September 2006

Enhancing the Senses: How Technological Advances Shape Our View of the Law

Steven Goldberg
Georgetown University Law Center

Follow this and additional works at: https://researchrepository.wvu.edu/wvlr

Part of the Forensic Science and Technology Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://researchrepository.wvu.edu/wvlr/vol109/iss1/4

This Article is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact researchrepository@mail.wvu.edu.
ENHANCING THE SENSES: HOW TECHNOLOGICAL ADVANCES SHAPE OUR VIEW OF THE LAW

Steven Goldberg *

It is a distinct honor for me to deliver the Edward G. Donley Memorial Lecture as part of this important symposium on forensic and biometric advances. **West Virginia University has a well-deserved national – indeed, international – reputation in these fields, owing to your bachelor of science degree program in Forensic and Investigative Sciences, your university-wide Forensic Science Initiative, and your Biometric Knowledge Center, among other activities. I have learned a great deal from the presentations over the last two days.

I wanted to speak today on Enhancing the Senses: How Technological Advances Shape Our View of the Law. Technology often enables us to see where we could not see before. When, in 1609, Galileo pointed his telescope at the moon, new worlds opened up.¹ Today, advances in fields ranging from iris scanning to voice recognition are opening up more new worlds, and new challenges as well for our legal system.

In this lecture I hope to show how, just as the telescope provided new perspectives, a careful look at some familiar legal ideas can also show some surprising implications for research, development, and deployment for forensics and biometrics.

Let’s begin with the funding of research. In recent months there has been a resurgence of interest in giving the President of the United States the line-item veto. Perhaps no topic seems more remote from this symposium, but I think a close look will show there is an important connection.

In most states, when the governor receives a spending bill, he can veto individual line items that he believes are wasteful.² In 1996, Congress gave the President the power to do the same thing.³ In 1998, however, in the case of Clinton v. City of New York, the Supreme Court found the line item veto uncon-

* Professor of Law, Georgetown University Law Center

** This manuscript is based on the Edward G. Donley Memorial Lecture given by Steven Goldberg on March 28, 2006 at the West Virginia University College of Law as part of the West Virginia Law Review symposium, “Brave New World – Developing the Legal Frontier in Light of Forensic and Biometric Advances.”


³ Id.
stitutional on the ground that under the U.S. Constitution the President has to sign or veto an entire bill.\(^4\)

On March 6, 2006, President Bush proposed new legislation that he believed could survive Supreme Court review.\(^5\) The prospects for passage are considerable – President Bush’s idea is supported by, among others, Senator John Kerry, Bush’s opponent in the last presidential election.\(^6\) Under the new proposal, the President could take out any line item in a spending bill, and send it back to Congress for an up or down majority vote.\(^7\) This would force Congress to go on record for individual projects rather than being able to lump them all together.

Now suppose the line item veto is passed and upheld in court. Over time, Presidents will be drawn to vetoing line items that the public would find silly and wasteful. And that’s where the danger to basic research comes in. It is the easiest thing in the world for politicians to make fun of pointy-headed basic research that has no obvious immediate application. Years ago, Senator William Proxmire used to give “Golden Fleece” awards to spending he regarded as wasteful. I studied his awards, and I found that he liked to single out relatively inexpensive basic research grants.\(^8\) Here, for example is how Proxmire described a study of aggression in primates that focused on when animals clench their jaws:

> The funding of this nonsense makes me almost angry enough to scream and kick or even clench my jaw. It seems to me it is outrageous. Dr. Hutchinson’s studies should make the taxpayers as well as his monkeys grind their teeth. In fact, the good doctor has made a fortune from his monkeys and in the process made a monkey out of the American taxpayer.\(^9\)

Now studies of aggression in animals can have real benefits; they can, in fact, lead to medicines that help thousands. Imagine how much more vulnerable to ridicule an odd sounding study of something like utilizing artificial intelligence models to study algorithms used in processing sensory data might be.

