privacy in the Fourth Amendment," she notes, then automatically-generated information (including) cognition, may be left without constitutional protection. In some circumstances, this is "the very information that individuals wish to keep the most private" (Farahany 2012b, Searching Secrets, 1308).

There is an answer to this problem and that is that the Supreme Court has not limited privacy interests to real and intellectual property. As noted earlier, even when blood or urine is removed from our body and is no longer our property, the Court recognizes that the "private medical facts" government can draw from it raises distinctive Fourth Amendment privacy concerns about blood and urine testing for drugs. This is not because individuals author such facts, or own them in any other sense. Moreover, we may have strong privacy interests in our thinking processes that are quite different from the intellectual property interests that authors have in their works: When we read someone else's work on an electronic reader or listen to someone else's song, for example, the copyright belongs not to us, but to the owner of the work. That owner is the one who has the right to control what happens to the work and when it can be accessible for others. But government spying on my reading or my choice of what music to listen to would nonetheless be an invasion of my intellectual privacy, even if it is not an invasion of my intellectual property (Cohen 1996, 983–989). One can argue that the memories I create when I read or listen to a work, and the way they are shaped by my distinctive understanding or hearing of it, makes

me an author at the very least of my own perceptions. But this move isn't necessary to ground the claim that privacy and freedom of thought should cover those perceptions – which has power not because I author them, but because they are mine (and, by default, generally inaccessible to the rest of the world), whether they consist of identifying, automatic, memorialized, or uttered content. That a piece of intangible information is my intellectual property, or akin to such intellectual property, is something that can certainly weigh in favor of finding that I have a reasonable expectation of privacy in that information. But it is not a necessary condition for such privacy to exist and provide a basis for Fourth Amendment protection.

In fact, among the kind of mental content that many individuals intuitively find to be the most private is mental content that defines features of their personality, even where it consists of "identifying" information. As noted earlier, some neuroimaging could conceivably probe a person's "connectome" (Seung 2012, 4–5) to try to "brainotype" that person (along the same lines probing of genome might aid an observer in genotyping her) (Farah et al. 2010, 126). Such mental-process information seems to be identifying, but it is still deeply private and should, like other mental-content information, receive robust protection against searches unless government can justify its need for access to it. What Farahany says is true of utterances – "when balancing government interests against the fortress of seclusion around the brain, only extraordinary circumstances should justify an intrusion" – should be true in other circumstances that freedom of thought is at stake in the Fourth Amendment context. And, as I have argued, First Amendment heightened scrutiny provides a ready-made model for how to secure such a "fortress" (Farahany 2012b, Searching Secrets, 1308).