American University Law Review

Volume 64 | Issue 2 Article 5

2014

A Slow March towards Thought Crime: How the Department of Homeland Security's Fast Program Violates the Fourth Amendment

Christopher A. Rogers
American University Washington College of Law

A Slow March towards Thought Crime: How the Department of Homeland Security's Fast Program Violates the Fourth Amendment

Keywords
Administrative searches & seizures; United States. Constitution. 4th Amendment; United States. Dept. of Homeland Security; Telepathy -- Government policy; Criminal intent -- Research; Criminal behavior, Prediction of -- Research; Right of privacy -- United States; Counterterrorism -- Government policy -- United States

A SLOW MARCH TOWARDS THOUGHT CRIME: HOW THE DEPARTMENT OF HOMELAND SECURITY'S FAST PROGRAM VIOLATES THE FOURTH AMENDMENT

CHRISTOPHER A. ROGERS*

The United States Government is currently developing a system that can read minds—a situation that George Orwell envisioned when he wrote Nineteen Eighty-Four. *The Future Attribute Screening Technology ("FAST"), currently being tested by the U.S. Department of Homeland Security (DHS), employs a variety of sensor suites to scan a person's vital signs, and based on those readings, to determine whether the scanned person has "malintent"—the intent to commit a crime.*

FAST is currently designed for deployment at airports, where heightened security threats justify warrantless searches under the administrative search exception to the Fourth Amendment. FAST scans, however, exceed the scope of the administrative search exception. Under this exception, the courts would employ a balancing test, weighing the governmental need for the search versus the invasion of personal privacy of the search, to determine whether FAST scans violate the Fourth Amendment. Although the government has an acute interest in protecting the nation's air transportation system against terrorism, FAST is not narrowly tailored to that interest because it cannot detect the presence or absence of weapons but instead detects merely a person's frame of mind. Further, the system is capable of detecting an enormous amount of the

---

* Associate Managing Editor, *American University Law Review*, Volume 64; J.D. Candidate, May 2015, *American University Washington College of Law*; B.A. History, February 2010, *Middlebury College*. I am sincerely grateful to the editors and staff of the *American University Law Review* for their work in making this Comment possible and to Professor Cynthia Jones who set me down the right track. I would also like to thank my friends and family—especially Elizabeth Rogers—whose constant support and encouragement made this process that much easier. All errors and mistakes are the author's own.

scannee's highly sensitive personal medical information, ranging from detection of arrhythmias and cardiovascular disease, to asthma and respiratory failures, physiological abnormalities, psychiatric conditions, or even a woman's stage in her ovulation cycle. This personal information warrants heightened protection under the Fourth Amendment. Rather than target all persons who fly on commercial airplanes, the Department of Homeland Security should limit the use of FAST to where it has credible intelligence that a terrorist act may occur and should place those people scanned on prior notice that they will be scanned using FAST.

Finally, if the Department of Homeland Security deploys FAST in a Minority Report*-like approach by using it to detect a person's intent to commit ordinary crimes—such as murder, theft, or drug smuggling—FAST does not fall under the administrative search requirement and must meet the Fourth Amendment's warrant requirement or another exception to the warrant requirement.*

TABLE OF CONTENTS

> It was terribly dangerous to let your thoughts wander when you were in any public place or within range of a telescreen. The smallest thing could give you away. A nervous tic, an unconscious look of anxiety, a habit of muttering to yourself—anything that carried with it the suggestion of abnormality, of having something to hide. . . . Your worst enemy, he reflected, was your nervous system. At any moment the tension inside you was liable to translate itself into some visible symptom.
>
> - George Orwell, *Nineteen Eighty-Four*[1]

INTRODUCTION

On April 15, 2013, three people died and hundreds were wounded when two homemade pressure cooker bombs exploded near the finish line of the Boston Marathon.[2] Employing images taken from security cameras, the Federal Bureau of Investigation identified two men as persons of interest and possible suspects because their images appeared near the blast zones moments before the bombs went off.[3] Prior to the explosions, no one suspected that Tamerlan and Dzhokhar Tsarnaev were about to detonate two improvised explosive devices in the crowded area around the finish line of the Boston Marathon.[4] However, over the next few years, the Department of Homeland Security (DHS) is hoping to deploy a system in America that would be able to detect the signs of agitation that precede such criminal acts—crime detection before the crime is even committed.[5] The system—Future Attribute Screening Technology ("FAST")—can remotely read a person's vital signs and then predict

---

1. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 71, 73 (Penguin Books 1987) (1949).

2. *Boston Marathon Terror Attack Fast Facts*, CNN, http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts (last updated Nov. 1, 2014, 5:06 PM).

3. *What We Know About the Boston Bombing and Its Aftermath*, CNN, http://edition.cnn.com/2013/04/18/us/boston-marathon-things-we-know (last updated Apr. 18, 2013, 9:54 AM).

4. *See* Jonathan Allen, *Factbox: Charges Filed Against Boston Marathon Bombing Suspect*, REUTERS (Apr. 22, 2013, 4:57 PM), http://www.reuters.com/article/2013/04/22/us-usa-explosions-boston-complaint-idUSBRE93L16C20130422 (showing that the Tsarnaev brothers were acting relatively normal prior to the blasts).

5. *See* Michael Solomon, *Uncle Sam's "Mal-intent": With Its FAST Program, the Federal Government Is Trying to Read Minds to Fight Terrorism*, IN THESE TIMES (Dec. 21, 2011), http://inthesetimes.com/article/12408/uncle_sams_mal_intent (positing that Future Attribute Screening Technology ("FAST") Mobile Modules "may one day roam the country" to predict if people will commit crimes).

whether that person has the indicators of "malintent," the intention to commit a crime.[6]

FAST implicates the Fourth Amendment's prohibition against unreasonable searches because it would allow the government to obtain vast quantities of sensitive medical data from the people scanned. This Comment argues that the Fourth Amendment prohibits DHS from using FAST scans to detect ordinary crimes without first securing a warrant based on probable cause. It further argues that the use of FAST—in its current form without limitation—to detect terrorism at airports and high-profile venues is an unreasonable administrative search in violation of the Fourth Amendment. These scans are not minimally intrusive because they can obtain highly sensitive medical data, and the scans are not narrowly tailored to detect weapons or explosives because they are designed to detect a frame of mind.

Part I of this Comment describes the FAST system and its functions. Part II discusses the applicable Fourth Amendment framework and the requirements for a reasonable administrative search, while Part III describes a person's privacy interest in medical data as implicated by FAST's conceivable ability to uncover medical, psychiatric, and other conditions through the scans. Part IV then demonstrates that a FAST scan is a Fourth Amendment search but that it meets the criteria to be analyzed under the administrative search exception to the warrant requirement. This Part further analyzes the reasonableness of FAST scans under administrative search jurisprudence and ultimately concludes that FAST scans are not reasonable under the administrative search exception to the Fourth Amendment and are therefore invalid. Specifically, FAST is too intrusive due to its potential to reveal sensitive medical data, and that its intrusiveness is not outweighed by the governmental interest in preventing terrorist acts because FAST scans are not narrowly tailored to further that governmental interest.

---

6. DEP'T OF HOMELAND SEC., FAST: FUTURE ATTRIBUTE SCREENING TECHNOLOGY 4 (2010) [hereinafter DHS FAST PRESENTATION], *available at* http://epic.org/privacy/fastpresentation.pdf (defining malintent as "[t]he mental state of individuals intending to cause harm to our citizens or our infrastructure").

I. BACKGROUND ON THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY

A. How FAST Works

The FAST system is grounded in research on human behavior and psychophysiology, relying on the theory that the body's autonomic nervous system reacts in certain ways and that, when those reactions are detected, the system can reveal a person's intentions.[7] The theory is based on an evolution of the polygraph: scientists have long known that changes in heart rate, blood pressure, and galvanic skin response are indicators that a person is lying.[8] Although a skilled liar can train herself to "appear honest," certain bodily functions, such as blinking, are controlled by the autonomic nervous system and cannot be consciously controlled.[9] FAST is designed to remotely detect these indices and determine whether a person has malintent.[10] While the public often believes that this type of technology is a figment of science fiction as in the movie *Minority Report*[11] or George Orwell's novel *Nineteen Eighty-Four*, the underlying theory is already employed in the legal world.[12] Behavioral detection is commonly used in the courtrooms because juries subconsciously judge the veracity of a witness's statements according to the witness's demeanor on the

---

7. Steven Cherry & Anne-Marie Corley, *Bad Vibes: A Quixotic U.S. Government Security System Seeks to Look into Your Soul*, IEEE SPECTRUM, Jan. 2010, at 60, 61; *see also* Marcus Holmes, *National Security Behavioral Detection: A Typography of Strategies, Costs, and Benefits*, 4 J. TRANSP. SECURITY 361, 364–67 (2011) (claiming that even though people can train themselves to look as if they are not lying, certain overt body functions cannot be controlled and can indicate emotional arousal).

8. Carol Eisenberg, *Homeland Security Exploring Mass-Scanning System*, MCCLATCHY-TRIB. BUS. NEWS, Aug. 15, 2007; *see* Holmes, *supra* note 7, at 366 (asserting that traditional polygraphs measure the variation in responses to answers based on blood pressure, respiration, heart rate, and skin conductivity measurements). Lie detector results "are not admissible in a court of law because of questions about their accuracy." Eisenberg, *supra*.

9. Holmes, *supra* note 7, at 365.

10. *See infra* text accompanying notes 117–26 (explaining how FAST is designed to remotely monitor individuals' physiological data).

11. MINORITY REPORT (Twentieth Century Fox 2002).

12. Holmes, *supra* note 7, at 371 ("Legal studies scholars have investigated the effect of non-verbal cues as the testimony of witnesses and judges over the past few decades and have determined that the mere appearance of a witness, defendant, or attorney can have a salient effect on judicial outcomes."). Casinos have used infrared cameras to detect cheaters for years because cheating causes a person's body temperature to rise. Cath Everett, *Biometrics-Based Surveillance: Big Brother or Vital Safeguard?*, COMPUTER FRAUD & SECURITY, Nov. 2009, at 5, 6.

stand; accordingly, experts often coach witnesses on how to act and dress on the stand to increase their believability.[13] Additionally, DHS has a long-standing behavioral detection program, currently used in airports, where trained agents visually identify cues of malintent.[14]

Although biometric devices are usually considered only in science fiction, the government is already employing "biometric devices that can strip a person bare on a cellular level," which can be more intrusive than a public strip search.[15] As history has shown, what was once science fiction can readily become reality, and constitutional scholars believe that soon the "nascent" technologies currently deployed by the government will be integrated "into a complex, interwoven cyber network aimed at tracking our movements, predicting our thoughts, and controlling our behavior."[16]

The National Academy of Sciences disagrees with the polygraph theory that underlies the FAST theory, noting that its own meta-analysis of polygraph research demonstrates that polygraphs are

---

13. Holmes, *supra* note 7, at 371 ("If, as these studies suggest, juries do rely on nonverbal behavior more than verbal content in making judgments, the accuracy of their interpretations of such nonverbal behavior might be crucial to the outcome of the case. . . . The jury's ability to interpret will often be tested when the jury trie[s] to determine whether a witness, client, or attorney is deceiving [it].").

14. *See generally* Justin Florence & Robert Friedman, *Profiles in Terror: A Legal Framework for the Behavioral Profiling Paradigm*, 17 GEO. MASON L. REV. 423, 425–30 (2010) (describing DHS's use of a behavioral profiling program that focuses on analyzing subtle human expressions and behavior as a security measure); *infra* notes 51–53 and accompanying text.

15. John W. Whitehead, *Upending Human Dignity and Shattering the Fourth Amendment: Strip Searches*, HUM. RTS. MAG., May 2013, *available at* http://www.americanbar.org/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/upending_human_dignity_fourth_amendment.html.

16. *Id.* Businesses use eye trackers, a type of biometric screening, to track where people look and to increase the effectiveness of advertisements. *What Is Eye Tracking?*, TOBII, http://www.tobii.com/en/about/what-is-eye-tracking (last visited Dec. 21, 2014). However, data-gathering is not limited to the business realm, as seen by the recent controversy with the National Security Agency, and although DHS needs to work out many "kinks" with FAST, the federal government is using advanced analytic technologies to detect and prevent crime. Yaniv Mor, *Big Data and Law Enforcement: Was "Minority Report" Right?*, WIRED (Mar. 5, 2014, 12:25 PM), http://www.wired.com/2014/03/big-data-law-enforcement-minority-report-right; *see also* Dave Lee, *New Adverts "Could Track Your Eyes" in Supermarkets*, BBC, http://www.bbc.com/news/technology-22351995 (last updated Apr. 30, 2013, 12:13 PM) (reporting that researchers at Lancaster University have created an eye tracking device that can easily detect separate users and that eye tracking technology will soon become "widely available"). "As technologies evolve, so too will the processes . . . used to capture bad guys." Mor, *supra*.

"[u]nreliable, [u]nscientific and [b]iased."[17] Polygraph critics note that there is not a clear link between deception and physiological responses.[18] Specifically, polygraphs measure indices that can vary by the minute for non-deceptive reasons, and some studies have shown that stress can have an inordinate amount of influence on these factors.[19] Polygraphs are also highly susceptible to countermeasures, such as when people control their breathing during hard questions and breathe hard during control questions.[20]

Compared to polygraphs, FAST measures similar indices and detects the variations between responses, which DHS's theory suggests will illuminate deception.[21] Proponents of FAST note that it is designed to correct the problems that plague polygraphs by focusing on signs of malintent rather than on signs of deception.[22] They argue that comparing FAST to polygraphs is immature and that FAST's accuracy rates "are almost certainly higher than actual polygraph accuracy."[23] Specifically, proponents argue that FAST "focuses on many more measures of the autonomic nervous system, and it has already had success in being able to detect different emotional states," thus increasing the likelihood that it is more accurate than a polygraph.[24] By focusing on more measures,

---

17. Holmes, *supra* note 7, at 366 (stating the National Academy of Sciences has concluded that many studies that had validated the use of polygraphs were flawed and that "the levels of accuracy in the studies are almost certainly higher than actual polygraph accuracy of specific-incident testing in the field" (internal quotation marks omitted)). Many conscious and unconscious biological and psychological factors can affect polygraph results. COMM. TO REVIEW THE SCIENTIFIC EVIDENCE ON THE POLYGRAPH, NAT'L ACAD. OF SCIS., THE POLYGRAPH AND LIE DETECTION 212–13 (2003). The National Academy of the Sciences concluded further that "the scientific base for detecting deception remains weak" but that it is "the best way for government agencies to assess techniques that are presented as useful for detecting and deterring criminals and national security threats." *Id.* at 221.