\(^5\) Fact Sheet: President Submits Line Item Veto Act to Congress, supra note 2.
\(^7\) Id.
\(^8\) STEVEN GOLDBERG, CULTURE CLASH: LAW AND SCIENCE IN AMERICA 53-54 (1994)[hereinafter CULTURE CLASH]. Although the spending programs singled out by former Senator Proxmire were typically individual grants awarded by agencies rather than line items in the federal budget, the problem is the same: it is easy for politicians to make fun of basic research.
\(^9\) Id. at 54.
But this sort of basic research in pattern recognition could have enormous importance down the road for biometric techniques such as voice recognition,\textsuperscript{10} techniques that could prove vital in recognizing terrorists. Today, there are line items in the budget that relate to biometrics\textsuperscript{11} and they could be vulnerable.

I am not interested here in whether the new line item veto bill is constitutional or even whether it is wise. My point is simply this: basic research will have a large say in the future of biometrics and forensics. And we should never take its popularity for granted. Most countries barely fund basic science at all; it is a fragile flower. Whether or not there is a line item veto, those who want to see a bright future for biometrics have to be active in promoting and protecting its research base.

Let's turn now to the typical way science and technology are funded in the United States.\textsuperscript{12} Typically, Congress passes and the President signs authorization and appropriation bills that operate on a department by department basis.\textsuperscript{13} In other words, the Defense Department appropriation bill contains, among many other things, money for research and development, as does the Health and Human Services budget, the Department of Energy budget, the National Science Foundation budget, and so on.\textsuperscript{14} The big story here is one of decentralization.\textsuperscript{15} Despite various proposals going back over a century, the United States, unlike many other countries, has never created a Department of Science.\textsuperscript{16}

As a result, there is overlap in the research efforts of the various agencies. And sometimes “overlap” is a polite term for duplication. Presently, for example, research and development on facial recognition technology is carried out by a variety of cabinet agencies, including State, Justice, Energy and Defense.\textsuperscript{17} Under the circumstances, it is important that federal efforts be coordinated through such groups as the White House Office of Science and Technology Policy.

Now I’ve been talking about government funding of research. Of course, scientists are not required to obtain such funding. Suppose a researcher has controversial views that the key agency decision makers believe are not well grounded in science. He might believe, for example, that he can determine whether a suspect under interrogation is lying by analyzing subtle changes in the


\textsuperscript{12} CULTURE CLASH, supra note 8, at 44-49.

\textsuperscript{13} Id.

\textsuperscript{14} Id.

\textsuperscript{15} Id.

\textsuperscript{16} Id.

heat emissions from the suspect's body. No one will fund him because they do not agree with him on the underlying science. Still, two basic realities remain.

First, the scientist can give speeches and publish papers trying to persuade the government and the society that he is right. The First Amendment protection for free speech extends to scientific speech.\(^\text{18}\) And this is something we should not take for granted. The former Soviet Union and Hitler's Germany had formidable scientific research programs that were hampered because no one in those countries was allowed to question the dominant scientific wisdom.\(^\text{19}\)

The second reality is that our unpopular biometrics researcher can carry out experiments if he can obtain private funding and if his research does not endanger public health and safety. Perhaps then his ideas will gain wider support.

Nonetheless, the fact remains that money is vital for scientific research and, for fundamental research, where the payoffs are distant and uncertain, the federal government remains a vital source of funding. With regard to science, the federal government has more power than it does in other fields. It would be unconstitutional for the government to fund the presidential campaign of the Republican, but not the Democratic party. But the government can fund one approach to polygraph research and not another.

This extraordinary government power suggests that a Department of Science would be a dangerous idea. Although it might look better on an organization chart, we don't want to put all of our eggs in one basket in the uncertain world of basic research funding. If various agencies take a variety of approaches, we may end up better off in the long run.\(^\text{20}\)

Let us now look at what happens when research leads to applications, and biometric and forensic advances enter society. I want to focus here on constitutional issues. In keeping with the theme of enhancing our vision, let's put off for a moment our discussion of searches and informational privacy, and look in some less familiar places.

In fact, let's begin with the first words of the First Amendment: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof."\(^\text{21}\) Religious freedom is a cherished part of American history and culture, but it can at times come into conflict with other values.

