DUKE LAW SCHOOL

Testimony and Statement for the Record of

Nita Farahany
Professor of Law, Duke Law School
Research Professor of Genome Sciences & Policy,
Institute for Genome Sciences & Policy

Hearing on
"What Facial Recognition Technology
Means for Privacy and Civil Liberties"

Before the

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

July 18, 2012
226 Dirksen Senate Office Building
Washington, DC

PREPARED STATEMENT OF NITA A. FARAHANY

Senate Judiciary Subcommittee on Privacy, Technology, and the Law:
"What Facial Recognition Technology Means for Privacy and Civil Liberties"

July 18, 2012

Prepared Statement of Nita A. Farahany, Professor of Law, Professor of Genome Sciences and Policy, Duke University, Durham, NC

Chairman Franken, Ranking Member Coburn, and distinguished members of the Subcommittee. Thank you for the opportunity to express my views about facial recognition technology, and its implications for privacy and civil liberties. My name is Nita Farahany. I am a Professor of Law and Research Professor of Genome Sciences and Policy at Duke University, and my research focuses on the ethical and legal implications of emerging technologies. I am also a member of the Presidential Commission for the Study of Bioethical Issues. I appear before you today in my individual, scholarly capacity.

I will focus my comments on the legal and constitutional implications of facial recognition technologies. I hope to show that, as a general matter, law enforcement use of these technologies is not, in itself, a Fourth Amendment search, let alone an unreasonable one. Although the Court has not yet addressed facial recognition technology, the doctrine regarding analogous identifying information and "open fields" supports this view.

I. Facial Recognition Technology and Biometric Identifying Information

I will begin by explaining why I believe that law enforcement use of facial recognition technology is not a Fourth Amendment search, let alone an unreasonable one, and I will explain how Supreme Court doctrine is consistent with this view. Because the Fourth Amendment safeguards the right of the people to be secure against unreasonable searches and seizures by the government—but not by private or commercial actors—my remarks will focus on law enforcement use of this technology.

A. Facial Recognition Technology in Context: Identifying Information

Facial recognition technology uses software to try to match one's facial characteristics (such as the distance between eyes, the bridge of the nose, cheekbones, and other facial topography) with an existing database of facial data to identify an individual.[1] As the technology has developed, the accuracy of identity matching has improved by

[1] Chandrakant D. Patel et al., Biometrics in IRIS Technolgy: A Survey, 2 International Journal of Scientific and Research Publications 3 (2012), *available at* (http://www.ijsrp.org/print-journal/ijsrp-jan-2012-print.pdf#page=5) (last accessed July 14, 2012).

capturing biometric features of faces such as skin texture, and by overcoming previous hurdles posed by dim lighting and subject movement with infrared imagery.[2] Facial recognition technology is part of a broader class of identification technology, which uses the physical characteristics of an individual to match identity.[3] Other biometric identification technologies, for example, fingerprinting and iris scans, are already being used by law enforcement.[4] In fact, police forces across the country are rolling out new mobile investigative devices, some of which simply attach to the back of an iPhone, that can scan a fingerprint, an iris, or a face, and compare the results against existing databases.[5] These biometric devices and techniques add more precision to the vast array of identifying information investigators regularly obtain about individuals.[6]

A novel feature of facial recognition technology is that the first step of the process—scanning a face of interest—is usually done from a distance and without the awareness of the individual being scanned. The technology does not require physical contact, close physical proximity, or physical detention of an individual to scan their face. Infrared imagery even allows scanning to occur while a person is moving freely and is in dim lighting.

Facial recognition technology captures the sort of identifying information that is the bread and butter of law enforcement: information about the characteristics, physical likeness, and other descriptive features of a suspect.[7] It is routine practice for investigators to collect identifying information from individuals including their name, birth date, weight, height, clothing size, shoe size, blood type, and traces of shed DNA.[8] Whether collected through police-targeted or automatic photographing, facial recognition technology collects identifying evidence about individuals, a class of evidence that has traditionally received only minimal constitutional protection.