18. Florence & Friedman, *supra* note 14, at 428–29.

19. *See* Holmes, *supra* note 7, at 366 (asserting that blood pressure varies from minute to minute for reasons that have nothing to do with deception).

20. *Id.*

21. *Id.* ("[D]eceptive answers should produce different physiological responses than non-deceptive answers."). Additional studies have also tested the theory using thermal screening and pattern detection rather than the traditional measurements of blood pressure, heart rate, respiration rate, and skin conductivity. *Id.*

22. *See id.* at 366–67 (postulating that the FAST program focuses on signs of harmful intent and that malintent shows through "abnormal behavior or extreme physiological reactions" (internal quotation marks omitted)); *supra* note 6 and accompanying text (defining malintent as intent to commit a crime).

23. Holmes, *supra* note 7, at 366–67 (internal quotation marks omitted).

24. *Id.* at 367 (internal quotation marks omitted).

proponents argue that FAST is able to detect the subtle difference between someone who is simply stressed for innocent reasons, such as missing a flight, versus someone with malintent.[25]

According to DHS, FAST uses non-intrusive sensors to detect physiological and behavioral cues, and the system aggregates the data under the Theory of Malintent to discover the mental state of a person and whether that person intends to cause harm.[26] The current manifestation of the system uses five sensor packages to obtain various readings from screened individuals, including sensors to measure the cardiovascular and respiratory systems, a remote eye tracker, thermal cameras, high-resolution cameras to track body movements, and audio capture devices.[27] Currently, DHS is considering other sensor packages, including pheromone level detectors.[28]

The current system is similar to the baseline-questioning approach used in polygraph examinations.[29] People are individually scanned while they wait in line or walk down a corridor to establish their own

---

25. *Id.*

26. SCI. & TECH. DIRECTORATE, DEP'T OF HOMELAND SEC., PART I: TECHNICAL DIVISIONAL REQUIREMENTS 12 (2010), *available at* http://epic.org/privacy/fasttechreqs.pdf (explaining that FAST will use "[m]ethods for non-invasively identifying deceptive and suspicious behavior"); SCI. & TECH. DIRECTORATE, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 2 (2008) [hereinafter DHS PRIVACY IMPACT ASSESSMENT], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf (describing the Theory of Malintent).

27. DHS PRIVACY IMPACT ASSESSMENT, *supra* note 26, at 4 (adding that DHS is considering using pheromone detection technology in FAST as well); SCI. & TECH. DIRECTORATE, DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST)/PASSIVE METHODS FOR PRECISION BEHAVIORAL SCREENING 5 (2011) [hereinafter DHS PRIVACY IMPACT ASSESSMENT UPDATE], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast-a.pdf. The cardiovascular and respiratory sensors can determine heart rate and calculate its variability as well as measure respiration rate and respiratory sinus arrhythmia. DHS PRIVACY IMPACT ASSESSMENT, *supra* note 26, at 4. The remote eye tracker tracks the gaze of an individual's eyes and measures his or her pupil diameter. *Id.* The thermal cameras measure changes in skin temperature and can assess electrodermal activity. *Id.* High-resolution video cameras take images of the face and body to analyze facial features and expressions and body movements. *Id.* FAST also uses an audio system to determine voice pitch changes. *Id.*

28. DHS PRIVACY IMPACT ASSESSMENT, *supra* note 26, at 4; *see* Calvin Biesecker, *DHS S&T Begins Testing System that Screens People for Hostile Intent*, DEF. DAILY, Sept. 19, 2008 (indicating that researchers at the University of Pennsylvania have linked different odors to different emotional states).

29. Cherry & Corley, *supra* note 7, at 61; *see also* DHS FAST PRESENTATION, *supra* note 6, at 15.

baseline.[30] Once a person's baseline is established, security officers will ask the person questions while the system analyzes changes in the person's autonomic nervous system to determine if that person has malintent.[31] Although the current system uses stimuli in the form of an officer questioning an individual, DHS plans to perfect the system to detect malintent without needing operator-induced stimulation.[32] DHS notes that this change would allow FAST to detect malintent from greater distances and in places where a person would not expect to be subject to security screening.[33]

FAST is still in the developmental phase, and DHS has released only a few results from laboratory and field tests.[34] The system has an eighty-one percent classification accuracy in a laboratory test setting, where contact sensors are used instead of remote sensors to validate the theory.[35] DHS later conducted controlled tests at undisclosed locations, recruiting volunteers from the food industry to work at a special event that required screening to protect important guests.[36] In the first "Draper" test, DHS assigned the volunteers a "malintent" or "no malintent" condition and asked them to smuggle a prohibited item into the venue.[37] Although this field test did not involve any

---

30. *See* Cherry & Corley, *supra* note 7, at 61 (revealing that individuals might be scanned while they wait in line at the airport); *see also* DHS FAST PRESENTATION, *supra* note 6, at 8 (describing that study participants present their identification to a guard before entering the screening and being questioned).

31. Cherry & Corley, *supra* note 7, at 61 (explaining that by answering a few questions, FAST "can figure out whether you're naughty or nice, all on the spot, without knowing anything else about you"); *see* DHS FAST PRESENTATION, *supra* note 6, at 16 (explaining that "[i]ndividuals must serve as their own baseline" before being asked control and relevant questions).

32. DHS PRIVACY IMPACT ASSESSMENT UPDATE, *supra* note 27, at 2 ("The overall goal of [the] FAST project is to determine whether technology can enable the identification and interpretation of a screened subject's physiological and behavioral cues or signatures without the need for operator-induced stimuli . . . .").

33. *Id.* DHS notes that this would limit the chance for people to alter their body language due to the passive, non-intrusive nature of the system because a person would have very little warning that he or she is being scanned. *Id.*

34. Cherry & Corley, *supra* note 7, at 60.

35. DEP'T OF HOMELAND SEC., FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) SYSTEM 2 [hereinafter FAST FACT SHEET], *available at* http://epic.org/privacy/fastinstallation.pdf (last visited Dec. 21, 2014).

36. DEP'T OF HOMELAND SEC., FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) 5 (2010) [hereinafter DHS FAST FOOD INDUSTRY STUDY], *available at* http://epic.org/privacy/fastinstallation.pdf.

37. DHS FAST PRESENTATION, *supra* note 6, at 9–10 (running the Draper test by placing food service volunteers into three categories: (1) no malintent, (2) malintent without device, and (3) malintent with goal of smuggling a recording

actual crimes, volunteers were unaware that they were involved in a test and were motivated by a monetary bonus if they made it through and by a loss of funds if they did not.[38] Similar to the planned operational deployment, the volunteers had a baseline recorded while approaching a guard where they presented identification.[39] Next, the volunteers entered the screening area to answer a few questions.[40] Based on a computer algorithm containing the malintent theory, the volunteers were then sent for additional screening if they showed indices of malintent based on the fluctuation between their vital signs when they initially approached a guard and when a guard subsequently questioned them.[41] DHS hopes that the system will soon be ready for deployment in less controlled venues, such as mass transit portals and border crossings, but still employing only volunteers.[42]

DHS would primarily use FAST as a preliminary screening tool to indicate whether a scannee should be screened further.[43] The system is designed to give screeners additional information about the people in a security line and "is not intended to provide 'probable cause' for law enforcement processes,"[44] meaning that no one can be arrested simply for triggering the scans.[45] Unlike a metal detector, which provides concrete evidence that the person has a concealed and unidentified metal object, a FAST scan would only increase suspicion

---

device into the facility); *see also* DHS FAST FOOD INDUSTRY STUDY, *supra* note 36, at 5 (reporting on a second test that recruited participants with food or security experience and assigning them malintent or no malintent conditions similar to the Draper test in 2011).

38. DHS FAST PRESENTATION, *supra* note 6, at 9–12.

39. *Id.* at 7, 15.

40. *Id.* at 7.

41. *Id.* The FAST system uses a complex statistical algorithm that can aggregate data from multiple databases to detect signs of malintent. Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1499 (2013) (explaining that FAST "rel[ies] upon complex statistical algorithms that can . . . 'predict' future criminal or terrorist acts" through covert cybersurveillance and data mining).

42. DHS PRIVACY IMPACT ASSESSMENT UPDATE, *supra* note 27, at 3.

43. Cherry & Corley, *supra* note 7, at 62 (highlighting that, for example, flight passengers who show malintent would be sent for additional screening, which is "the same thing that happens when a passenger's behavior sets off suspicion in the frontline security officers"). DHS claims the system would allow security screenings to go faster for the vast majority of people because the only people who would need to go through the secondary screening would be those that triggered FAST. *See id.* ("We have a lot of people in line, and we have to get them through quicker. We have to identify the people of interest." (internal quotation marks omitted)).

44. DHS PRIVACY IMPACT ASSESSMENT UPDATE, *supra* note 27, at 2.

45. Cherry & Corley, *supra* note 7, at 62.

that a person might intend to commit a crime.[46] FAST merely flags a person for additional review and, similar to polygraphs, the results of a FAST scan cannot be used in a court of law.[47]

B. Criticism of the FAST System

Commentators are critical of FAST for two main reasons: (1) FAST potentially has an indefinite scope, and (2) the theory underlying FAST is undermined by the same flaws that plague the polygraph. These fears are not unfounded given DHS's indication that the system could be deployed at airport and border checkpoints or at large public events, such as sporting venues or high-profile conventions.[48] Further, DHS intends to deploy mobile units across cities to detect crimes before they occur.[49] Because FAST can capture data remotely and the scannees may not realize that they are being scanned, the government could covertly monitor ordinary citizens.[50]

DHS already uses behavioral detection specialists in airport screenings and high profile events.[51] During the 2005 Presidential Inauguration, DHS posted Screening of Passengers by Observation Techniques ("SPOT") agents at Metro stations in the District of Columbia to detect indices of malintent.[52] If the government uses behavioral detection technology beyond the national security

---

46. Lindsey Gil, Note, *Bad Intent or Just a Bad Day? Fourth Amendment Implications Raised by Technological Advances in Security Screening*, 16 B.U. J. SCI. & TECH. L. 231, 254–55 (2010).

47. Eisenberg, *supra* note 8.

48. FAST FACT SHEET, *supra* note 35, at 2.

49. Solomon, *supra* note 5.

50. Hu, *supra* note 41, at 1499; Margit Sutrop & Katrin Laas-Mikko, *From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics*, 29 REV. POL'Y RES. 21, 22–23 (2012); *Future Attribute Screening Technology (FAST) Project FOIA Request*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/fastproject (last visited Dec. 21, 2014) (arguing that FAST is a "sensor array used to conduct covert surveillance of individuals who are not suspected of any crime").

51. Florence & Freidman, *supra* note 14, at 425–26. Screening of Passengers by Observation Techniques ("SPOT") is a DHS program wherein DHS Behavioral Detection Officers screen airport passengers for people who exhibit strange or anxious behavior, such as "changes in mannerisms, excessive sweating on a cool day, or changes in the pitch of a person's voice." *Id.* SPOT focuses on subtle behavior, such as "facial micro-expressions" and body language. *Id.* at 426. Facial micro-expressions can include the slant of one's eyebrows, while body language can be as innocuous as slumped posture or excessive pocket patting. *Id.*

52. *Id.* at 434 (arguing that because SPOT does not require any specialized screening equipment, it can be "highly beneficial to *all modes of transportation*" and "could foreshadow an expanded use of the program at other public places frequented by large numbers of Americans").

context, "[i]t is not inconceivable that the U.S. intelligence community's alleged domestic use of spy satellites could be combined with SPOT-like visual cue observation[s] so that virtually everybody in a public place is subject to behavioral profiling at all times."[53] As DHS plans to use FAST for ordinary crime detection,[54] the mass surveillance of Americans' intimate activities would become a cheap and easy endeavor for the government to pursue.[55]

The more common concern is that, similar to a polygraph, the indicators that DHS ascribes to malintent can be triggered for other reasons, such as going to see one's mistress.[56] DHS nevertheless notes that the system is able to detect whether a suspect is just nervous or in fact has malintent because the system measures the scannee against his or her own individualized baseline.[57] Moreover, because FAST only detects intent to commit a crime, it is unlikely that it would be able to detect when someone unknowingly carries a bomb into a secure area or if a terrorist believes that what he is doing is not a crime.[58] A researcher at Carnegie Mellon University questions the theory that certain biometrics are related to intent, while other researchers fear a prohibitive number of false positives.[59] The Government Accountability Office (GAO) also expressed concerns with the reliability of behavioral detection since peer-reviewed publications "do not support the use of behavioral indicators to

---

53. *Id.* at 434–35. Justin Florence and Robert Friedman's article was published before there was widespread knowledge of the FAST system and that DHS was already developing a remote behavioral detection program.

54. Solomon, *supra* note 5 (postulating that DHS could deploy mobile units to detect crime before it occurs).

55. Everett, *supra* note 12, at 6.

56. Cherry & Corley, *supra* note 7, at 61.

57. *Id.*

58. *Id.* at 62 (suggesting that FAST in its current form would be useless against people who unknowingly carry bombs because the theory behind the technology is premised on what people know).

59. *See id.* ("In screening large populations for exceedingly rare occurrences, false positives dominate outcomes; any researcher engaging in a modicum of quantitative analysis would reject the hypothesis immediately."); Pam Benson, *Will Airports Screen for Body Signals? Researchers Hope So*, CNN, http://www.cnn.com/2009/TECH/10/06/security.screening (last updated Oct. 6, 2009, 9:15 PM) (relating that Professor Stephen Fienberg of Carnegie Mellon University does not believe the available peer-reviewed research validates the theory of malintent or that malintent can be determined via measurements of an individual's vital signs); *see also* Solomon, *supra* note 5 (asserting that some researchers claim using physiological indicators to predict malicious intent could inadvertently cause FAST to flag "innocent people").

identify mal-intent or threats to aviation."[60] Combined with the inability to detect certain actions, FAST possesses potential weaknesses.