About two years ago, a number of Muslim women in Alabama protested when state officials made them remove their head scarves before taking their photos for a driver's license.\(^\text{22}\) The women had a religious obligation to wear

\(^\text{18}\) CULTURE CLASH, supra note 8, at 28-31.
\(^\text{20}\) See CULTURE CLASH, supra note 8, at 53.
\(^\text{21}\) U.S. CONST. amend. I.
\(^\text{22}\) Alabama Muslims Denied right to Islamic Attire, http://www.cair-
ENHANCING THE SENSES

their hijab or head scarf. The photograph on a driver's license is a kind of biometric identifier, and, in the future, it may be routinely linked to more elaborate electronic recognition systems.

How does our society resolve this kind of conflict between religious expression and the law? If the government singles out a religious practice and bans it because it disagrees with the religion in question, that is a clear violation of free exercise. But what if a neutral state law that serves a valid governmental purpose runs up against a religious practice, as happened in the driver's license case? No one claims that the requirement of a photograph on a driver's license was aimed at discriminating against Islam.

As a matter of federal constitutional law, a neutral statute of this type can be applied despite religious objections, in other words, the free exercise challenge will fail. Many states follow this approach as well, although some hold, as a matter of state law, that the religious practice will be allowed unless there is a compelling state interest in applying the statute to the religious group.

But perhaps most importantly, in a case like the drivers license problem in Alabama, the government is free to carve out an exemption for a religious practice if it so chooses. Our society allows the government to accommodate strongly held religious beliefs when possible.

And, in fact, after complaints from the Muslim women, Alabama authorities began to look more closely at their state law that required that no one could wear a head covering when they had their driver's license photo taken. Did all head coverings really cause a problem when you are identifying someone by looking at a driver's license? The Muslim head scarf covers the woman's hair, but not her face. And under Alabama law, nothing prevented a woman from wearing a wig when her driver's license photo was taken. Finally, a compromise was reached and the Alabama law was changed to allow an exception to the no head covering rule in cases of genuine religious need. The head still had to be visible from the top of the forehead to the bottom of the chin and the hairline had to be visible from side to side. The Islamic women were delighted. And Alabama's policy came in to line with the majority of the states that have considered this issue.


23 Id.


27 Id.

28 After Protests, Alabama Scraps Driving License Hijab Ban

The new Alabama policy also allowed medical exceptions to its photograph requirements. Id.
When we look even more closely, we will see that this resolution demonstrates an important and, to some, controversial feature of American law. Under Alabama law today, you can wear a head covering when your driver’s license photo is taken if you have a religious reason, but you cannot wear a head covering if you have a political or artistic or cultural reason. This is not an exception for everyone. It is not even-handed. It quite clearly favors religion over other forms of activity. The same is true when the government, as it does in many states, says that Native Americans can use peyote, an otherwise illegal drug, in their religious rituals. These states do not allow individuals to use peyote for philosophical or political reasons.  

This is allowed because religion is special in the American system. The Constitution singles out the free exercise of religion for protection. Thus legislators are often free to accommodate religious expression, and biometric and forensic technologies are more likely to flourish when their implementation does accommodate religion to the extent possible. Needlessly, pushing a technology against religious values is every bit as unwise as pushing it against privacy values. In the end, no technology can survive, nor should it, if it does not gain a basic level of public support.

If religious freedom often gets less attention than privacy in discussions of new technologies, the same could be said of the First Amendment rights to free speech and assembly. The Constitution says that Congress shall “make no law . . . abridging the freedom of speech . . . or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” To understand the implications of this for our purposes, we have to go back to a civil rights case in 1958.

In that year, the United States Supreme Court set aside an Alabama court order requiring the NAACP to publicly disclose its membership list. The Court found that the order infringed on the rights of free expression and association because “revelation of the identity of [NAACP] rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility.”