The second step of the process—comparing the scanned face to an existing database of photographs to find a match—is akin to the now-commonplace use by law enforcement of other identifying databases. Police routinely check local and national databases to find the identity of individuals by using their license plates, social security numbers, fingerprints, iris scans, and DNA to probe databases that contain such information. And all of this is nothing more than an automated version of what police have done for centuries: compare information acquired in the world with information held at police headquarters, looking for a match.

---

[2] Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS.COM (http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm) (last visited Dec. 4, 2011).

[3] *See* SUBCOMM. ON BIOMETRICS, NAT'L SCI. & TECH. COUNCIL, PRIVACY & BIOMETRICS: BUILDING A CONCEPTUAL FOUNDATION 4 (2006), *available at* http://www.biometrics.gov/docs/privacy.pdf (defining biometrics as "automated methods of recognizing an individual based on measurable biological . . . and behavioral characteristics").

[4] *See id.* at 15-17 (describing existing technologies for such biometric methods).

[5] Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL ST. J. DIGITS BLOG (July 13, 2011, 7:56 AM), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works.

[6] *See* Nita A. Farahany, *Incriminating Thoughts*, 64 STANFORD L. REV. 351, 368-70 (2012).

[7] *Id*. at 368.

[8] *Id.*

Neither the first step—scanning—nor the second step—querying government databases—implicates individual interests safeguarded by the Fourth Amendment. Neither step is properly characterized as a Fourth Amendment "search," let alone an "unreasonable" one, because under current law, neither step intrudes upon a legally cognizable privacy interest.

B. Scanning and Database Queries are Not Fourth Amendment "Searches"

a. Scanning from Afar

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[9] A Fourth Amendment search only occurs when the government intrudes upon a legally cognizable interest of an individual. Neither scanning an individual's face in public afar, nor querying a database to see if there is a match, intrudes on a cognizable privacy interest of an individual, so neither step constitutes a Fourth Amendment search.

If the police use facial recognition technology to scan an individual's face while in a public place, and that individual is not detained or touched as he is scanned, then no Fourth Amendment search has occurred. Neither his person nor his effects have been disturbed, and he lacks any legal source to support a reasonable expectation that his facial features will be hidden from government observation.[10] He has chosen to present his face to the world, and he must expect that the world, including the police, may be watching. Cameras and machines may now be doing the scanning, but for constitutional purposes, this is no different from an alert police officer "scanning" faces in a public place. This has never been thought to be a Fourth Amendment search.

By analogy, if the police observe an individual while he in public, and then return to the police station to flip through mug shot books to identify the individual they saw, no Fourth Amendment search or seizure has occurred. When the individual appeared in a public place, he relinquished his privacy interest in his seclusion. By subsequently observing the individual or comparing him against mug shot books, the police have not intruded on any legal interest retained by the individual. When an individual voluntarily forgoes seclusion, he cannot insist that the police avert their eyes.[11]

---

[9] U.S. CONST. amend. IV.

[10] Whether an expectation of privacy is reasonable or not has always turned on bodies of law outside of the Fourth Amendment. Privacy expectations are reflected in laws or societal norms, so a reasonable expectation of privacy "must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *See* United States v. Jones, 132 S. Ct. 945, 951 (2012) ("[O]ur very definition of 'reasonable expectation of privacy' . . . we have said [is] an expectation 'that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understanding that are recognized and permitted by society.'" (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1988))).

[11] *See* California v. Greenwood, 486 U.S. 35 (1988) (holding that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home).

If the police were to use sense-enhanced technology to surreptitiously peer through the walls of a person's home, the police will intrude upon his real property interests and seclusion he has sought by taking refuge in his home.[12] Those interests support a reasonable expectation of privacy that an individual can exclude the police from surreptitiously observing him while secluded from public view inside his home. Because his reasonable expectation of privacy will be invaded if the police observe him this manner, a Fourth Amendment search will have occurred. Yet notice a crucial difference here between facial scanning in public and spying on an individual while inside their home: to obtain the facial scan, the police do not in any way invade the personal security or property of the individual.[13] They merely observe the individual from afar, in public, and capture the image that they see.[14] This does not constitute a search.