C. How FAST Purports to Protect a Scannee's Privacy

DHS provides extensive security for the participants' personally identifiable information (PII) during testing.[61] All participants are identified through an anonymous code that is not linked to any PII.[62] Any PII received from the intake surveys is secured in a separate laboratory accessible only to laboratory personnel, and all testing data is stored on a private network.[63] Further, any data obtained during the tests is retained only to validate the system and the DHS Science and Technology Directorate (DHS S&T) receives only aggregate results.[64]

DHS has not disclosed how it will protect the data that it obtains during FAST's operational deployments,[65] but proponents note

---

60. *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities: Testimony Before the Subcomm. on Transp. Sec. of the H. Comm. on Homeland Sec.*, 113th Cong. 31–32 (2013) (prepared statement of Stephen M. Lord, Managing Director, Forensic Audits and Investigative Service, Government Accountability Office). The Government Accountability Office's (GAO) concerns have focused on the SPOT program and "human observation unaided by technology," so its conclusions, though valid, may not fully conform to FAST; however, GAO has mentioned that some studies concluded that behavioral indicators generally are unable to detect malintent. *Id.* at 31. Some members of the media criticize DHS for "fall[ing] for a classic form of self-deception: the belief that you can read liars' minds by watching their bodies." *Behavior Detection Isn't Paying Off*, N.Y. TIMES (Apr. 6, 2014), http://www.nytimes.com/2014/04/07/opinion/behavior-detection-isnt-paying-off.html?_r=0.

61. PII is any information that can identify a person, including demographic information, video and audio recordings, images, medical records, and psychophysiological measurements. DHS PRIVACY IMPACT ASSESSMENT, *supra* note 26, at 6–7.

62. *Id.* at 5, 8 (assigning a unique anonymous identifier to the test participants to guard their individual data, including demographic, medical and psychiatric information, and medication and substance use data).

63. *Id.* at 8–9; *see also* DHS PRIVACY IMPACT ASSESSMENT UPDATE, *supra* note 27, at 6 (noting that video and thermal data is password protected and encrypted, that all data is anonymized and aggregated before being reported, and that once data starts being collected, there is no external network connection).

64. DHS PRIVACY IMPACT ASSESSMENT, *supra* note 26, at 4–5 (explaining that the data obtained from the test is only shared outside the testing laboratory in the aggregate); DHS PRIVACY IMPACT ASSESSMENT UPDATE, *supra* note 27, at 6 (indicating that DHS S&T "does not have access to, and does not retain, the information collected by researchers").

65. *See* Sutrop & Laas-Mikko, *supra* note 50, at 29 ("[I]t has not been determined which kind of privacy policy will be implemented for operating the system in reality.

that the system would be unable to obtain PII from the scans.[66] Additionally, DHS has indicated that it plans to dispose of the data after each scannee has passed through the system and has been cleared.[67]

Despite these assurances, the system could potentially be used to gather data on the public, including using facial recognition to compare against criminal databases or to track movements of people through recognition of their biometrics, rather than using PII.[68]

So far we only have the promise of . . . Homeland Security Advanced Research Projects Agency [that] '[t]he system does not record or maintain your information. Once any issues are resolved, the information is dumped.'"); Email from Jeramie D. Scott, Summer Law Clerk, EPIC Open Gov't Project, Alex Stout, Summer Law Clerk, EPIC Open Gov't Project, & John Verdi, Dir., EPIC Open Gov't Project, to Diane Saunders, Acting Freedom of Info. Act Officer, U.S. Dep't of Homeland Sec. (June 7, 2011), *available at* http://epic.org/privacy/profiling/EPIC_FOIA-FAST-Project.pdf (highlighting that while laboratory testing is anonymized, DHS has not indicated whether it would follow the same procedures with field-testing).

66. *See* Sutrop & Laas-Mikko, *supra* note 50, at 29 (quoting the deputy director of the Homeland Security Advanced Research Projects Agency that FAST would not record or maintain PII); Cherry & Corley, *supra* note 7, at 61 (explaining that DHS has developed the system to ensure that it does not tie scanned data to PII); *Real-life "Minority Report" Program Gets a Try-out*, CBS (Oct. 7, 2011, 5:27 PM), http://www.cbsnews.com/news/real-life-minority-report-program-gets-a-try-out (asserting that a deployed system would not capture PII). *Contra Real-life "Minority Report" Program Gets a Try-out*, *supra* (highlighting that FAST is labeled a "privacy sensitive system," which is defined as a system that "collects, uses, disseminates, or maintains" PII (internal quotation marks omitted)).

67. Cherry & Corley, *supra* note 7, at 61.

68. *See* Sutrop & Laas-Mikko, *supra* note 50, at 31 (predicting "function creep" with biometric identification that would lead to tracking ordinary citizens in public places). The Department of Defense has a program that seeks to positively identify people who pose a threat to U.S. national security through the use of biometrics. *See* DEP'T OF DEF., DEFENSE BIOMETRIC ENABLED INTELLIGENCE (BEI) AND FORENSIC ENABLED INTELLIGENCE (FEI) 1–2 (2012), *available at* https://info.publicintelligence.net/DoD-BiometricIntelligence.pdf; *Identity/Biometric Enabled Intelligence*, BOOZ ALLEN HAMILTON, http://www.boozallen.com/consulting/technology/cyber-security/identity/identity-biometric-enabled-intelligence (last visited Dec. 21, 2014) (outlining that biometric-enabled intelligence can be collected overtly and covertly to match people to a place or activity by using biometrics such as facial scans, video, and "3D full-body scans").

II. FOURTH AMENDMENT JURISPRUDENCE

A. The Fourth Amendment Principles Underlying an Administrative Search

The Fourth Amendment protects people from unreasonable governmental searches.[69] In *Katz v. United States*,[70] Justice Harlan's concurring opinion set forth the current test to determine whether government activity constitutes a search under the Fourth Amendment.[71] Under that test, a Fourth Amendment search occurs when "a person ha[s] exhibited an actual (subjective) expectation of privacy" in the place searched and "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[72] As the majority of the Court emphasized in *Katz*, the Fourth Amendment's purpose is to "protect[] people, not places."[73]

However, the Supreme Court has expressly noted that this right only applies to things in which a person has an expectation of privacy—not to things that a person knowingly exposes to the public.[74] The Supreme Court has distinguished through a number of cases that evidence that is exposed to the public is not protected by the Fourth Amendment, such as by aerial observations of an enclosed backyard[75] or by the police going through a person's garbage.[76] This

---

69. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

70. 389 U.S. 347 (1967).

71. *Id.* at 361 (Harlan, J., concurring).

72. *Id.* (explaining that "a man's home" is a place when he can expect privacy but that he cannot expect privacy in information he places in the public domain). Although the *Katz* test on its face seems to displace the common law doctrine of a search involving a physical trespass into a protected area, it only supplements the common law test. United States v. Jones, 132 S. Ct. 945, 951–52 (2012).

73. *Katz*, 389 U.S. at 351; *see also* Schmerber v. California, 384 U.S. 757, 767 (1966) (postulating that the overriding purpose of the Fourth Amendment is "to protect personal privacy"); Bourgeois v. Peters, 387 F.3d 1303, 1315 (11th Cir. 2004) ("In their persons and property, however, individuals 'are not shorn of all Fourth Amendment protections when they step from their homes onto the public sidewalks.'" (quoting Delaware v. Prouse, 440 U.S. 648, 662–63 (1979))).

74. *See, e.g.*, *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

75. Florida v. Riley, 488 U.S. 445, 450–51 (1989) (finding that a homeowner does not have a reasonable expectation of privacy when it was possible to view the marijuana plants in the greenhouse from an aerial or elevated perspective); California v. Ciraolo, 476 U.S. 207, 213–15 (1986) (determining that if the public can see evidence, even if it is inside of a person's home, then police officers need not

doctrine affirms that "an individual may not legitimately demand privacy for activities conducted out of doors . . . , except in the area immediately surrounding the home."[77] The Court rests its analysis on the notion that no "intimate activities" take place in open fields outside of the home and that there is no societal interest in protecting such outside activities, especially when members of the general public can easily observe these activities.[78] However, the Court has not addressed the question of what occurs when a police officer, while on a public thoroughfare, observes the activities that occur inside of a house.[79] Several federal courts of appeals have addressed this issue and concluded that officers can look through the windows of a home to observe evidence but that to seize that evidence, the officers must still obtain a warrant to enter the protected area.[80] There is no Fourth Amendment search if the item was knowingly exposed to the public.

The Fourth Amendment most clearly prohibits a physical trespass into a protected area, but the analysis becomes more difficult when the government uses technology to "see into" a protected area

---

"shield their eyes when passing by [the] home on public thoroughfares" and concluding that an individual did not have an expectation of privacy in marijuana plants on his property when they were visible to the public from an aerial view).

76. California v. Greenwood, 486 U.S. 35, 39–40 (1988). *Greenwood* notes that a mere expectation of privacy is not enough: society must be prepared to recognize the expectation as reasonable. *Id.* at 40. In the case of trash, society is not ready to recognize an expectation of privacy in one's garbage as reasonable because garbage is "readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.* (footnotes omitted).

77. Oliver v. United States, 466 U.S. 170, 178 (1984).

78. *Id.* at 179.

79. *See* Craig M. Bradley, *"Knock and Talk" and the Fourth Amendment*, 84 IND. L.J. 1099, 1099–1100 (2009) (exploring the "knock and talk" police procedure where police officers, without probable cause, knock on a door so they can observe items within a house and noting that the Supreme Court had not addressed whether this procedure violates the Fourth Amendment).

80. *See, e.g.*, United States v. Wells, 648 F.3d 671, 678 (8th Cir. 2011) (noting that officers have a lawful right to observe activities conducted within a protected area from a public street but that they may not enter the home without a warrant or absent exigent circumstances); United States v. Daoust, 916 F.2d 757, 758 (1st Cir. 1990) (finding that as long as the police had a right to be where they could observe evidence, they could legally view anything they could see); *see also* Bradley, *supra* note 79, at 1099–1100 (stating that federal courts of appeals and state courts have approved of the "knock and talk" procedure). *But see* Pate v. Mun. Court, 89 Cal. Rptr. 893, 895 (1970) (finding a search when a suspect closed his motel room curtains and the officer climbed a trellis to look into the suspect's room on the second floor of the motel).

without a physical trespass. The Supreme Court explained in *Kyllo v. United States*[81] that when the government uses a sense-enhancing device not generally used by the public to obtain information from a protected place that could only otherwise be obtained through a physical trespass, a search has occurred.[82] The *Kyllo* test emphasizes what the search reveals rather than the search method used.[83] The *Kyllo* Court noted that the thermal imager at issue in the case could detect intimate activities such as "at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate.'"[84]

The Court has recognized an exception to this general rule, however, when the device used cannot obtain any intimate details about the place searched but, rather, can only reveal the existence or non-existence of contraband.[85] In *United States v. Place*,[86] the Court held that using a drug-sniffing dog that could only reveal the presence or absence of contraband was merely a sense-enhancing search, not an extra-sensory search; since the sense-enhancing search could not reveal intimate details, it was not a search under the Fourth Amendment.[87] Accordingly, the Court's Fourth Amendment jurisprudence allows warrantless binary sense-enhancing searches[88] since they are not searches under the Fourth Amendment but

---

81. 533 U.S. 27 (2001).

82. *Id.* at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use." (citations omitted)).

83. Luke J. Albrecht, Case Comment, *Constitutional Law—The Use of a Thermal Imaging Device Constitutes a Search Under the Fourth Amendment*—Kyllo v. United States, *533 U.S. 27 (2001)*, 36 SUFFOLK U. L. REV. 249, 255 (2002) (arguing that the Court properly focused its analysis in *Kyllo* on the place that was searched and not on the intrusiveness of the search).

84. *Kyllo*, 533 U.S. at 38.

85. United States v. Place, 462 U.S. 696, 707 (1983) ("[T]he canine sniff is *sui generis*. We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure.").

86. 462 U.S. 696 (1983).

87. *Id.* at 707 (reasoning that a drug-sniffing dog can tell authorities only limited information about the contents of a container—whether or not the container contains contraband—and thus does not embarrass the owner of the property). *Place* held further that with probable cause, the government is able to briefly detain an individual's luggage to obtain a search warrant from a judge. *Id.*

88. The term "binary search," as used here, means a search that can only reveal the presence or absence of contraband—nothing more.

disapproves of extra-sensory searches that have the potential to reveal intimate details about the place searched.[89]

The Court recently ruled in *Riley v. California*[90] that police officers cannot search the contents of a person's cell phone without a warrant because the person has a reasonable expectation of privacy in the phone's contents.[91] The Court relied on the "vast quantities of personal information" that cell phones contain and distinguished the searches from the "brief physical search" that the doctrine normally encompasses.[92] Specifically, cell phones contain sensitive personal information, such as videos, prescriptions, and bank statements, that were not feasibly carried around with a person "[p]rior to the digital age."[93] Cell phones contain Internet search histories that could show that the person "search[ed] for certain symptoms of disease," information on individuals' locations and private lives, and "sensitive records previously found in the home."[94] The Supreme Court prohibited law enforcement from searching phones without a warrant specifically because phones contain highly sensitive information.

The Court has allowed limited searches without a warrant, but only where an officer has reasonable suspicion that a person is armed and dangerous *prior* to conducting the search. In *Terry v. Ohio*,[95] the Court justified this narrow exception with the need to protect the officer, where the officer "has reason to believe that he is dealing with an armed and dangerous individual."[96] The Court, however, noted that the suspicion had to arise before the search: the search could not be used to justify the need for the search.[97]

---

89. *See Place*, 462 U.S. at 707 ("A canine sniff by a well-trained narcotics detection dog . . . 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 . . . luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive than a typical search.").

90. 134 S. Ct. 2473 (2014).

91. *Id.* at 2492, 2494 (holding that neither the officer safety nor the preservation of evidence justification permitted officers to search the contents of the defendant's cell phone without a warrant).

92. *Id.* at 2485.

93. *Id.* at 2489–90.

94. *Id.* at 2489–91.

95. 392 U.S. 1 (1968).

96. *Id.* at 27.

97. *See id.* at 30 (finding that "[a]t the time" the decision to search for weapons was made, the officer "had reasonable grounds to believe that [the] petitioner was armed and dangerous").