More recently, the Court struck down a Los Angeles law requiring any publicly distributed handbill to identify its author, as well as an Ohio ban on anonymous campaign literature. These results are consistent with one of the

30 See generally McConnell, supra note 26.
32 U.S. CONST. amend. I.
34 Id. at 462.
most famous chapters in our Nation’s political history, the Federalist Papers. The Federalist Papers, which rallied support for the Constitution and play a role in its interpretation to this day, were published under pseudonyms.37

In 1999, the Court decided a case which brings us close to the intersection with the technologies we are concerned with today. In Buckley v. American Constitutional Law Found., Inc., the Court invalidated, on the authority of the earlier cases I described, a Colorado requirement that individuals circulating ballot initiative petitions wear a badge bearing their name.38 The Court noted that ballot initiatives were often controversial and that the requirement deterred people from participating in the political process.39

Now imagine an automated facial recognition technology that can scan a political rally and reliably tell the government the names of the people attending that rally. In theory, it would be like making everyone at that rally wear a name tag. The 1999 decision would be meaningless if you could tell the names of the people seeking names on a ballot initiative not by requiring a name tag but rather by scanning their faces into an automated system.40 Of course, anyone who appears in public runs the risk that they will be recognized, but the Court’s decisions hold that the government cannot increase that risk by requiring name tags, and a facial recognition system would appear to raise similar problems.

Now at this point I think it is essential to emphasize that the technology I am discussing is not the problem: it is the use of the technology. Indeed, a reliable facial recognition system could reduce infringements on First Amendment liberties. Let me explain.

The real question here is the government’s interest in scanning a crowd in the first place. If the government is infiltrating a political rally because it wants to undermine legitimate political opposition to its policies, we have a major free speech and assembly problem whether the government is using secret informants, a requirement that citizens wear name tags, or an automated facial recognition system. We are dealing with a government abusing its powers, and we hope that our system is robust enough to stop such abuses.

So let’s turn to the more conceptually difficult case, where the government has a valid interest in scanning a crowd, even at a political rally. Perhaps the government has received a specific reliable threat of a terrorist attack that will endanger those at the rally as well as citizens nearby. Imagine that the government has a photograph of the terrorist who is planning to carry out the threat.

---

39 Id. at 197-98.
Here, the government could use undercover agents, armed with the photograph, to look for the suspect. But, people are not always very good at matching a photograph to a face, and the agents may, consciously or not, fall back on stereotypes, including racial stereotypes, in deciding who to stop and question, thus offending citizens while missing the real suspect. If — and it's a big if — an automated facial recognition system could do better in terms of avoiding mistakes, it could also avoid racial stereotypes and safeguard citizens while protecting their rights.

So technology intersects with freedom of religion and freedom of speech, and in both cases distinguishing between appropriate and inappropriate government programs is vital. Let's turn now to the more familiar area of search and seizure.

In some settings, biometric technologies, such as those that recognize faces or how people walk, can be deployed without the traditional requirement of a warrant based on probable cause. In so-called administrative searches, where the government is carrying out health and safety functions rather than focusing on a criminal investigation, the Fourth Amendment requires only that the search be reasonable.

The leading case here, the Supreme Court's 1981 decision in Donovan v. Dewey, arose in the context of mine safety. Under federal law, inspectors can show up at mines unannounced and with no probable cause. They have to be let in. The Court upheld this, noting the commercial setting, the pervasive government regulation of mines, and, most importantly, the fact that the agency in question had procedures to assure the fair implementation of its inspection system. In other words, administrative law principles prevented the government from repeatedly searching one mine, perhaps because the owner was politically unpopular, while ignoring other mines. This administrative framework justifies the extensive searches, using a variety of techniques, that we see at airports and elsewhere.

Another area where traditional probable cause is not required, with possible implications for new technologies, is when the police simply stop an individual for questioning. In 1968, in the case of Terry v. Ohio, the Supreme Court held that the police could stop an individual and pat him down to make sure he was not carrying a weapon if they had "reasonable suspicion" that something was amiss. "Reasonable suspicion" is less than probable cause, but, the Court

41 See, e.g., Connie Mayer, Due Process Challenges to Eyewitness Identification Based on Pretrial Photographic Arrays, 13 PACE L. REV. 815, 820 (1994) ("[T]he photograph is merely a two-dimensional depiction of a person. Often a witness cannot discern height and weight accurately from a photograph. If the photograph is old and no longer accurately depicts its subject, it may also lead to a false identification.").
43 Id.
44 Id. at 604-06.
45 392 U.S. 1 (1968).
reasoned, the "stop and frisk" they were authorizing was less intrusive than a full-blown search.\textsuperscript{46}