But even if it did constitute a search, it would likely be a constitutionally reasonable one, consistent with the Fourth Amendment. An unreasonable search occurs when the degree of insult or intrusion of an individual's legal interest outweighs the societal interest in the evidence being sought. So if the police surreptitiously observe an individual inside his home, the search will only be unreasonable if the degree of intrusion on the individual outweighs the societal need for the evidence sought. Since the Court primarily uses property rights to inform Fourth Amendment privacy interests, it likewise measures the intrusiveness of the search by assessing the physical intrusion upon the property, instead of the personal indignity that one may have endured by having their personal information revealed. Because protection of the home receives the most stringent Fourth Amendment protection, even a legitimate societal need for observing an individual inside their home is unlikely to be found reasonable.[15] By contrast, searching or seizing a person's likeness by scanning their face from afar does not interfere with their personal security or a right to exclude others they may otherwise enjoy. No physical violence or even physical interference occurs: Mere observation is not tantamount to a search, and certainly not an unreasonable one.

---

[12] *See* Kyllo v. United States, 533 U.S. 27 (2001) (finding the use of thermal imaging to scan a person's home to be a Fourth Amendment "search").

[13] E.g., Florida v. Riley, 488 U.S. 445 (1989) (holding that no Fourth Amendment search had occurred when a police helicopter flew overhead at low altitude a greenhouse and the pilot looked through a hole in the roof of the greenhouse and saw drugs being grown inside); California v. Ciraolo, 476 U.S. 207 (1986) (finding that aerial surveillance of a person's yard blocked from view by an outer fence because the Fourth Amendment does not require that police "shield their eyes when passing by a home on public thoroughfares," so the surveillance was not a search when it took place from a public place); Dow Chemical v. United States, 476 U.S. 227 (1986) (determining that the taking of photography from navigable airspace was not a Fourth Amendment search).

[14] *See* generally Orin S. Kerr, *An Equilibrium Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 522-29 (2011) (discussing Fourth Amendment "open fields" cases that allow surveillance of the curtilage of one's home).

[15] *See* Nita A. Farahany, *Searching Secrets*, 160 U. Penn. L. Rev. 1239, 1255 (2012), citing *Payton v. New York*, 445 U.S. 573, 585 (1980) ("[P]hysical entry of the home is the chief evil against which the Fourth Amendment was directed." (quoting United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972))); Mincey v. Arizona, 437 U.S. 385, 391 (1978) (holding that one does not forfeit her Fourth Amendment rights to her home by committing a crime); Alderman v. United States, 394 U.S. 165, 171-72 (1969) (linking property rights to the ability to raise a motion to exclude evidence based upon the Fourth Amendment).

b. Probing A Database

Is using a captured image to query a photographic database for a match a Fourth Amendment search? Just as a criminal suspect lacks a cognizable legal basis to complain when the police peruse mug shots at the police station, neither can an individual successfully claim that a police query of a photographic database constitutes a search of *their* persons, houses, or effects.

If the information within the database and the probe used to search it have been lawfully collected, there is no additional Fourth Amendment interest that a claimant has in preventing the police from matching their identity.[16] Ultimately, the privacy concern usually advanced regarding the inclusion in or probing of forensic databases is whether an individual has a right to *secrecy* of identifying information. But the Court has never recognized a Fourth Amendment privacy interest in the secrecy of identifying information.[17] So the probe of a photographic database is not properly considered a separate Fourth Amendment search.

c. Scanning During "Stops"

The police might instead choose to use facial scanning technology during a brief investigative stop, which requires a slightly different constitutional analysis. Beginning with *Terry v. Ohio*,[18] the Court has held that if a police officer has a reasonable suspicion that someone has committed, is committing, or is about to commit a crime, the officer may detain the individual without a warrant for a brief investigative stop. While such stops are Fourth Amendment "searches" and a person is "seized" while they are detained, a warrantless stop based on reasonable suspicion may nevertheless be a reasonable search and/or seizure.