B. The Administrative Search Exception to the Warrant Requirement

Although a search is presumed unreasonable without a warrant, the Court has carved out several exceptions when a warrant is not required.[98] The administrative search exception[99] allows a warrantless search of people and places in highly regulated industries pursuant to a regulatory scheme as long as the governmental interest in the search outweighs its intrusion of people's privacy rights.[100] The administrative exception excuses the need for individual suspicion in highly regulated industries if there is a substantial governmental interest and the inspection furthers a governmental regulatory

---

98. *See* United States v. Robinson, 414 U.S. 218, 224 (1973) (recalling that a search incident to a lawful arrest has long been a traditional exception to the warrant requirement); Chimel v. California, 395 U.S. 752, 766 (1969) (allowing a search of an area within an arrestee's reach). The exceptions are "(1) stop-and-frisk search[es]; (2) administrative searches; (3) the border search; and (4) searches based on express or implied consent." Bethany A. Gulley, Note, *Criminal Law—No Right to Revoke and Avoid Search—Ninth Circuit Rules that Consent to Airport Screening Cannot be Revoked in an Administrative Search.* United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007)*, 31 U. ARK. LITTLE ROCK L. REV. 515, 518 n.34 (2009) (citation omitted).

99. In order for the balancing requirement of an administrative search to apply, a court must first find that a special need exists. United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007); *see also* United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007) (en banc) (using a "special need" for security checkpoints to allow airport screenings under the administrative search exception); Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 275–76 (2011) (stating that the Supreme Court uses the "special needs test" to determine the validity of administrative searches (internal quotation marks omitted)). First, a court must determine whether there is a special need beyond normal law enforcement needs. *Id.* at 276. If so, then the court will balance the governmental need for the search versus the intrusiveness of the search. *Id.* Under this balancing test, the court must factor the subject's privacy interest versus the government's interest in the search and the scope of the governmental intrusion. *Id.*

100. New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (explaining that the test for determining the reasonableness of a search involves assessing if the search was justified and, as conducted, was reasonably related to the circumstances that justified it); Camara v. Mun. Court, 387 U.S. 523, 530, 533–35 (1967) (finding that since an administrative search does not seek evidence of criminality, it is less of an intrusion and is outweighed by the governmental interest in "securing city-wide compliance with minimum physical standards for private property").

Since the administrative search doctrine is a widely used exception to the warrant requirement, one would expect its boundaries to be clear, but "the rules governing administrative searches are notoriously unclear." Primus, *supra* note 99, at 257. Some commentators have suggested that administrative search law actually conflates two separate doctrines—so-called "dragnet searches" and "special subpopulation searches"—and that much of the confusion around its use comes from the melding of these doctrines. *Id.* at 259 (internal quotation marks omitted).

scheme.[101] A highly regulated industry is one where there is "such a history of government oversight that no reasonable expectation of privacy could exist for a proprietor over the stock of such an enterprise," such as weapons distributors, pawnshops, mines, quarries, and junkyards.[102] This later was expanded to include "special subpopulations," such as students or governmental employees, and both are now analyzed under whether the government has a "special need" to conduct the search.[103] To further the governmental regulatory scheme, the search must perform the functions of a warrant, give notice of the search, and limit the discretion of the searching officers; the search also needs to be narrowly tailored to further that scheme.[104] The administrative search exception is commonly invoked to justify warrantless searches in airports.[105] The exception can be invoked only in exceptional circumstances, however, and cannot be used to further the ordinary course of police investigations, such as drug interdiction or solving murders.[106] Moreover, to fit within the

---

101. New York v. Burger, 482 U.S. 691, 702–03 (1987) (citing Donovan v. Dewey, 452 U.S. 594, 600–02 (1981)); *see also* Primus, *supra* note 99, at 270 ("First, the searches had to be justified in terms of the balance between the importance of the government's interest and the degree of intrusion upon individuals. . . . Second, dispensing with the requirement of individualized suspicion had to be necessary in order to advance the governmental interest at stake. Third, the searches had to be cabined in ways that limited the discretion of executive officials . . . .").

102. *Burger*, 482 U.S. at 700–04 (citations omitted) (internal quotation marks omitted).

103. Primus, *supra* note 99, at 287–88.

104. *Burger*, 482 U.S. at 702–03.

105. *See* United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973) (explaining that the government screens airline passengers as part of an administrative scheme to prevent people from bringing explosive devices on to or hijacking planes), *overruled in part by* United States v. Aukai, 497 F.3d 955 (9th Cir. 2007) (en banc).

106. Maryland v. King, 133 S. Ct. 1958, 1982 (2013) (Scalia, J., dissenting) ("[S]uspicionless searches are *never* allowed if their principle end is ordinary crime-solving."); City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) (explaining that never before has the administrative exception been used to justify warrantless searches for the purpose of routine law enforcement); New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (commenting that courts may substitute the administrative search test for the traditional Fourth Amendment requirement that a search cannot be conducted unless it is accompanied by a warrant based on probable cause only in "exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable"). The administrative search is likely the exception that would be invoked by the government to justify the use of the FAST scans. *Cf.* Gil, *supra* note 46, at 246–49, 261 (stating that security searches in airports fall under the administrative search exception). The special need must be a unique problem that

exception, these searches must be minimally intrusive and directly related to the special governmental need.[107]

Despite being an exception to the warrant requirement, administrative searches must be reasonable. The federal courts of appeals, particularly the U.S. Court of Appeals for the Ninth Circuit, have enumerated a balancing test to determine the reasonableness of the administrative search, using the totality of the circumstances approach, by weighing the governmental "need" versus the intrusion onto a person's individual privacy.[108]

---

law enforcement officers would not encounter in the course of their day-to-day routine. WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 3.9(a) (3d ed. 2007).

107. *See* Renée McDonald Hutchins, *The Anatomy of a Search: Intrusiveness and the Fourth Amendment*, 44 U. RICH. L. REV. 1185, 1201, 1206–07 (2010) (explaining that the Supreme Court has allowed the warrantless use of technology only when the amount of information revealed is "tightly circumscribed"); Gil, *supra* note 46, at 247 (explaining that the administrative search exception requires that the search be minimally intrusive and the governmental interest must be significant and legitimate). To determine the validity of a "special needs" search, courts must consider three factors: (1) the government's need for the search, (2) the character and nature of the search, and (3) the nature of the privacy interest involved. Cassidy v. Chertoff, 471 F.3d 67, 75 (2d Cir. 2006).

108. The Ninth Circuit in *United States v. Davis* took the lead in developing this doctrine. 482 F.2d 893 at 910 (arguing that requiring officers to secure warrants to screen airline passengers would "frustrate the governmental [administrative] purpose" but limiting the government's authority to only those searches that are not intrusive (internal quotation marks omitted)). Other circuits have adopted the Ninth Circuit's analysis. *See, e.g.*, Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011) (citing United States v. Knights, 534 U.S. 112, 118–19 (2001)) (arguing that the balancing of the government's interest in deterring and preventing passengers from bringing explosive devices on to airplanes overcomes an individual passenger's interest in his or her privacy, particularly because the Transportation Security Administration has put in place safeguards to protect passengers' privacy); United States v. Hartwell, 436 F.3d 174, 178–79 (3d Cir. 2006) ("Suspicionless checkpoint searches are permissible under the Fourth Amendment when a court finds a favorable balance between the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty." (internal quotation marks omitted)); United States v. Albarado, 495 F.2d 799, 807–08 (2d Cir. 1974) (discussing the Ninth Circuit's reasoning in *Davis*, where the court held that airport security searches fall under the administrative search exception because they are designed to catch would-be hijackers, and to justify the constitutionality of airport searches). The Supreme Court also endorsed the Ninth Circuit's analysis in a footnote. *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 675 n.3 (1989) (recalling that the special needs search doctrine has long been established under cases like *Davis*).

A minimally intrusive search is one that is "well-tailored to protect [an individual's] personal privacy"[109] and furthers a governmental interest.[110] To further a governmental interest, the regulatory scheme must fulfill the purpose of a warrant and be: (1) known to scannees prior to its occurrence; (2) limited in scope; and (3) narrowly tailored to the government's special need.[111] For example, an administrative airport search is valid if the search is limited to searching for guns, explosives, or other dangerous devices that may jeopardize airport safety.[112] These searches are ultimately justified by the governmental interest in preventing terrorist attacks, but they become unconstitutional once they are used to target common criminal activity, such as drug smuggling, larceny, money laundering, or identity theft.[113] Indeed, the special need must be unique to the situation.[114]

III. PRIVACY INTEREST IN MEDICAL DATA

A. Remotely Gathering Medical Data

When the Fourth Amendment was drafted, a physician could only obtain medical data through a physical examination.[115] It is now possible for a doctor to diagnose a patient only from looking at the patient's medical records and vital signs without ever physically examining the patient.[116] Additionally, physicians can now remotely

109. *Aukai*, 497 F.3d at 962 (quoting *Hartwell*, 436 F.3d at 180).

110. New York v. Burger, 482 U.S. 691, 702–03 (1987).

111. *Id.* In the context of airport security searches, the search must be "conducted in good faith for the purpose of preventing hijacking or like damage and with reasonable scope and the passenger [must have] been given advance notice of his liability to such a search so that he can avoid it by choosing not to travel by air." United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974) (citation omitted).

112. *Aukai*, 497 F.3d at 960 (reasoning that airport screening searches are part of a regulatory scheme to prevent plane bombings and hijackings).

113. *Davis*, 482 F.2d at 908–09 (requiring that courts must exclude evidence from airport searches that are "subverted" into general searches for criminal evidence); *see also Aukai*, 497 F.3d at 959 (indicating that that "special governmental needs" exceed those of "normal . . . law enforcement" but must be balanced against individual expectations of privacy (quoting *Von Raab*, 489 U.S. at 665–66)); *Albarado*, 495 F.2d at 807–08 (proposing that administrative searches in an airport context are not designed to catch criminals but to deter armed hijackers).

114. Nicholas v. Goord, 430 F.3d 652, 662–63 (2d Cir. 2005).

115. *See* L.G. Eichner, *The Practice of Domestic Medicine During the Colonial Period*, 41 TREDYFFRIN EASTTOWN HIST. Q. 100, 103 (2004) (explaining that a physician would compare a patient's symptoms to descriptions of diseases in medical textbooks to diagnose the patient).

116. *What Is Telemedicine?*, AM. TELEMEDICINE ASS'N, http://www.americantelemed.org/about-telemedicine/what-is-telemedicine#.VEpaEvldXOI (last visited Dec. 21,

monitor long-term patients through non-invasive electrocardiographic and respiratory monitors that track arterial oxygen saturation, skin temperature, body weight, blood pressure, and blood glucose levels[117]—similar to the metrics that will be analyzed by the FAST system.

By remotely scanning vital signs, a FAST scan would be able to remotely gather medical data on the scannees. The FAST system is designed to remotely monitor physiological characteristics such as heart rate, respiratory rate, eye movement, body temperature, pheromone levels, and audio levels.[118] The measurements are then used to detect abnormalities in physiology.[119] Respiratory measurements are used to evaluate respiratory disorders, such as respiratory dysfunction and cystic fibrosis, as well as to measure the severity of the disease in patients with asthma or community-acquired pneumonia.[120] Using FAST's respiratory sensors, DHS would be able to measure these rates, and if so inclined, to obtain a detailed medical record on any person scanned by FAST.

Measuring beat-to-beat fluctuations in heart rate provides an analysis of the principal cardiovascular control systems, and it can determine the overall health of the cardiovascular system and

---

2014) (informing on the nature of telemedicine, which includes a review of medical records, remote gathering of vital signs, and possibly a video conference between patient and doctor); *see also* Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1136 (3d Cir. 1995) (reporting that a doctor diagnosed an employee with human immunodeficiency virus (HIV) after only reviewing the employee's medical records).

117. Sara Colantonio et al., *Decision Support for Remote Management of Chronic Patients*, 83 LECTURE NOTES INST. FOR COMPUTER SCIS. SOC. INFORMATICS & TELECOMMS. ENGINEERING 38, 38–39 (2012) (discussing the advances in technological monitoring of patients with chronic diseases).

118. *See supra* notes 26–28 and accompanying text.

119. Gary B. Smith et al., *Hospital-Wide Physiological Surveillance—A New Approach to the Early Identification and Management of the Sick Patient*, 71 RESUSCITATION 19, 20 (2006) (recognizing that vital sign measurements are important for detecting changes in physiology).

120. *E.g.*, Iley B. Browning et al., *Importance of Respiratory Rate as an Indicator of Respiratory Dysfunction in Patients with Cystic Fibrosis*, 97 CHEST 1317, 1319 (1990) (cystic fibrosis); *see* Walter Karlen et al., *Improving the Accuracy and Efficiency of Respiratory Rate Measurements in Children Using Mobile Devices*, PLOS ONE, June 2014, at 1, 1 (recounting that respiration rate is a "marker of serious respiratory illness" and "the main diagnostic criterion for childhood pneumonia"); Steven Kesten et al., *Respiration Rate During Acute Asthma*, 97 CHEST 58, 60–62 (1990) (finding that asthmatics had a higher respiratory rate when having an attack); J.P. McFadden et al., *Raised Respiratory Rate in Elderly Patients: A Valuable Physical Sign*, 284 BRIT. MED. J. 626, 627 (1982) (finding that respiratory rates in an invaluable diagnostic tool for respiratory disorders in elderly patients).

whether a patient has one of the seven classes of arrhythmias.[121] FAST's cardiovascular measurement would be able to assess autonomic imbalances, disease, and mortality rates by measuring heart rate because heart rate variation is associated with cardiovascular disease.[122] Heart rate variability is one of the most important measurements that can predict atherosclerotic plaque progression, which leads to heart attacks, congestive heart failure, and susceptibility to diabetic neuropathy.[123]

Most troubling however, is that FAST can also measure chemosensory stimuli such as pheromone levels, which can indicate the existence of psychiatric diseases like anxiety and depression, as well as stress levels or a person's emotional status, like fear or excitement.[124] Further, pheromones are associated with whether a

---

121. Solange Akselrod et al., *Power Spectrum Analysis of Heart Rate Fluctuation: A Quantitative Probe of Beat-to-Beat Cardiovascular Control*, 213 SCIENCE 220, 220 (1981) (cardiovascular system health); K.C. Chua et al., *Cardiac State Diagnosis Using Higher Order Spectra of Heart Rate Variability*, 32 J. MED. ENGINEERING & TECH. 145, 154 (2008) (arrhythmia).

122. Julian F. Thayer et al., *The Relationship of Autonomic Imbalance, Heart Rate Variability and Cardiovascular Disease Risk Factors*, 141 INT'L J. CARDIOLOGY 122, 123 (2010) ("[A]utonomic imbalance may be a final common pathway to increased morbidity and mortality from a host of conditions and diseases, including cardiovascular disease. Heart rate variability (HRV) may be used to assess autonomic imbalances, diseases and mortality. Parasympathetic activity and HRV have been associated with [many diseases] including CVD . . . ."). *See generally* Kim Fox et al., *Resting Heart Rate in Cardiovascular Disease*, 50 J. AM. C. CARDIOLOGY 823, 823 (2007) (explaining that heart rate is an indicator of cardiovascular disease and can determine the risk of cardiovascular mortality).