In 2004, a deeply divided 5-4 Supreme Court extended \textit{Terry} in the case of \textit{Hiibel v. Sixth Judicial District Court}.\textsuperscript{47} Deputy Sheriff Lee Dove of Humboldt County, Nevada set out to investigate a telephone call which alleged that a man in a red and silver GMC truck on Grass Valley Road had assaulted a woman. When Dove found the truck, with a woman sitting in it and a man standing beside it, he asked the man for identification. The man refused. Eventually, after warning the man that he could be arrested for failing to provide his name, Dove arrested the individual.

The arrested individual, one Larry Dudley Hiibel, was convicted and fined $250 under Nevada law for having obstructed a police officer by failing to identify himself. In some, but not all, states it is a crime to fail to identify yourself when stopped by a law enforcement official.\textsuperscript{48} Hiibel argued that his Fourth and Fifth Amendment rights had been violated, but five members of the U. S. Supreme Court disagreed.\textsuperscript{49}

\textit{Terry v. Ohio} held that the police could stop and frisk you. It left open the question of whether you could be forced to identify yourself. In \textit{Hiibel}, Justice Kennedy reasoned that you could, since the intrusion was not great and knowing the identity of a suspect could clear them, or alert the police to a domestic disturbance problem, or otherwise serve valid state goals.\textsuperscript{50} Justice Stevens, in dissent, raised a concern relevant to us here when he wrote, "A name can provide the key to a broad array of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases."\textsuperscript{51} We might add that new technologies, such as facial recognition, could link you to such a database even if you do not give your name.

\textit{After Hiibel}, individual states have the freedom to decide whether to require citizens to give their names when stopped by the police in the absence of probable cause. And they will also make the initial decisions about the deployment of more advanced identification technologies in the stop and frisk setting. If they make those decisions with sensible consideration of the accuracy of their systems and of public attitudes, then they will enjoy more long-term success than if they try to ram a system down the public's throat.

So searches in regulated areas, such as airports, and minor intrusions, such as "stop and frisk" encounters, are generally associated with government victories in court. Unsurprisingly, we begin to see the government losing cases

\textsuperscript{46} \textit{Id.} at 25-26.
\textsuperscript{47} 542 U.S. 177 (2004).
\textsuperscript{48} \textit{Id.} at 182-83.
\textsuperscript{49} \textit{Id.} at 185, 189.
\textsuperscript{50} \textit{Id.} at 186.
\textsuperscript{51} \textit{Id.} at 196.
more often when the traditional requirement of probable cause comes into play, particularly when the police are searching a private home.

This, of course, was the setting for the Supreme Court’s 2001 decision in *Kyllo v. United States*, a case with direct relevance to biometric and forensic technologies. In *Kyllo*, Agent William Elliott of the United States Department of the Interior suspected that marijuana was being grown in the home of Danny Kyllo in Florence, Oregon. Because he lacked the probable cause necessary to obtain a search warrant, Elliott, along with another federal agent, sat in a car across the street from Kyllo’s home and used a thermal imager – an Agema Thermovision 210 – to scan the residence. The imager detected infrared radiation coming from Kyllo’s house, which revealed that the roof over the garage and a side wall of the house were relatively hot compared with the rest of the house and with neighboring houses. Agent Elliott concluded that Kyllo was using halide lights to grow marijuana in his home.

Using the results from the imager along with other information, Elliott obtained a warrant for a search from a Federal Magistrate Judge. Once inside Kyllo’s home, federal agents found a marijuana growing operation that involved more than 100 plants. Kyllo appealed his marijuana manufacturing conviction on the ground that use of the thermal imager without probable cause constituted an unreasonable search under the Fourth Amendment. The United States Supreme Court agreed with Kyllo.

The Court was divided 5-4 in the *Kyllo* case. Justice Scalia’s opinion for the majority emphasized the traditional protection the Fourth Amendment provides for the home. But, Scalia recognized that visual surveillance of the home without probable cause has long been allowed, noting that the Court has held that “[t]he Fourth Amendment . . . has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.”