During a *Terry* stop, the police may require an individual to disclose his identity,[19] and a facial recognition scan for identification is not meaningfully different. Indeed, a suspect can be "arrested and prosecuted for refus[ing]" to disclose his identity during a stop based on reasonable suspicion.[20] As the Court has explained, states may require a suspect to disclose his name during an investigative stop because the individual privacy interest in identity is negligible compared to the legitimate government interests promoted by the inquiry.[21]

---

[16] See, e.g., Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 20 (2008) ("The Fourth Amendment does not require governments to discard any information they have already lawfully collected.")

[17] *See* Nita A. Farahany, *Searching Secrets*, 17, at 1277-82 (discussing Fourth Amendment doctrine concerning identifying information); Nita A. Farahany, *Incriminating Thoughts*, supra note 6, at 368-72 (discussing the category of identifying evidence and constitutional protections of the same).

[18] 392 U.S. 1 (1968).

[19] Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004).

[20] *Id.* at 186-87 (citation omitted).

[21] *See id.* at 188 (noting that the "stop and identify" statute at issue in the case served the useful purpose of increasing the likelihood that a suspect would actually disclose his identity to a police officer).

If a police officer detains an individual based on reasonable suspicion, using facial recognition technology during that stop would not meaningfully change the Fourth Amendment reasonableness of the search and seizure. The individual privacy interest that the Court recognizes during "stop and frisk" detentions is the personal security the individual and an interest against interference with his free movement, not the secrecy of their personal information or his personal identity. In other words, the Court has not included secrecy of personally identifying information as a relevant privacy interest in determining the reasonableness of a "stop and frisk" detention.[22] If the police can take the more intrusive step of requiring a suspect to state his name, it can surely take the less intrusive approach of connecting a name to the face automatically.

In fact, when it comes to identifying information, the Court has held that individuals have minimal, if any, expectation of privacy in the secrecy of their identifying information.[23] This is because the Fourth Amendment provides no protection for what "a person knowingly exposes to the public, even in his own home or office."[24] The physical characteristics of a person's face, its shape and contours are constantly exposed to the public, so no person can have a reasonable expectation that others will not observe his facial features. Indeed, the Court has held that compelling a suspect to provide physically identifying information—such as fingerprints[25] or voice exemplars[26]—is usually reasonable because such techniques intrude upon no cognizable individual interest. A facial scan is far less intrusive than either of these. Lower courts have held similarly in other identification and location-determination cases, even including the use of beepers to pinpoint location.[27] In short, in each of these identifying-information cases, the Court has held that the relevant individual interest at stake is in personal security or privacy as seclusion, but has not acknowledged a privacy interest in keeping personal information a secret.

The measure of personal intrusion during an investigative stop using facial recognition scanning will likely be the length of the detention and the physical intrusiveness of the

---

[22] For example, the Court in *United States v. Dionisio*, 410 U.S. 1 (1973), noted that

> the Fourth Amendment provides no protection for what "a person knowingly exposes to the public, even in his own home or office . . . ." The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. . . . No person can have a reasonable expectation that others will not know the sound of his voice . . . .

Id. at 14 (first alteration in original) (citation omitted) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[23] *See* Farahany, supra note 17.

[24] *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (describing the reasonable expectation that others will be familiar with one's physical features).

[25] *See* Davis v. Mississippi, 394 U.S. 721, 727 (1969) ("Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search.").

[26] *See Dionisio*, 410 U.S. at 14 ("No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.").

[27] *See* Recent Development, *Who Knows Where You've Been?: Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 314-15 (2004) (describing *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004), which held that pinpointing one's location or movement through one's beeper is not subject to a reasonable expectation of privacy).

search techniques employed. If by using such technology the police held an individual for longer, or required that he pose in a compromising or otherwise physically arduous manner, then *those* actions could render the search more intrusive and affect its reasonableness. But since the police can use facial recognition software unobtrusively and almost instantaneously, its use should not change the constitutional calculus of a *Terry* stop or convert an otherwise reasonable search and seizure into an unreasonable one.