123. Borejda Xhyheri et al., *Heart Rate Variability Today*, 55 PROGRESS CARDIOVASCULAR DISEASES 321, 321 (2012).

124. Denise Chen & Jeannette Haviland-Jones, *Human Olfactory Communication of Emotion*, 91 PERCEPTUAL & MOTOR SKILLS 771, 778–80 (2000) (finding that a person's emotional states influence their body odor); Bettina M. Pause et al., *Startle Response Potentiation to Chemosensory Anxiety Signals in Socially Anxious Individuals*, 74 INT'L J. PSYCHOPHYSIOLOGY 88, 91 (2009) (concluding that people communicate information about their emotional states through their chemosensory senses); Alexander Prehn et al., *Chemosensory Anxiety Signals Augment the Startle Reflex in Humans*, 394 NEUROSCIENCE LETTERS 127, 127 (2006) (adding that "chemosensory anxiety signals can be consciously identified" in humans). Humans can recognize differences in pheromones to recognize kin versus non-kin. Babies, for instance, are more receptive to their mother's breast than to another's breasts. Richard H. Porter, *Olfaction and Human Kin Recognition*, 104 GENETICA 259, 260–61 (1999) (kin and maternal odor); Richard H. Porter & Jan Winberg, *Unique Salience of Maternal Breast Odors for Newborn Infants*, 23 NEUROSCIENCE & BEHAV. REVS. 439, 439–40 (1999) (breast odor recognition). Pheromones also play a role in mate selection. Carole Ober et al., *HLA and Mate Choice in Humans*, 61 AM. J. HUM. GENETICS 497, 502–04

woman is ovulating and genetic compatibility.[125] These vital signs, which DHS could scan with FAST, implicate medical data that is as intimate, if not more so, than the Supreme Court's concern in *Kyllo* of the government knowing when a woman takes her evening bath.[126]

B. Special Protection of Medical Records

The highly sensitive nature of medical information is underscored by the special protection that the law gives medical data, even when held by a third party. Traditionally, people do not have a privacy interest in non-medical data held by a third party, and there is therefore no search when that data is disclosed to the government.[127] However, people maintain a limited privacy right in medical records maintained by a third party.[128] Unlike traditional data, medical records are legally protected, and the government's need to access those records must be balanced against the patient's privacy interest

---

(1997) (finding that humans tend to not mate with humans who share similar pheromones). Although many studies begin in animal studies, similar results have been found in humans. *E.g.*, Chen & Haviland-Jones, *supra*, at 771–72.

125. Seppo Kuukasjärvi et al., *Attractiveness of Women's Body Odors over the Menstrual Cycle: The Role of Oral Contraceptives and Receiver Sex*, 15 BEHAV. ECOLOGY 579, 584 (2004) (finding that males preferred a female's odor when the female was nearing ovulation); Claus Wedekind & Sandra Füri, *Body Odour Preferences in Men and Women: Do They Aim for Specific MHC Combinations or Simply Heterozygosity?*, 264 PROC. ROYAL SOC'Y BIOLOGICAL SCI. 1471, 1476 (1997) (finding that men and women can distinguish odors based on genetic compatibility). Researchers have also linked pheromones to indicators of sexual orientation. Yolanda Martins et al., *Preference for Human Body Odors Is Influenced by Gender and Sexual Orientation*, 16 PSYCHOL. SCI. 694, 694 (2005) (suggesting that sexual orientation may affect the production of pheromones); Michael Craig Miller, *Human Pheromones*, HARV. MENTAL HEALTH LETTER, Nov. 2006, at 8 (detailing that some scientific research discovered a relationship between sexual orientation and responses to olfactory stimuli).

126. Kyllo v. United States, 533 U.S. 27, 38 (2001).

127. United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012) ("A customer ordinarily lacks 'a reasonable expectation of privacy in an item,' like a business record, 'in which he has no possessory or ownership interest.'" (quoting United States v. Cormier, 220 F.3d 1103, 1108 (9th Cir. 2000))). *But see* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (arguing that the Court should reconsider whether individuals have a reasonable expectation of privacy in information given to third parties because in the "digital age, . . . people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"); *cf.* 18 U.S.C. § 2703(d) (2012) (requiring that electronic records beyond the basic subscriber information held by a communication service requires a warrant for government access).

128. *See* Whalen v. Roe, 429 U.S. 589, 598–600, 602 (1977) (determining that unwarranted disclosures of stored medical records would be an invasion of privacy).

in those records.[129] In order to access these medical records, the requestor must have a legitimate need for them—a higher protection than that given to non-medical data held by third parties.[130] Although the Health Insurance Portability and Accountability Act's (HIPAA) prohibition against knowingly obtaining individually identifiable health information likely does not apply in the context of FAST because FAST is a system, and the government is neither a provider, plan, employer of the scannees, nor clearinghouse,[131] its provisions highlight the extra protections that Congress has assigned to medical data. Unlike data that is held by a third-party, HIPAA contains specific requirements that must be met before law enforcement is able to obtain medical data.[132]

---

129. *Cf.* Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1137, 1140 (3d Cir. 1995) (holding that the governmental intrusion for accessing an AIDS patient's records was minimal since the administrator only disclosed his medical status to people who already knew of his condition and the patient was not discriminated against since he was promoted); Gen. Motors Corp. v. Dir. Nat'l Inst. for Occupational Safety & Health, 636 F.2d 163, 165–66 (6th Cir. 1980) (noting that the government's need to conduct a safety study to determine the cause of a skin disease was balanced against the privacy interest in medical records and the protection against disclosure).

130. *Se. Pa. Transp. Auth.*, 72 F.3d at 1139 (finding that there is a strong governmental interest in controlling health care costs by monitoring employees' medical prescriptions, but that the need is for the records alone, not for the data contained within them); *see also* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577–78 (3d Cir. 1980) (concluding that the government has a legitimate interest in medical records of workers who work in a dangerous work environment to monitor them for health and safety reasons). In order to obtain these records, the following seven-factor analysis is used: "(1) the type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest favoring access." *Se. Pa. Transp. Auth.*, 72 F.3d at 1140 (citing *Westinghouse Elec. Corp.*, 638 F.2d at 578).

131. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) punishes "[a] person who knowingly . . . obtains individually identifiable health information relating to an individual." Pub. L. No. 104-191, § 262(a), 110 Stat. 1936, 2029 (codified at 42 U.S.C. § 1320d-6(a)(2) (2012)). However, Congress qualified this provision by defining "individually identifiable health information" as information that "(A) is created or received by *a health care provider, health plan, employer, or health care clearinghouse*; and (B) relates to the past, present, or future physical or mental health or condition of an individual . . . ." *Id.* § 262(a), 110 Stat. at 2023 (codified at 42 U.S.C. § 1320d(6)) (emphasis added).

132. Specifically,

> Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six

The special interest in medical data is heightened when that data is obtained directly from a suspect in the course of law enforcement activities. The Fourth Amendment specifically protects "[t]he right of the people to be secure in their persons."[133] This protection is based on the notion that the human body is inherently private and that an intrusion into a person's body "can lead to the utmost affliction of indignity and humiliation."[134] The Supreme Court recently ruled that a blood test, even when the individual is obviously intoxicated and where law enforcement knows how quickly alcohol naturally metabolizes in the blood, still required a warrant if one was practical to obtain.[135] In *Missouri v. McNeely*,[136] a majority of the Court rejected the State of Missouri's argument that the State's interest in preventing drunk driving outweighed any privacy interest a person had in her body.[137] Justice Sotomayor, in the majority opinion, stated that the exigency must be established on a case-by-case basis based on the totality of the circumstances.[138] Further, Chief Justice Roberts

---

> circumstances, and subject to specified conditions: (1) as required by law . . . and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 7 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

133. U.S. CONST. amend. IV.

134. Demetrius Klitou, *Backscatter Body Scanners—A Strip Search by Other Means*, 24 COMPUTER L. & SEC. REV. 316, 316 (2008) (arguing that backscatter scanners intrude on a person's Fourth Amendment right to privacy since they take detailed images of a person's body).

135. Missouri v. McNeely, 133 S. Ct 1552, 1557–58, 1560, 1568 (2013) (holding that obvious intoxication was not an exigent circumstance even though alcohol dissipates in a person's bloodstream over time and that law enforcement should have obtained a warrant before it physically intruded inside of the defendant's body). *McNeely* did not address whether there would ever be an exigent circumstance that would require a warrantless blood test. *Id.* at 1569 (Kennedy, J., concurring).

136. 133 S. Ct 1552 (2013).

137. *Id.* at 1567. The Court found that a nonconsensual blood test violates a person's privacy interest, despite the government's interest in preventing drunk driving. *Id.* at 1560–67.

138. *Id.* at 1560–61.

noted in a concurring opinion that "bodily intrusions like blood draws constitute searches and are subject to the warrant requirement."[139]

In a seemingly contradictory opinion during the same term, the Supreme Court in *Maryland v. King*[140] held that it was constitutional for police to take a DNA swab of an arrestee because the test is minimally intrusive and does not involve a physical intrusion into a person's body.[141] The Court further noted that the search affected by a DNA swab fell under its reasonableness jurisprudence rather than its individualized suspicion jurisprudence.[142] The Court justified its approach by noting that law enforcement always has the right to search an arrestee for identification purposes.[143] The Court also stressed that an arrestee's DNA profile is nothing more than part of his or her identity, similar to his or her name, address, or physical description.[144] "In sum," the Court said, "there can be little reason to question the legitimate interest of the government in knowing for an absolute certainty the identity of the person arrested, in knowing whether he is wanted elsewhere, and in ensuring his identification in the event he flees prosecution."[145] Specifically, the Court noted that law enforcement used the swabs to identify arrestees, not to solve crimes.[146]

The Court expressly distinguished and separated DNA swabs from typical administrative searches in *King*, reserving the use of DNA swabs only for serious arrests and not for administrative searches or lessor crimes.[147] Additionally, the Court confirmed that DNA swabs

---

139. *Id.* at 1569 (Roberts, C.J., concurring in part and dissenting in part); *see also* Schmerber v. California, 384 U.S. 757, 770 (1966) ("Search warrants are ordinarily required for searches of dwellings, and absent an emergency, no less could be required where intrusions into the human body are concerned.").

140. 133 S. Ct. 1958 (2013).

141. *Id.* at 1969 ("A buccal swab is a far more gentle process than a venipuncture to draw blood. It involves but a light touch on the inside of the cheek; and although it can be deemed a search within the body of the arrestee, it requires no surgical intrusions beneath the skin." (internal quotation marks omitted)).

142. *Id.* at 1970.

143. *Id.* (proclaiming that it is "uncontested" that the government has a right to search an arrestee's body when the person is legally arrested).

144. *Id.* at 1972 ("The DNA collected from arrestees is an irrefutable identification of the person from whom it was taken. Like a fingerprint, the 13 CODIS loci are not themselves evidence of any particular crime . . . .").

145. *Id.* at 1977 (internal quotation marks omitted).

146. *Id.* at 1978–79.

147. *Id.* at 1970–71. *But see id.* at 1989 (Scalia, J., dissenting) (suggesting that the majority's position is impossible to enforce because the majority did not define what is a "serious crime[]" (internal quotation marks omitted)); Elizabeth E. Joh, Term Paper, Maryland v. King*: Policing and Genetic Privacy*, 11 OHIO ST. J. CRIM. L. 281, 294

do not present privacy concerns, noting that the swabs were, by statute, limited to collecting the "noncoding parts of the DNA that do not reveal the genetic traits of the arrestee" and the police legally could only obtain this noncoding DNA.[148] The Court also brushed aside any concerns that these swabs could obtain any medical data because "[t]he argument that the testing at issue in this case reveals any private medical information at all is open to dispute."[149] However, the Court concluded that the use of swabs would raise constitutional privacy concerns if the police were able to determine medical traits from the DNA swabs.[150] Further, the Court has found that non-intrusive procedures that reveal medical data are subject to heightened privacy requirements.[151]

Justice Scalia gives a better Fourth Amendment analysis, and perhaps the correct one, in his scathing rebuke of the majority opinion as an opinion that "taxes the credulity of the credulous."[152] In his view, the majority did not understand how DNA evidence actually works and the Court's ruling would open up the door to pretextual DNA stops.[153] He mocked the majority's reliance on identification, noting that three months passed between the defendant's arrest and the date the state tested his DNA, and that an additional fourth month passed before the state test results revealed a DNA match, thus discounting the majority's assertion that there was any need for identification for safety reasons before placing the suspect in the jail population.[154] Specifically, Justice Scalia noted that DNA profiles of arrestees are only entered into the system *after* the arrestee has already been identified and the only justification the majority gave for doing DNA swabs was to solve unsolved crimes that had DNA evidence.[155] Furthermore, Justice Scalia noted that the only permissible identification aspect of DNA was to identify human remains or missing persons: DNA had never been used in the

---

(2013) ("Regrettably, Justice Kennedy's majority opinion is at once too optimistic and [too] doctrinally insufficient.").

148. *King*, 133 S. Ct. at 1979.

149. *Id.*

150. *Id.*

151. *See* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 616–17 (1989) (determining that urinalyses and breathalyzer tests "can reveal a host of private medical facts" and thus implicate privacy concerns).

152. *King*, 133 S. Ct. at 1980 (Scalia, J., dissenting).

153. *Id.*

154. *Id.* at 1984.

155. *Id.* at 1984, 1986.

booking context as only those who had already been positively identified were placed into the system.[156]

The fact that the swab is statutorily prohibited from obtaining the chromosomes that contain genetic material does not put it precisely at odds with the general premise that medical data, even when obtained directly from a person, enjoys a heightened level of protection. Even though the Court in *King* approved of the use of DNA swabs, these swabs were statutorily prohibited from obtaining the genetic markers that could uncover genetic diseases.