Moreover, Scalia conceded that “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” For example, in 1986 the Court upheld aerial surveillance of a fenced back-yard on the ground that “[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable to expect” that your back-yard is private.

So if an agent in an airplane can survey your back-yard, what is wrong with Agent Elliott using a thermal imager from across the street? The difference is your expectation of privacy about the inside of your house. The Court reached this conclusion by relying on its 1967 decision in *Katz v. United

---

53 Id. at 40.
54 Id. at 32.
55 Id. at 33-34.
States.\textsuperscript{57} \textit{Katz} upheld a Fourth Amendment challenge to warrantless eavesdropping by a listening device placed on the outside of a telephone booth on the theory that \textit{Katz} had justifiably relied on the privacy of the booth.\textsuperscript{58} The \textit{Katz} test holds that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."\textsuperscript{59}

Scalia's opinion for the Court in \textit{Kyllo} recognized that changing societal expectations of privacy shape Fourth Amendment rights under \textit{Katz}.\textsuperscript{60} In other words, if law enforcement officials and others were routinely scanning the infrared emissions coming from your house, you would not be justified in believing that using a heat source inside the house was a private affair. The Court twice noted that the search of Danny Kyllo's home was being set aside in part because thermal imaging devices are "not in general public use."\textsuperscript{61}

The four dissenting Justices did not believe that any reasonable expectation of privacy enjoyed by Danny Kyllo had been violated in this case. They felt Kyllo had no privacy interest in heat emissions that were, after all, being sensed after they had left his house. In the dissenters' view, Agent Elliott's use of a "fairly primitive thermal imager" was the same as if he had noticed that Kyllo's house was warmer than a nearby building because "snow melts at different rates across its surfaces."\textsuperscript{62}

Two main lessons for new technology emerge from \textit{Kyllo}. The first is that as a technology becomes widespread, our constitutional zone of privacy shrinks. The majority in \textit{Kyllo} does not deny this aspect of the \textit{Katz} test. As we have seen, it implied that if the thermal imager had been in common use it would have upheld the search. Thus, if someday a device that analyzes voices can reach from across the street into your living room, and use of that device becomes widespread, the Fourth Amendment will have little application.

If the first lesson supports the use of intrusive technologies, the second cuts in the other direction. All nine Justices in \textit{Kyllo} expressed concern about future technologies that impinge on privacy. The lesson here is that crucial public support for such technologies will be lacking unless they are deployed and monitored in a way that protects societal values.

It is not surprising that the majority made this point. In the course of holding that the search was improper, Justice Scalia said that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."\textsuperscript{63} He then detailed what he had in mind:

\begin{itemize}
\item \textsuperscript{57} 389 U.S. 347 (1967).
\item \textsuperscript{58} \textit{Id.} at 353.
\item \textsuperscript{59} \textit{Kyllo}, 533 U.S. at 33.
\item \textsuperscript{60} \textit{Id.}
\item \textsuperscript{61} \textit{Id.} at 34, 40.
\item \textsuperscript{62} \textit{Id.} at 41, 43 (Stevens, J., dissenting).
\item \textsuperscript{63} \textit{Id.} at 36.
\end{itemize}
The ability to "see" through walls and other opaque barriers is a clear, and scientifically feasible, goal of law enforcement research and development. The National Law Enforcement and Corrections Technology Center, a program within the United States Department of Justice, features on its Internet Website projects that include a "Radar-Based Through-the-Wall Surveillance System," "Handheld Ultrasound Through the Wall Surveillance," and a "Radar Flashlight" that "will enable law enforcement officers to detect individuals through interior building walls."64

But it was not just the majority that was concerned about emerging technologies and privacy. Although the dissenters in Kyllo would have allowed the use of the thermal imager, they did not believe that any technology could be used simply on the ground that it is only enhancing our senses. Justice Stevens's opinion for the four dissenters noted that:

Although the Court is properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession, it has unfortunately failed to heed the tried and true counsel of judicial restraint. Instead of concentrating on the rather mundane issue that is actually presented by the case before it, the Court has endeavored to craft an all-encompassing rule for the future. It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.65

So while the majority in Kyllo wanted to step in now, the dissent wanted to let the legislatures have the first crack at limiting future developments. Either way, the lesson for public policy is clear: unless biometric applications are strongly justified and carefully limited, vital public assent will be lacking.