C. Supreme Court Doctrine Protects Privacy as Seclusion but not Secrecy

Real property law informs whether an individual has a reasonable expectation of privacy in secluding—i.e. restricting access to others—the property searched.[28] Facial recognition technology does not interfere with a cognizable Fourth Amendment privacy interest, such as interference with real or intellectual property rights, nor does it intrude upon personal security or movement. As such, there is no source of law upon which a reasonable expectation of privacy to object to facial recognition scanning could be grounded.[29]

Concepts of possession and property are at the core of the Fourth Amendment, as its possessive pronoun makes clear: "the right of the people to be secure in *their* persons, houses, papers, and effects." And so, from the beginning,[30] the Court has turned to property law to inform Fourth Amendment interests.[31] When the Court first encountered the modern investigative technique of wiretapping, for example, which like facial recognition enables investigators to obtain evidence without any physical interference with one's property, the Court found that no search had occurred because conversations are not tangible property or "material things" that the Fourth Amendment protects.[32] Likewise, facial recognition technology does not implicate any property interests.

Now, to be sure, the Court has subsequently extended the Fourth Amendment beyond property, as Justice Brandeis had urged in dissent. In *Katz v. United States*, the Court held that the Fourth Amendment applies to tangible and intangible interests such as private conversations,[33] because it safeguards from unreasonable search and seizure what an

---

[28] Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1, 3-4 (1979); *see also id.* ("An equivalent term is 'retirement' in its complex modern sense in which we speak of a person being 'retiring' and also of a person being 'retired.'").

[29] *See* Farahany, supra note 15, at 1254 (explaining that the most consistently recognized subjective and objective expectation of privacy is one that derives, at least in part, "'from the right to exclude others from the property in question.'")(internal citations omitted).

[30] 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.").

[31] *See* Boyd v. United States, 116 U.S. 616, 627 (1886) (stating that the "sacred and incommunicable" right of property is only set aside "for the good of the whole" (quoting Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (C.P.) 1066 (Eng.)). *See also* Farahany, supra note 17, at 1244-49 (reviewing how property law has informed Fourth Amendment privacy interests).

[32] Olmstead v. United States, 277 U.S. 438, 457 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[33] In *Katz v. United States*, 389 U.S. 347 (1967), FBI agents attached a device to the outside of a public telephone booth to listen to the defendant's conversations, and the Government argued that this eavesdropping did not implicate the Fourth Amendment because no trespass upon the defendant's property occurred. The government rejected the idea that an intrusion upon a constitutionally protected area must occur for the Fourth Amendment to apply.

individual "seeks to preserve as private."[34] Justice Harlan concurred and proposed the expectation-of-privacy analysis[35] that the Court eventually adopted.[36] This privacy test holds that a Fourth Amendment search occurs when an individual has a subjective expectation of privacy, that society recognizes as reasonable, which has been invaded.[37] Consistent with this analysis, the key Fourth Amendment question concerning facial recognition technology is whether its investigative use intrudes upon a privacy interest that society recognizes as reasonable.

Even with this expanded view of individual interests, however, an individual who is scanned in public cannot reasonably claim that facial recognition technology captures something he has sought to seclude from public view. Instead, he must argue that he has a reasonable expectation of privacy in his personal identity associated with his facial features. Under current doctrine, courts would properly reject such a claim. Despite the shift in *Katz* from purely property-based privacy protections to seclusion more generally, the Court has not recognized an independent privacy interest in the secrecy of identifying information per se.

Consequently, it is the physical intrusiveness of facial recognition technology, and not the extent to which it reveals personally identifying information, that will determine its reasonableness in a Fourth Amendment inquiry.[38] And because the technology is physically unobtrusive and does not reveal information that is secluded or otherwise hidden from public view, it is not properly characterized as a Fourth Amendment search.

Most recently, in *United States v. Jones*,[39] the Court revisited its property-invasion-as-privacy rationale, holding that the government's installation of a GPS tracking device on a suspect's vehicle constitutes a search subject to the Fourth Amendment.[40] In so doing, it left open whether the Fourth Amendment protects more than just intrusion upon seclusion. Justice Scalia, writing for the majority, emphasized that the government had "physically occupied private property for the purpose of obtaining information."[41] Invoking Lord Camden's opinion in *Entick v. Carrington*[42] and the text of the Fourth Amendment itself, Justice Scalia reaffirmed the significance of property rights to search and seizure analysis.[43] Although acknowledging that the Court had expanded beyond a strictly property-based approach in *Katz*, the opinion nevertheless emphasized that