Although courts rarely analyze mass data collection under the special needs doctrine, a federal district court recently held that such broad data collection programs, even pursuant to a valid statutory scheme, are too broad and violate the Fourth Amendment.[157] In *Klayman v. Obama*,[158] the U.S. District Court for the District of Columbia confirmed that there is "no governmental interest . . . more compelling [for] the security of the Nation" than the prevention of terrorism when determining the constitutionality of the National Security Agency's (NSA) Bulk Telephony Metadata Program to identify unknown terrorists and prevent terrorist attacks against the United States.[159] The NSA's program was designed to identify potential terrorists "*faster*" than normal investigative techniques.[160] However, the lynchpin of the court's analysis was that the collection program did not independently prevent any imminent attack because the suspects had been identified through traditional means and not through the data collection program.[161] Additionally, the court found that the data collection program infringed upon the reasonable expectation of privacy that the plaintiffs had in their telephone records that the NSA collected with the program.[162] Despite traditional jurisprudence that government acquisition of telephone records held by a third party was not a search,[163] the NSA's data collection program was so dissimilar to the traditional relationship

156. *Id.* at 1986.
157. Klayman v. Obama, 957 F. Supp. 2d 1, 40–41 (D.D.C. 2013).
158. 957 F. Supp. 2d 1 (D.D.C. 2013).
159. *Id.* at 39 (quoting Haig v. Agee, 453 U.S. 280, 307 (1981)).
160. *Id.* at 40.
161. *Id.*
162. *Id.* at 39.
163. *See* Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (concluding that the petitioner was not subjected to an illegal search when a phone company, without a warrant and at law enforcement's request, used a pen register to collect information about the petitioner's outgoing phone calls because people do not have a reasonable expectation of privacy in the phone numbers they dial).

between law enforcement and phone companies because of the nature and quantity of private information NSA obtained in telephone metadata on almost every telephone user, and, "*more importantly*, what that information can tell the Government about people's lives."[164] As a result, the court said that the NSA's "almost-Orwellian" collection program was unreasonable under the Fourth Amendment.[165]

Unlike ordinary non-medical data, the government must have a compelling interest to obtain medical data directly from a suspect's body; therefore, the government must generally comply with the warrant requirement due to the intrusion upon a person's individual privacy—the potential to obtain medical data.[166] Data that is collected through biometric scans—such as FAST—can contain information concerning medical conditions, and such information is necessarily protected under the same analysis as other medical data that can be obtained directly from a person's body.[167]

IV. THE REASONABLENESS OF FAST UNDER THE FOURTH AMENDMENT

A. FAST Scans Are Fourth Amendment Searches

A FAST scan violates the Fourth Amendment because it is an extra-sensory search that obtains sensitive information that could otherwise be obtained only by a physical intrusion into a person's body. FAST does not perform an allowable binary search, such as a dog sniff that reveals only the presence or absence of contraband.[168] FAST does not detect the presence or absence of contraband but, rather, only a potential state of mind—the intent to commit a crime.[169] Although some commentators note that a FAST scan might indicate the existence of a criminal and guilty mind—nominally, a binary search[170]—a guilty mind is not independently a crime.[171] Unlike dog

---

164. *Klayman*, 957 F. Supp. 2d. at 32–37.

165. *Id.* at 33, 40–41. Due to its national security implications, the district court judge stayed the order of injunction preventing the collection of phone metadata pending appeal to the U.S. Court of Appeals for the District of Columbia Circuit. *Id.* at 43–44.

166. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1560–61 (2013).

167. *See* Hu, *supra* note 41, at 1481 (explaining that biometric identification systems can harvest general behavioral and biographical data that, if pieced together, could create a picture of person's personal habits and activities).

168. United States v. Place, 462 U.S. 696, 707 (1983).

169. *Supra* note 6 and accompanying text.

170. *E.g.*, Jim Harper, Florida v. Jardines*: Bolstering the Fourth Amendment*, JURIST (Oct. 31, 2012, 12:40 PM), http://jurist.org/hotline/2012/10/jim-harper-florida-jardines.php.

sniffs, which only reveal the presence or absence of contraband, FAST searches reveal not only the presence of malintent, but potentially also the existence of private medical information because of the vital signs that FAST scans.[172] Since FAST is not limited to revealing the presence or absence of contraband, it is not a binary search and therefore is excluded from the requirements of the Fourth Amendment.

Rather, FAST would fall under the Supreme Court's definition of an extra-sensory search. *Kyllo* limits extra-sensory searches that reveal intimate details of a constitutionally protected area that could not otherwise be obtained without a physical trespass by prohibiting the use of technology that is not in general public use.[173] Similar to *Kyllo*, where the use of a thermal imager had the potential to reveal intimate details of the house,[174] the use of FAST has the potential to reveal private medical details about a person.[175] Normally, this medical data could not be obtained except through a physical examination.[176] Similar to the *Kyllo* analysis, this data could customarily only be obtained by a physical trespass into a protected area because a scan of the human body that could reveal medical data is a search under the *Kyllo* analysis and is an extrasensory search.[177] Further, *Kyllo*'s exception for when the technology is in "general public use" is inapplicable to FAST[178] even though all but

171. *See generally* MODEL PENAL CODE § 2.01(1) (Proposed Official Draft 1962) ("A person is not guilty of an offense unless his liability is based on conduct which includes a voluntary act or the omission to perform an act of which he is physically capable.").

172. *Supra* notes 119–26 (delineating the medical information that is obtained from vital signs).

173. Kyllo v. United States, 533 U.S. 27, 34 (2001); *see supra* notes 82–89 and accompanying text.

174. *Kyllo*, 533 U.S. at 37.

175. *See supra* Part I.C.1.

176. Thomas Frank, *Anxiety-Detecting Machines Could Spot Terrorists*, USA TODAY, http://usatoday30.usatoday.com/news/nation/2008-09-18-bioscanner_N.htm (last updated Sept. 22, 2008) (quoting a DHS consultant that FAST is "picking up things with sensors that can't necessarily be detected by the human eye" (internal quotation marks omitted)).

177. The *Kyllo* Court emphasized what the search *could* reveal, not what the search *actually* revealed. *See Kyllo*, 533 U.S. at 35. Similarly, FAST has the potential to reveal private medical data.

178. *Id.* at 34. Justice Scalia noted that the police should not be barred from using technology that the public could use to obtain information from a protected area; therefore the police could use technology that was in the public realm to obtain the details of a protected area. *Id.* at 33–34 (holding that the advance of technology has exposed private areas to public view).

one of the sensors used in FAST is commercially available.[179] As Justice Kagan stated in her concurrence in *Florida v. Jardines*,[180] a dog is in the "general public use" but the specialized training for the dog's drug detection ability is not publically available.[181] Because FAST's specialized technology—the combined sensor package and the malintent theory algorithm—is not available to the public, *Kyllo*'s public domain exception does not apply. Therefore, a FAST scan is a search that falls under the Fourth Amendment's warrant requirement unless another exception applies.

Granted, there is an argument that there would be no search at all because people "knowingly expose[d]" their vital signs in public areas to anyone with the ability to detect them.[182] However, as noted above, this analysis is similar to that used in *Kyllo*, wherein heat was "knowingly exposed" to the curb and was detectible by a thermal imager.[183] Similar to the infrared camera used in *Kyllo*, the technology used in FAST reveals medical information concerning a person that could only otherwise be obtained through a physical intrusion into a person's body. Like the infrared camera, which "sees" through the walls of the house, FAST's sensors remotely gather, from a distance, a person's vital signs. Therefore, it is unlikely that a court would declare a FAST scan a non-search on the basis that the person "knowingly exposed" his or her vital signs for public viewing.

B. FAST Scans Do Not Fall Under an Exception to the Warrant Requirement

As a FAST scan is not an allowable binary search, and more likely an impermissible extrasensory search, it is unconstitutional unless one of the exceptions to the Fourth Amendment applies. Of the many exceptions to the warrant requirement, the administrative search exception is most applicable to a FAST scan because FAST is designed to find people with criminal intent attempting to enter

---

179. Benson, *supra* note 59; *see Kyllo*, 533 U.S. at 34, 39 n.6 (identifying the public availability of a technology as one factor in the Court's analysis).

180. 133 S. Ct. 1409 (2013).

181. *Id.* at 1418 (Kagan, J., concurring) ("[D]rug-detection dogs are highly trained tools of law enforcement, geared to respond in distinctive ways to specific scents so as to convey clear and reliable information to their human partners. They are to the poodle down the street as high-powered binoculars are to a piece of plain glass. Like the binoculars, a drug-detection dog is a specialized device for discovering objects not in plain view (or plain smell)." (citation omitted)).

182. *See* United States v. Katz, 389 U.S. 347, 351 (1967).

183. *Supra* notes 173–81 and accompanying text.

specific areas, similar to airport screening checkpoints.[184] The federal courts of appeals have routinely held that airport security measures are administrative searches due to their routine nature and the high governmental interest in preventing terrorist bombings and hijackings of airplanes.[185] Specifically, airport searches fall under the administrative search exception because their "primary goal is not to determine whether any passenger has committed a crime but rather to protect the public from a terrorist attack."[186] DHS has designed FAST to be implemented in airport security screens before using it in other operational scenarios.[187] As FAST is designed primarily as a screening tool to prevent terrorism in secure locations, it would fall under the administrative exception, and its constitutionality would rest upon the reasonableness of the search it produces.[188] However, if DHS were to employ FAST on the streets in an effort to prevent ordinary crimes, FAST falls out of the administrative search exception and must comply with ordinary Fourth Amendment jurisprudence unless another exception applies.[189]

The courts have noted that a search conducted under the administrative search exception must serve a purpose that is distinct from ordinary crime prevention.[190] Once the government shows that

---

184. *See* Gil, *supra* note 46, at 237, 246–47 (arguing that a field-test of the FAST system—MALINTENT—was valid as an administrative search or was valid as a non-search investigatory stop).

185. Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011) (emphasizing the government's need to ensure public safety at airports); United States v. Aukai, 497 F.3d 955, 958–59 (9th Cir. 2007) (requiring a substantial risk to public safety to allow suspicionless searches that go beyond the need for normal law enforcement); United States v. Albarado, 495 F.2d 799, 806 (2d Cir. 1974) (reasoning that although law enforcement does not typically detect weapons at airports, using a magnetometer to screen for weapons is a "reasonable search" given the "minimal invasion in all respects of a passenger's privacy weighed against the great threat to hundreds of persons if a hijacker is able to proceed to the plane undetected").

186. *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

187. *Supra* notes 48–50 and accompanying text (indicating that DHS has stated its intention to potentially deploy the system outside of airport checkpoints and in sporting venues and convention centers as well as on street corners).

188. *See* Gil, *supra* note 46, at 237.

189. For an analysis of FAST under other exceptions to the Fourth Amendment's warrant requirement, see *id.* The analysis of FAST under other exceptions is outside of the scope of this Comment.

190. *E.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 38 (2000) (noting that the Supreme Court has never "indicate[d] approval of a[n] [administrative search] whose primary purpose was to detect evidence of ordinary criminal wrongdoing"); New York v. Burger, 482 U.S. 691, 724 (1987) ("In the law of administrative searches . . . the government may not use an administrative inspection scheme to

its purpose is not ordinary law enforcement activities, the courts, when analyzing cases before them, employ a balancing test between (1) the governmental interest and (2) the invasion of an individual's privacy interest.[191]

1. Governmental interest

To determine if an administrative search is valid, a court will weigh the governmental need for the search against the intrusion of personal privacy. "[T]here must be a 'substantial' government interest that informs the regulatory scheme pursuant to which the inspection is made . . . [and], the warrantless inspections must be 'necessary to further [the] regulatory scheme.'"[192] The regulatory scheme must also perform the functions of a warrant by giving those searched adequate notice and limiting the scope of the searching officers.[193] Therefore, for there to be a valid governmental need: (1) the government must have a special need; and (2) the search must further that regulatory scheme by (a) providing adequate notice, (b) limiting the scope of the search, and (c) being narrowly tailored to further the special need.

a. Special need

In order for an administrative search exception to be valid, the government must have a special interest distinct from law enforcement, meaning an interest that goes beyond solving ordinary crimes and that is unique to the situation.[194] The Supreme Court has generally recognized that preventing terrorism is such an interest. In *City of Indianapolis v. Edmond*,[195] the Court commented that preventing terrorism "would almost certainly" fall under the

---

search for criminal violations."); MacWade v. Kelly, 460 F.3d 260, 268 (2d Cir. 2006) ("[A]s a threshold matter, the search must serve as its immediate purpose an objective distinct from the ordinary evidence gathering associated with crime investigation." (quoting Nicholas v. Goord, 430 F.3d 652, 663 (2d Cir. 2005))); United States v. Bulacan, 156 F.3d 963, 967 (9th Cir. 1998) (stating that the rule is "well established" that warrantless searches designed for purposes other than crime prevention may be permissible).

191. *E.g.*, *Elec. Privacy Info. Ctr.*, 653 F.3d at 10; United States v. Heckenkamp, 482 F.3d 1142, 1148 (9th Cir. 2007); United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974).

192. *Burger*, 482 U.S. at 702–03 (second alteration in original) (quoting Donovan v. Dewey, 452 U.S. 594, 600, 602 (1981)).

193. *Id.* at 703.

194. *Supra* Part I.B.1.

195. 531 U.S. 32 (2000).

administrative search exception.[196] Multiple circuit courts have held further that terrorism definitely falls under the administrative search exception.[197] However, these searches are unconstitutional when their primary purpose is to uncover evidence of "ordinary criminal wrongdoing."[198]

Although DHS contends that FAST is designed to deter terrorism at airports and border checkpoints, it is possible that DHS will expand the program to detect ordinary crimes before they are committed.[199] Under this deployment, FAST would clearly violate the Court's prohibition against allowing the administrative search exception for ordinary crime prevention.[200]

A search is not an administrative search if its *primary* purpose is to assist law enforcement with the detection and prosecution of ordinary crimes. However, a search that has an indirect or ancillary purpose of detecting ordinary crime can still qualify as an administrative search

---

196. *Id.* at 44; *see also* Chandler v. Miller, 520 U.S. 305, 323 (1997) ("[W]here the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as reasonable—for example, searches now routine at airports . . . ." (internal quotation marks omitted)); Cassidy v. Chertoff, 471 F.3d 67, 80–81 (2d Cir. 2006) (indicating that "the threat of terrorism is omnipresent" and that there is no clear limit to the government's power to conduct searches under this justification, as well as upholding searches of ferry passengers' luggage in the instant case); MacWade v. Kelly, 460 F.3d 260, 271 (2d Cir. 2006) (arguing that *Edmond* did not require the government to use checkpoint security for only an "imminent" terrorist attack and concluding that a search program to discover concealed explosives to protect mass transportation from terrorist attacks fell under the administrative search exception); *cf.* Bourgeois v. Peters, 387 F.3d 1303, 1307, 1312–13 (11th Cir. 2004) (refusing to expand the special needs doctrine to include searching for weapons at a protest site upon unfounded suspicion that radical groups were infiltrating the otherwise peaceful protest group).