Let us turn now from searches to the most discussed aspect of biometric and forensic technologies – the broad questions of privacy raised whenever the government maintains information on its citizens. Even if information is validly obtained for an important social purpose, how can we be sure that the information will not be used in improper ways? The constitutional issue here concerns what is called informational privacy. While there is no square holding on the subject, the Supreme Court has suggested that the due process clause may obligate the government to use reasonable measures to assure that information in

64 Id. at 36 n.3.
65 Id. at 51 (Stevens, J. dissenting).
government databases not be used for unauthorized purposes in ways that would impair an individual's privacy.\textsuperscript{66}

The suggestion came in 1977 in the Court's decision in \textit{Whalen v. Roe}.\textsuperscript{67} Under New York law, prescriptions for legitimate but addictive drugs had to be recorded on a computer database. The state used the database in an effort to prevent these drugs from being diverted into unlawful channels. The state wanted, for example, to make sure that "unscrupulous pharmacists [were not] repeatedly refilling prescriptions."\textsuperscript{68}

Although the computer system was designed to prevent leaks, and public disclosure of a patient's identity was made a crime, a privacy rights challenge to the system was brought by those who feared that the information could leak out and that patients would be stigmatized as addicts. The statute was upheld, with the Court noting that the New York system was set up to protect privacy and that there was no evidence that information had fallen into the wrong hands.\textsuperscript{69} But in his opinion for the Court, Justice Stevens suggested that future databases might not be constitutionally acceptable if they were not adequately protected against improper use:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme . . . evidence[s] a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data, whether intentional or unintentional, or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.\textsuperscript{70}

This suggestion that the Due Process Clause of the Fourteenth Amendment protects informational privacy means that a government biometric database with inadequate safeguards could be challenged by an individual in that

\textsuperscript{67} \textit{Id.}
\textsuperscript{68} \textit{Id.} at 592.
\textsuperscript{69} \textit{Id.} at 601.
\textsuperscript{70} \textit{Id.} at 605-06.
database on the theory that the government had violated his rights. Regardless of whether a court challenge would succeed, it is obvious that the public wants protection from unwarranted disclosures from databases. Biometric databases will be judged by that standard.

Consider, for example, a large federal agency that decides to use retinal scanning to control entrance to the workplace every morning. The information obtained from the scan is stored in digital form. There are two related concerns here. First, information from retinal scans might reveal health information, such as whether an individual has diabetes. The federal agency did not justify its access screening program on an assessment of anyone’s health, so it would be troubling if the agency were using that health information in deciding, for example, who got promotions. The second concern is that the information from the scan could leak out, so unauthorized entities could obtain identity information and health information concerning unsuspecting employees. Obviously, it is in everyone’s interest to limit this biometric to its authorized uses, and to prevent leaks of the biometric information.

Even when information from new technologies is gathered and maintained lawfully, there may be a further question of its admissibility in court. You have heard a good deal at this conference about the admissibility of scientific information under the Frye test, which is used in some states, and the Daubert test, which is used in other states and in the federal system. Both are designed to provide a reasonable assurance of reliability for our trial system, and both divide functions between the judge and the jury. Basically, as you know, the judge serves as a gatekeeper. Some expert evidence is deemed so unreliable that the jury simply cannot hear it; other expert evidence can go to the jury subject to cross-examination and the testimony of opposing experts. This approach is applied to biometrics ranging from polygraphs to DNA.

I just want to make one observation about this field: the case-by-case gatekeeper role by the trial judge, with all of its inevitable uncertainties and lack of uniformity, is not going to go away.

Occasionally I meet true believers on either side of the debate about the gatekeeper role, but I find that they are not really willing to go all the way with their beliefs. There are those who maintain that all expert evidence should go to the jury. The judge, as gatekeeper, they maintain, may be preventing the jury from hearing an unpopular point of view that will turn out to be true. The judge, in other words, might be keeping the next Galileo off the stand. As for unreliable or dishonest “experts,” we can, they say, rely on cross-examination and opposing experts to set the jury straight.