---

[34] *Id.* at 351-52.
[35] *See id.* at 361 (Harlan, J., concurring).
[36] *See* Smith v. Maryland, 442 U.S. 735, 740-41 (1979) (The Court held that the government's use of a pen register—a device that records the phone numbers one dials—was not a Fourth Amendment search. The Court explained that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.")
[37] *Katz*, 389 U.S. at 361. Since *Katz*, Fourth Amendment law has also addressed the concealment of information. But even in *Katz*, the Court ultimately focused on Katz's seclusion of himself in the phone booth and not on his interest in the substantive secrecy of his conversation.
[38] *See* Terry v. Ohio, 392 U.S. 1, 30-31 (1968) (holding that the Fourth Amendment permits "reasonable inquiries" to determine a suspect's identity).
[39] 132 S. Ct. 945 (2012).
[40] *Id*. at 949 (2012).
[41] *Id.*
[42] (1765) 19 How. St. Tr. 1029 (C.P.) (Eng.).
[43] *Jones*, 132 S. Ct. at 949.

property rights remain the central source of individual interests protected by the Fourth Amendment.[44] While the police could have obtained the same information in *Jones* without a physical trespass, and such an intrusion might still be unconstitutional under *Katz*, the facts in *Jones* did not require the Court to resolve that question.[45]

What remains after *Jones* is an incomplete picture of which individual interests beyond real property interests, if any, that the Fourth Amendment protects. At the very least, *Jones* repudiates the view that *Katz* was "a shift in Fourth Amendment jurisprudential paradigms from a property-based framework to an expectation-of-privacy framework."[46] Real property law remains central to Fourth Amendment individual interests. And under a property analysis, facial recognition is clearly not a search.

To be sure, the *Jones* majority also emphasized that trespass upon property and the *Katz* expectation-of-privacy test coexist in Fourth Amendment jurisprudence. But even under a privacy-based analysis, the use of facial recognition technology is not analogous to the wiretap in *Katz*, and as such is not properly characterized as a search. If facial recognition technology captures facial features that an individual has not secluded,[47] then unlike *Katz*, its investigative use does not intrude upon information that an individual has kept hidden. Without trespass upon real property, or upon information that a person has sought to hide, there is no legitimate source of law upon which a reasonable expectation of privacy could be founded.

Conclusion

As I have explained, governmental use of facial recognition technology does not generally constitute a Fourth Amendment search, let alone an unreasonable one. Nevertheless, this technology does raise novel privacy concerns, which are certainly the proper concern of Congress.

As some of the other panelists have emphasized, it is a brave new world, in which our reasonable expectation of privacy may seem to be under assault by technology. And Congress may indeed have a role to play in striking the proper balance between privacy and security in this area. I would emphasize, though, that the legal and ethical landscape here is very complex, implicating a variety of cross-cutting interests. (The answers may be different depending on whether these tools are being used by governments or by private actors, and it may matter whether people have opted into a database or been included against their will.). These sorts of technological advances may indeed diminish our privacy. But they are also extraordinarily useful, to private individuals, to corporations, to social networks, and to law enforcement. I am not at all certain that legislation is required in this area. But in any case, I would encourage the Subcommittee to consider carefully the legal,

---

[44] *Id.* at 950.

[45] *Id.* at 954. Since the government took the position that GPS tracking did not constitute a search, the Court left for another day the further question of which individual interests, beyond intrusion upon property, an individual could claim to assess the reasonableness of the search that had occurred.

[46] David A. Sullivan, A Bright Line in the Sky?: Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology, 44 ARIZ. L. REV. 967, 974 (2002).

[47] E.g. by wearing a mask, a veil, or other head covering that hides their visage.

ethical, and social implications of any legislative response. Again, I thank you for the opportunity to appear before you today, and I look forward to your questions.

Appendix to the Testimony and Statement for the Record of

Nita Farahany
Professor of Law, Duke Law School
Research Professor of Genome Sciences & Policy,
Institute for Genome Sciences & Policy

Hearing on
"What Facial Recognition Technology
Means for Privacy and Civil Liberties"

Before the

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law