197. *See, e.g.*, Corbett v. Transp. Sec. Admin., 767 F.3d 1171, 1179–80 (8th Cir. 2014) ("The [magnetometers] at airport checkpoints are a reasonable administrative search because [of] the governmental interest in preventing terrorism . . . ."); Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011) (reviewing the various circuits that have held such); *MacWade*, 460 F.3d at 275 (allowing suspicionless searches at subway entrances to deter terrorism); *cf.* Gil, *supra* note 46, at 248–49 (noting that the government has a significant interest in preventing terrorists from gaining access to government buildings, such as courthouses).

198. *Edmond*, 531 U.S. at 41 ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.").

199. *See supra* notes 48–53 and accompanying text.

200. *But see* United States v. Schafer, 461 F.2d 856, 859 (9th Cir. 1972) (finding that the reporting of inadvertently discovered contraband in the course of an otherwise valid administrative search does not invalidate an administrative search).

and be reasonable if it passes the balancing test.[201] In its current form, FAST is not designed to gather evidence; DHS specifically claims that FAST's purpose is to identify suspects for additional screening.[202] Even though FAST is designed to detect malintent, it is not designed to gather evidence for use in law enforcement proceedings. Because the government's need to prevent terrorism is significant, FAST is not a tool of ordinary law enforcement, at least with regard to airport screenings and other screenings to prevent terrorism.

If DHS were to deploy FAST as a pre-crime detection program to prevent ordinary crimes, those searches would no longer be protected by the administrative search exception and would constitute an unconstitutional warrantless search in violation of the Fourth Amendment.[203] As a pre-crime detection tool, FAST would not be permissible under *Terry v. Ohio*, which requires that law enforcement have reasonable suspicion that a person is armed and dangerous prior to searching the person.[204] A search prior to this suspicion does not fall within the protection of *Terry*.[205] FAST scans violate *Terry* because FAST scans search a person to obtain information about whether the person has malintent *before* reasonable suspicion arises. However, the government could use FAST to detect acts of terrorism.[206]

b. Furthering the regulatory scheme

The second prong of the governmental reasonableness test requires that individuals have advance notice of the search and a chance to avoid it, that the search is limited in scope and duration, and that the search is narrowly tailored to detect the special governmental need.[207]

---

201. *See* Ferguson v. City of Charleston, 532 U.S. 67, 82–83 (2001) (disallowing drug testing of patients where the immediate objective was to gather evidence for law enforcement purposes).

202. *See supra* notes 43–47 and accompanying text.

203. *See* Bourgeois v. Peters, 387 F.3d 1303, 1312–13 (11th Cir. 2004) (rejecting a city government's argument that a search designed to enforce a criminal statute banning possession of dangerous items was independent of the city's general interest in public safety and law enforcement because the purported distinction was "untenable"); *supra* note 106 (citing cases which note that the administrative search is only valid when its purpose is not to detect ordinary criminal wrongdoing).

204. Terry v. Ohio, 392 U.S. 1, 27–28 (1968).

205. *Id.*

206. *Supra* notes 201–02.

207. *See* New York v. Burger, 482 U.S. 691, 702–03 (1987); MacWade v. Kelly, 460 F.3d 260, 273 (2d Cir. 2006) requiring that an administrative search must be

i. Notice requirement

Although FAST is not designed to give notice, the courts are likely to find that a reasonable person would expect to be searched at an airport and therefore would be on notice of a FAST search. An administrative search is valid only if members of the public are aware that they will be searched and people are able to avoid the search by electing not to try to enter the secured area.[208] The notice requirement requires that the person or place being searched in the administrative search context be "advise[d]" that she is being searched.[209] Often, especially in the airport setting, passengers are intimately aware that they will be subject to a search once they enter a certain area, such as an airport security line.[210] Given the increase in the quantity and scope of security regulations after the September 11, 2001 terrorist attacks, it is "inconceivable" that airplane passengers are unaware that they must be searched before boarding airplanes.[211] Airport travelers have constructive notice that they will be subject to a form of search prior to boarding an aircraft. People who choose not to be searched may do so by opting not to fly.[212]

"narrowly tailored to achieve its purpose," be limited in duration, and provide notice of the search); United States v. Hartwell, 436 F.3d 174, 180–81 (3d Cir. 2006) (same); United States v. Marquez, 410 F.3d 612, 616 (9th Cir. 2005) (holding that a screening search in an airport is reasonable if it is a good faith effort that is narrowly tailored to detect weapons or explosives and if passengers can avoid it by choosing not to fly).

208. *See* United States v. Aukai, 497 F.3d 955, 960–62 (9th Cir. 2007) (arguing that by walking into a secured area of the airport, the respondent "subject[ed] himself to the airport screening process"). *Aukai* relied on a federal statute that authorizes security screenings of passengers and noted that the "election occurs when a prospective passenger walks through the magnetometer or places items on the conveyor belt of the x-ray machine." *Id.* at 961. *See generally* 49 U.S.C. § 44901 (2012) (requiring DHS to provide for screening of all people and cargo on passenger airplanes operating in interstate commerce).

209. *Burger*, 482 U.S. at 703. The statutory program must perform the functions of a warrant, including notice and limiting the discretion of the searching officers. *Id.*

210. *Hartwell*, 436 F.3d at 180–81 ("[A]ir passengers are on notice that they will be searched.").

211. *Id.* at 181.

212. *Id.*; *see also Burger*, 482 U.S. at 711 (rationalizing in the context of a statute requiring vehicle inspections that the statute replaced the warrant notice requirement because it placed businesses subject to the statute on notice that they were subject to search); Am.-Arab Anti-Discrimination Comm. v. Mass. Bay Transp. Auth., No. 04-11652-GAO, 2004 WL 1682859, at *3 (D. Mass. July 28, 2004) (finding that since a transit authority gave the public notice that passengers on its trains and buses would be subject to searches, it adequately gave the public an option to avoid the searches by taking alternative routes to work).

The current design of FAST is to scan people before they enter a security zone.[213] The main benefit of the pre-security screening is that people will not realize that they were being scanned.[214] In *United States v. Aukai*,[215] the Ninth Circuit was concerned that in a post-September 11th world, allowing consent for screening would enable terrorists to test the system and just elect not to fly "on the cusp of detection" until a weakness in the security checkpoint system was found.[216] The court refused to allow people to avoid being searched once they have started the security process, but the court declined to extend the power to the government to search people who had not yet attempted to go through security.[217] The Ninth Circuit also rejected the government's position that a person's consent to be searched started upon entering the airport.[218] As long as FAST is applied only to those who enter the security line—where a valid ticket is required—and not to those merely dropping passengers off, passengers will have notice that they will be searched once they are in a secure area.

Constitutional issues would arise, however, if DHS proposed to use FAST beyond airport security screening and on the streets to detect ordinary crimes. Airport screenings qualify as administrative searches only because their primary purpose is to protect the public from terrorist attacks rather than to detect ordinary crimes, and the notice requirement of a warrant is met because people constructively know that they will be searched when they fly.[219] This notice prong would not be satisfied if FAST were used outside of places people expect to be searched—such as on the streets of their local towns.

ii. Limited in scope

A FAST scan is limited in scope because it takes only a few seconds to complete—less time than current airport security screenings—and officers have no discretion regarding who will be screened. An

213. *Supra* notes 39–41 and accompanying text.
214. *Supra* notes 39–41 and accompanying text.
215. 497 F.3d 955 (9th Cir. 2007).
216. *Id.* at 960–61.
217. *Id.*
218. *Id.* at 961 n.9. The court admitted that it may be possible for the government to argue that a person consented to a search merely by entering the airport facility, but that issue was not before the court at the time. *Id.* at 961 n.8 (declining to speculate on whether the secure area "extend[s] from the airplane boarding gate to the street door").
219. Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011).

administrative search is reasonable only if it is also limited in duration and scope.[220] The scope of an administrative search must be limited in its scope to reduce the fear and stigma associated with being singled out for screening.[221] The courts have upheld administrative searches only when they do not detain suspects for an extended period of time and when the officers search everyone instead of arbitrarily searching individuals.[222] When every passenger is searched, the searching officer has no discretion to choose who to search, which prevents the officer from using improper motives as the basis to search certain people.[223] When the search does detain passengers for lengthy periods, the courts usually find that searches do not invade heavily on a person's individual privacy and are therefore constitutional.[224]

FAST easily satisfies the requirement that a search be limited in scope because the officers have no discretion in choosing whom to scan: everyone is scanned upon entering the scan zone.[225] Further, the system is designed to speed up the security process to a few

---

220. *See* Illinois v. Lidster, 540 U.S. 419, 425 (2004) (citing Florida v. Royer, 460 U.S. 491, 497 (1983)) (finding that highway stops of motorists were not presumptively unconstitutional when the stops were brief and merely asked the individuals stopped to help apprehend a fugitive).

221. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 559–60 (1976) (expounding that routine checkpoint vehicle searches are minimally intrusive when the stopping officer stops every car that passes through the checkpoint); MacWade v. Kelly, 460 F.3d 260, 273 (2d Cir. 2006) (characterizing searches by uniformed officers "out in the open" as ones that are minimally intrusive because they do not make people fear additional screenings); United States v. Hartwell, 436 F.3d 174, 180 (3d Cir. 2006) ("Since every air passenger is subjected to a search, there is virtually no 'stigma attached to being subjected to search at a known, designated airport search point.'" (quoting United States v. Skipwith, 482 F.2d 1272, 1275 (5th Cir. 1973))).

222. *See, e.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451–53 (1990) (sobriety checkpoints); *Aukai*, 497 F.3d at 962–63 (airport searches); *MacWade*, 460 F.3d at 273 (subway searches).

223. *See* Am.-Arab Anti-Discrimination Comm. v. Mass. Bay Transp. Auth., No. 04-11652-GAO, 2004 WL 1682859, at *4 (D. Mass. July 28, 2004) (approving of a searching scheme in a mass transit system where all bus and train riders were subject to search once they entered a secure zone).

224. *Sitz*, 496 U.S. at 448 (finding that a twenty-five-second sobriety checkpoint stop is minimally intrusive); *Aukai*, 497 F.3d at 963 (reasoning that although an eighteen minute airport security screen was "longer" than screenings in other situations, the length was appropriate to determine whether the individual subject to the search was carrying weapons or other contraband).

225. *See* DHS FAST PRESENTATION, *supra* note 6, at 2 (indicating that DHS designed FAST to increase the speed of security screenings while minimizing the effect on passengers). The system would not work unless every person was scanned.

seconds, eventually reducing the time burden to no detention at all.[226] Therefore, FAST is appropriately limited in the scope of its scans and meets this requirement.

iii. Narrowly tailored

FAST is not narrowly tailored to prevent terrorist activities because it is possible that it can be circumvented if a person is unaware that a crime is being committed or even believes that the act being taken is a not crime. An administrative search is narrowly tailored so long as it "is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives . . . [and] is confined in good faith to that purpose."[227] However, it does not need to be the least intrusive measure possible.[228] The U.S. Court of Appeals for the District of Columbia Circuit held that the need to protect the public from airplane hijackings is "particularly acute" and implied that any measures to detect and deter attempts to carry explosives aboard a plane would be allowed.[229] However, the court still noted that to use the millimeter wave scanner at a checkpoint, it must be designed to "deter[] attempts to carry aboard airplanes explosives in liquid or powder form."[230]

FAST is designed to detect malintent—not explosives or weapons. Unlike magnetometers, which inform security officials of the presence or absence of metallic objects (a binary search), FAST does neither: FAST cannot detect weapons or explosives but can detect only the intent to commit a crime.[231] Further, FAST cannot distinguish between intent to commit a *terrorist* action and intent to commit a *garden-variety* crime. Therefore, FAST does not satisfy the

---

226. *See supra* note 43 and accompanying text.

227. *Aukai*, 497 F.3d at 962 (internal quotation marks omitted).

228. Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011) (alterations in original) (quoting City of Ontario v. Quon, 560 U.S. 746, 763 (2010)).

229. *Id.* (quoting City of Indianapolis v. Edmond, 531 U.S. 32, 47–48 (2000)).

230. *Id.*

231. *See supra* notes 6, 57 and accompanying text (defining "malintent" as intent to commit a crime); *see also* Gregg Henriques, *Attributions of Malintent: A Dangerous Form of Attribution*, PSYCHOL. TODAY (Apr. 7, 2013), http://www.psychologytoday.com/blog/theory-knowledge/201304/attributions-malintent (defining "malintent" as "having harmful or malicious intent").

Supreme Court's requirement that administrative searches have a unique government need apart from ordinary law enforcement.[232]

However, having the intent to commit a crime, without more, does not provide enough for law enforcement to act.[233] Although DHS has not released specific information on the results of its FAST tests, it is likely that the detection of malintent would show equally a person intending to commit a terrorist attack and a drug courier—the former falling under the special needs exception, and the latter falling under ordinary crime prevention.

Critics are concerned that FAST could mistakenly flag a person who was flying to see a paramour, despite DHS's assertions that this would be impossible.[234] Further, unlike backscatter or millimeter wave technology[235] that can detect items of any composition hidden against the body, FAST can do neither if a suspect's state of mind lacks malintent.[236] The detection of a state of mind is not tailored to further the regulatory scheme of preventing acts of terrorism; rather, it could detect the routine crime of drug smuggling and possibly the

---

232. *See Edmond*, 531 U.S. at 38 (explaining that the Court has never approved of administrative searches used for detecting ordinary crimes); *see also* New York v. Burger, 482 U.S. 691, 724 (1987) (Brennan, J., dissenting) (citing precedent for this requirement).

233. *See supra* note 171 and accompanying text (explaining that a person does not commit a crime by merely having a guilty thought).

234. *See supra* note 56 and accompanying text (expounding that DHS could find evidence of malintent where an individual has no criminal aspirations and instead has guilty thoughts for purposes independent of criminal intent).