72 Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).
74 For a survey of which jurisdictions use which test, see David E. Bernstein & Jeffrey D. Jackson, The Daubert Trilogy in the States, 44 Jurimetrics J. 351 (2004).
To these true believers, I pose a simple question: should we let defendants in criminal cases present astrologers as witnesses? Could an astrologer testify, for example, that because the defendant’s moon was in the seventh house, he had no choice but to commit the crime? Here, the true believers waiver. And it is not because they think the jurors would laugh at astrology. If that were the case, there would be no danger in allowing the horoscope expert to take the stand. No, the true believers waiver because they know that the average juror may be more likely to believe in astrology than he or she is to believe in the accuracy of modern psychiatry or even modern forensics. In this case, even the true believers are sufficiently elitist to allow the judge to act as a gatekeeper.

True believers on the other side take a tough guy approach. They want the trial judges to relentlessly prevent juries from hearing everything they view as “junk science.” Even under Daubert and Frye, they believe juries hear far too many fringe experts trying to win acquittals for defendants or big judgments for plaintiffs on the basis of ideas that the mainstream scientific community believes to be untested and unpersuasive.

To these true believers, I ask whether, in a high profile murder case, they would have the judge prevent the jury from hearing eyewitness testimony. After all, if you actually look at the data, the scientific basis for the accuracy of eyewitness testimony is, to put it politely, far from obvious. Well, they don’t like that idea and in fact, they even resist allowing experts to testify about the weaknesses of eyewitness testimony. All of a sudden these opponents of “junk science” become born again believers in the historic and vital social role of the jury, an ancient institution that reflects our society’s values, not just impersonal science.

This example of the inevitable compromises that occur when law meets science in the courtroom is emblematic of broader truths concerning law and science throughout our society, from funding issues to the intersection with First Amendment rights to search and seizures and on to privacy.

Science is concerned with progress, with the accumulation of more and more testable knowledge about the natural world. It values powerful theoretical structures that can explain a host of phenomena. Newton’s theory of gravity applies not only when you drop an apple, but also when you drop a personal computer, even though the latter did not exist in Newton’s day.

Law is concerned with process, the peaceful resolution of social disputes. Multiple points of view have to be heard, values as well as facts are vital, and context is crucial. No one would apply the legal system from Newton’s day to our problems. Legal results do not seek to achieve the status of a formula that applies everywhere on earth.

---

75 See, e.g., ADULT EYEWITNESS TESTIMONY: CURRENT TRENDS AND DEVELOPMENTS (David F. Ross et al. eds., 1994).

76 See, e.g., United States v. Smithers, 212 F.3d 306 (6th Cir. 2000).

77 The contrast in this paragraph and the next between science’s emphasis on progress and the law’s focus on process is drawn from CULTURE CLASH, supra note 8, at 6-20.
The most important single message that comes out of all of this is that those of us who urge consideration of the social context of science are not anti-science. You are not helping biometrics if you try to run roughshod over religious objections, desires for anonymity in political action, or concerns for privacy. A mindless “pro-science” attitude or a view that “only science matters” is a recipe for a society where science is does not reach its full potential. Imagine if, in the 1950’s, nuclear engineers paid more attention to social concerns like the disposal of nuclear waste from reactors. Nuclear energy would not be worse off today, it would be better off.

You know, in 1609, when Galileo pointed his telescope at the moon, what he saw did not strike everyone as pretty. Aristotle and the Church had taught for millennia that the moon was a perfectly round sphere. The innocent in those days were not called pure as the driven snow, they were called pure as the moon. Galileo, of course, saw that the moon had mountains and craters; it was far from a perfect sphere.

When the implications of technology force a scientist to look closely at the law, he or she sees plenty of mountains and craters; plenty of imperfections and uncertainties. But we are comfortable with the way the moon really is today, and we can become comfortable with the real world of the law; in fact, understanding that reality is vital for the future of biometrics and the forensic sciences. Thank you.

---

78 CULTURE CLASH, supra note 8, at 96-98.