235. Backscatter scanners, which are no longer used in airports, send scattered x-rays at a person and are able to provide high resolution images of a person in their nude form. *Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening)*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/airtravel/backscatter (last visited Dec. 21, 2014). Active millimeter wave technology scanners (the chamber that spins two antenna panels around the scannee), which are actively used in airports, use microwaves or ionizing radiation to reflect off a person, enabling security officials to construct a three-dimensional image of the scannee and see any shapes on the body that do not belong. *Assessment of Checkpoint Security: Are Our Airports Keeping Passengers Safe? Hearing Before the Subcomm. on Transp. Sec. & Infrastructure Prot. of the H. Comm. on Homeland Sec.*, 111th Cong. 74 (2010) (statement of Mitchel J. Laskey, President and CEO, Brijot Imaging Systems, Inc.). A newly developed passive millimeter wave technology merely measures the naturally emitted millimeter waves from the body and detects objects that obstruct those waves. *Id.* This project is in use in foreign countries but still under testing as of 2010 in the United States. *Id.*

236. *See* Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011) (highlighting that millimeter wave scanners can deter terrorists from bringing explosives in liquid or powder form onto airplanes); *see also supra* note 46 and accompanying text (distinguishing between a FAST scan that detects malintent and a metal detector that detects the physical presence of a metal object).

arguably legal act of cheating on one's spouse.[237] Since FAST only detects malintent, it would theoretically not work if a person was unknowingly carrying a concealed bomb into a secured area, allowing the program to be circumvented. It is also unclear whether FAST could detect a terrorist who thought that he was justified in his actions and therefore not committing a crime.[238] As such, the FAST system is not narrowly designed to further the regulatory scheme of preventing acts of terrorism since its primary purpose is to scan a person's mind for potential criminal mens rea.[239] Also, it is ineffective at detecting and deterring attempted terrorist attacks. Therefore, FAST is not narrowly tailored to the government's purpose of preventing terrorist acts and fails this part of the administrative search requirement.[240]

2. Intrusion of personal privacy

Administrative searches must be balanced between the governmental need for the search and the search's intrusion upon a

---

237. *See supra* notes 56–57 and accompanying text (comparing critics' concerns that the system is not narrowly tailored to DHS's statement that FAST sensors can distinguish between malintent and mere anxiety). Although adultery technically remains illegal in twenty-one states, Jolie Lee, *New Hampshire Senate Votes to Repeal Anti-Adultery Law*, USA TODAY (Apr. 17, 2014, 4:39 PM), http://www.usatoday.com/story/news/nation-now/2014/04/17/anti-adultery-laws-new-hampshire/7780563, it is now rarely enforced after the Supreme Court's decision in *Lawrence v. Texas*, 539 U.S. 558 (2003), as shown with the recent admission by General David Petraeus, who admitted to an adulterous relationship in Virginia where adultery remains a criminal offense, Ethan Bronner, *Mass. Among 23 States Where Adultery Is a Crime, but Rarely Prosecuted*, BOS. GLOBE (Nov. 12, 2012), http://www.bostonglobe.com/news/nation/2012/11/15/adultery-still-crime-states-including-mass/KiIPGRcFnAeT4CGmenFTKM/story.html.

238. *See supra* note 58 and accompanying text (emphasizing that malintent encompasses intent to commit a crime, which may be lacking in terrorists who do not believe their activities are criminal in nature).

239. *See supra* notes 231–32 and accompanying text. Proponents are likely to argue that the millimeter wave scanners similarly can detect ordinary criminal activity, such as attempts to smuggle drugs tapped to the body. However, courts have emphasized that searches must be designed in "good faith" to further the regulatory scheme. *See* United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007). However, by the definition of "malintent," FAST is designed to detect a *criminal mindset*, not one of *terrorism*, and therefore is not tailored to further the regulatory scheme. *See supra* notes 6, 199–201 and accompanying text.

240. United States v. Edwards, 498 F.2d 496, 500 (2d Cir. 1974) (finding that administrative searches must have a "good faith" purpose of detecting and preventing the special need (quoting United States v. Bell, 464 F.2d 667, 675 (2d Cir. 1972)).

person's individual privacy.[241] A person has a heighted privacy interest in his or her person and medical records, even when a third party holds those records.[242] Although the remoteness of the FAST scan make it minimally intrusive, the appropriate test is not how physically intrusive the scan is but, rather, how much private information is revealed.[243] Generally, when a governmental request requires disclosure of a person's medical records, the request is allowed when there is a governmental need for the *medical records* themselves.[244] The courts have rarely looked at situations when the government directly obtained medical information from a person, the few situations being for blood tests following a driving under the influence arrest.[245] Even in *McNeely*, the Supreme Court held that a warrant was required before the police could perform a nonconsensual blood test to determine an arrestee's blood alcohol content even though alcohol metabolizes in the blood over time.[246] A straight blood test, which is able to obtain the complete information obtained in a blood sample, is more similar to a FAST search that can obtain all the information of a vital signs scan. As such, a FAST scan should trigger the same heightened privacy interests as other tests that can discover medical data, similar to *McNeely*.[247] Therefore, a FAST scan would intrude on a person's heightened privacy rights.

The Court has required a warrant to obtain medical evidence even when a traditional exception to the warrant requirement might otherwise apply.[248] The one time that the Supreme Court allowed a warrantless medical test that used DNA swabs, it did so because of the

---

241. *Supra* note 191 and accompanying text (explaining that courts balance the governmental interest against the individual's privacy interest when determining if an administrative search is reasonable).

242. Doe v. Broderick, 225 F.3d 440, 443, 449–51 (4th Cir. 2000) (concluding that a law enforcement officer violated the petitioner's reasonable expectation of privacy in his patient records at a methadone clinic where the officer searched the records in the clinic file room without a warrant); *see supra* Part I.C (detailing that individuals have a heightened privacy interest in personal medical information).

243. United States v. Kyllo, 533 U.S. 27, 38 (2001).

244. *See* Whalen v. Roe, 429 U.S. 589, 598, 602 (1977) (finding that the State of New York had a vital interest in controlling the distribution of Schedule II narcotics and therefore could request doctors provide the State with narcotics prescription records).

245. *See, e.g.*, Missouri v. McNeely, 133 S. Ct. 1552, 1556 (2013) (rejecting the opportunity to create a per se exigency exception to the warrant requirement for nonconsensual blood testing in drunk driving cases).

246. *Id.* at 1560–61.

247. *Supra* notes 127–38.

248. *Supra* Part I.C.2 (underscoring that medical information is highly sensitive and thus highly private).

practical concerns of solving crimes rather than the given reason of an administrative booking.[249] Even though an arrestee had a minimal expectation of privacy in a DNA swab, the Court specifically noted that the test would not be able to obtain any medical information from the swab other than a person's identity since the swab only obtained noncoding DNA sequences.[250] However, no court has addressed the mass gathering of medical information under the administrative search exception.[251]

A FAST scan operates by revealing medical data directly from the scannee.[252] Since the question of the government obtaining medical data generally falls outside of the bounds of normal exceptions to the warrant requirement, courts will likely scrutinize the FAST program and the data obtained through it under a Fourth Amendment analysis.[253] Typically, medical data has heightened protections but can be requested by the government only when there is a compelling governmental need for the medical records and proper protection of those records.[254] Similarly, the government has no need for the medical data that it is obtained from a FAST scan beyond the need to aggregate the data to predict the scannee's state of mind. The government would obtain mass medical information on everyone who is scanned instead of information pertaining to specific individuals or health concerns.

Additionally, FAST identifies people for further screening only to determine if the person poses a threat. The U.S. District Court for the District of Columbia in *Klayman* held that the NSA's mass collection of private information infringed upon the privacy interests of telephone users despite the national security concerns expressed

---

249. *See* Maryland v. King, 133 S. Ct. 1958, 1970–71 (2013) (explaining that an officer should know a suspect's criminal history during routine booking).

250. *Id.* at 1979. *See generally supra* note 139 (discussing the Supreme Court's decision in *King*).

251. Recently, however, the U.S. District Court for the District of Columbia addressed the Fourth Amendment implications of an NSA program that mass collected phone metadata from the public. *See infra* notes 255–58 and accompanying text.

252. *See supra* notes 118–26, 167 and accompanying text (noting that the sensor packages on FAST can obtain sensitive medical information on the scannee).

253. *See supra* notes 118–26 and accompanying text.

254. Doe v. Broderick, 225 F.3d 440, 450–51 (4th Cir. 2000) (finding no need existed when a law enforcement officer searched methadone treatment records to find a suspect for a jewelry heist); Gen. Motors Corp. v. Dir. of Nat'l Inst. for Occupational Safety & Health, 636 F.2d 163, 165–66 (6th Cir. 1980) (allowing government access to records when there was a governmental need to research factory safety conditions and the government could properly protect the records it accessed).

by the government.[255] The court downplayed the national security issues because the government could not provide any example of where it had identified a terrorist using anything other than traditional investigative means.[256]

Similarly, FAST will only identify suspects for further screening and will not independently prevent airplane hijackings.[257] FAST is merely a tool to indicate whether people should be screened further—the government must still identify threats through subsequent traditional measures.[258] Therefore, under the *Klayman* analysis, FAST's invasion of individuals' privacy interests would outweigh the governmental interest in preventing terrorism since FAST would not detect terrorist attempts but would merely identify people for further screening.[259]

Courts have condoned the use of intrusive technology when the technique is narrowly tailored to the regulatory scheme and adequate safeguards are taken. In *Electronic Privacy Information Center v. Department of Homeland Security*,[260] the D.C. Circuit analyzed the implications of Transportation Security Administration (TSA) employing Advanced Imaging Technology ("AIT") (millimeter wave and backscatter scanners) at airport screenings, which originally displayed images of a scannee's nude body.[261] The court held that these scans were not too intrusive: passengers could opt for a pat down instead of the scan, and the scannee's privacy was protected because the images produced were distorted and would subsequently be deleted.[262]

Currently, DHS has not explained how FAST data would be protected.[263] To protect a person's privacy, DHS would have to ensure that the information obtained through a FAST scan cannot be retained in any manner and that the data cannot be linked to an identifiable person during the scan, similar to the testing

255. Klayman v. Obama, 957 F. Supp. 2d 1, 40–41 (D.D.C. 2013).

256. *Id.* at 40.

257. *See supra* notes 43–47 and accompanying text (identifying that FAST only identifies people for additional screening).

258. *Supra* notes 43–47 and accompanying text.

259. *Supra* note 41 and accompanying text.

260. 653 F.3d 1 (D.C. Cir. 2011).

261. *Id.* at 10–11.

262. *Id.* at 10. The court did not address whether using AIT was a "virtual strip search" in violation of Islamic beliefs against revealing a person's nude body because such a person was not properly before the court. *Id.* at 9.

263. *See supra* notes 65–66 and accompanying text.

procedures.[264] The data would further need to be deleted after the determination of malintent was made, which is more difficult than the AIT image since FAST must aggregate data from different scans and compare it against the scannee's baseline.[265] Although DHS claims that each scannee develops his or her own baseline,[266] DHS cannot retain scans to develop a community baseline to which scannees are compared, as retention of data would not protect the scannee's privacy interest.

FAST's invasion of personal privacy will not outweigh the government's need to prevent terrorism. The Supreme Court has noted that individuals have a heightened interest in their medical records, and lower courts have held that the mass gathering on data must directly serve the governmental need. FAST does neither. Instead, FAST directly obtains medical data from scannees and because it has a low accuracy rate and could be easily circumvented, it is not effective at detecting terrorist activities. Any detection of terrorist attempts, even with FAST, will still be done by the already highly effective screening techniques employed today. As such, even if the government met its requirements under the administrative search exception, the invasion of personal privacy outweighs the governmental need, rendering FAST unreasonable under the administrative search exception.

CONCLUSION

FAST is a system that is designed to scan the body's vital signs and, based on the aggregate data, to determine whether a person has malintent—the intent to commit a crime. Although FAST is currently in the developmental phase, DHS intends to deploy the system to airports, border crossings, and potentially in high risk areas, such as stadiums. FAST is a pre-screening tool: its purpose is merely to identify individuals to be subjected to more rigorous screening techniques, and by itself, FAST is not able to provide probable cause for an arrest.

---

264. *See supra* notes 67–68 and accompanying text; *see also Elec. Privacy Info. Ctr.*, 653 F.3d at 10 (determining that TSA has taken precautions to protect an individual's privacy in the context of AIT, such as distorting the product of an AIT scan and deleting it as soon as the individual has been cleared and permitting passengers to opt-out of an AIT scan and elect the traditional pat down instead).

265. *Cf. Elec. Privacy Info. Ctr.*, 653 F.3d at 10 (highlighting TSA's privacy measures of deleting the images created by the millimeter wave scanners).

266. *See supra* notes 30–34 and accompanying text.

In the terrorism context, the governmental interest must be weighed against an individual's right to privacy. FAST scans implicate two privacy interests: personal medical data, to which the Supreme Court has given heightened protection, and mass data collection, an act which some courts suggest violates the Fourth Amendment.

However, FAST scans will not violate the Fourth Amendment if the government uses certain safeguards: (1) the person subject to the scan is on notice that the scan it about to take place, (2) the scan is limited in scope, and (3) the scan is narrowly tailored to advance the governmental interest. If a FAST scan meets these requirements—such as by only being used at airports when there is viable intelligence that a specific flight will be targeted by terrorism, by placing those on notice seeking to be on that flight that they are subject to behavioral scanning, and by limiting its use to only those who seek to board the flight—then the search may be reasonable. However, due to the secrecy surrounding FAST, it is unclear whether DHS will limit FAST in such a way.

If DHS were to deploy the system in cities to detect crimes before the crimes are committed, it would place FAST outside of the administrative search exception and into the warrant requirement of the Fourth Amendment. The government may use a search method that is more intrusive than another method as long as the method chosen is minimally intrusive under a Fourth Amendment analysis. Currently, the traditional screening methods are effective, as evidenced by the scarcity of terrorist acts conducted on airplanes, and to satisfy the requirements of warrantless searches, FAST itself must be instrumental in deterring or preventing terrorist attacks. The program is also not narrowly tailored to detect terrorism because it is designed to detect malintent, which could range from covertly visiting one's paramour, to drug smuggling or terrorism. As such, the program is not narrowly tailored to the regulatory scheme that it is promoting.

Having "malintent" is not a crime itself, as thoughts alone are not crimes until there is some action upon them. In 1949, George Orwell feared that the government would detect and punish thought-crime by 1984; Orwell was prescient in his prediction, as the Department of Homeland Security is currently developing a system to detect such thoughts. Fortunately, the Supreme Court has interpreted the Fourth Amendment in a way that would prevent the government from employing such a system and lead the United States into an Orwellian future.