1-1-2008

Less Privacy Please, We're British: Investigating Crime with DNA in the U.K. and the U.S.

Duncan Carling

Follow this and additional works at: https://repository.uchastings.edu/hastings_international_comparative_law_review

Part of the Comparative and Foreign Law Commons, and the International Law Commons

Recommended Citation


Available at: https://repository.uchastings.edu/hastings_international_comparative_law_review/vol31/iss1/11

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings International and Comparative Law Review by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.
Less Privacy Please, We’re British:
Investigating Crime with DNA in the U.K. and the U.S.

By DUNCAN CARLING*

I. Introduction

DNA evidence is having an enormous impact on our criminal justice system. Police are now able to compare traces of DNA left at a crime scene against a national database of offenders, which often allows police to solve crimes for which they had no other leads. As of July 2007, the FBI’s National DNA Index System (NDIS) has aided over 52,800 investigations, thereby preventing an incalculable number of additional crimes.1 DNA evidence is also freeing many people who were in prison for crimes they did not commit. Post-conviction tests have exonerated 207 people in the United States so far, fifteen of whom were awaiting the death penalty.2 But although DNA technology is now a well-established investigative tool, legal issues continue to arise.

The United States and Great Britain are the world leaders in the use of DNA databases for criminal investigations. The British started using a national database in 1995, while the U.S. database became operational in 1998.3 The law in this area is evolving differently in

---

* J.D. Candidate, May 2008, University of California, Hastings College of the Law.
each country, however. For example, the British police are allowed to collect samples from a much wider range of people, and are authorized to use the data in ways that are not permitted in the United States.

This note will compare the differences between the American and British DNA database programs, and discuss how these differences came about. The first section will briefly review the nature of a criminal DNA database. This field is an intersection of biology, software, and law; this note will discuss the bare minimum of science necessary to clarify the legal issues that follow. The second section will review the differences between the United States and United Kingdom programs. It will review how the legislation differs, and discuss two notable differences in practice: the collection of DNA from people who have been arrested but not convicted, and the technique of looking for an offender's relatives in the database. The final section will offer an explanation as to why these differences have arisen. Our respective constitutional frameworks provide only part of the explanation; our disparate cultural views on privacy are equally significant in shaping these national programs.

II. An Overview of DNA Databases

A. DNA Evidence

DNA is a molecule composed of deoxyribonucleic acid and found in the nucleus of almost every cell in the human body. We inherit half of it from our father and half from our mother, and it carries our human genetic information. DNA defines many of our physical characteristics and possibly our propensity for certain kinds of behavior.

The entirety of genetic content contained in our DNA is called the human genome. Ninety-eight percent of the data is the same for every human, but the remaining two percent is unique to each individual. In the 1990s, scientists made significant advancements in

4. Parliamentary Office of Science and Technology, supra note 3.
5. Id.
their understanding of the human genome. Now we are aware of specific regions in the genome which can be accurately used as personal identifiers, analogous in some ways to a fingerprint.

These locations in the genome, called loci, function as markers where genetic samples can be compared against each other. At these markers we have DNA sequences called alleles. Because people inherit genetic variations, the length or sequence of a person's alleles at these markers will vary. The specific length or sequence of an allele is represented by a number, and these numbers are stored in databases for comparisons. When investigators compare DNA samples from a crime scene against a database, they are comparing numbers that represent the alleles present at these markers.

The significance of a match depends in part on how many markers are being compared. The FBI compares alleles at thirteen markers, while the British police make comparisons at ten. But the significance of a match also depends on how common, or rare, the alleles at those markers are. When the alleles in the profile are rare, the significance of a match is much higher. If the alleles in a profile are common, the significance of the match can be strengthened by comparing alleles at more markers. The chance of two unrelated people sharing a common allele at a single marker might be one in ten, but the chance of them sharing uncommon alleles at 16 markers could be one in 700 quintillion or less.

For the purposes of this note, there are two things to keep in mind about DNA. First, a comparison of DNA markers may yield something other than a "match" or "no match." Because of the way DNA is inherited within a particular family group, DNA profiles of individuals who are related to each other are more likely to contain similarities than profiles of unrelated individuals. It is therefore possible to look in the database not just for the offender's profile, but also look for profiles that may belong to a parent, child, or sibling of the offender.

8. Id.
9. Id. at 29.
10. Id. at 34.
11. Id. at 45.
14. Id. at 36.
Second, a comparison based on DNA markers does not involve the full array of information that DNA potentially holds about someone. The portion of the genetic sequence that investigators use for markers is commonly referred to as "junk DNA" because it does not contain any otherwise useful information.\(^\text{16}\) While the probative value of "junk DNA" is debated,\(^\text{17}\) DNA profiles used currently by law enforcement reveal nothing about the person other than their gender and what their DNA "fingerprint" looks like. However, because information elsewhere in the genome can be used to predict things like appearance, health, or behavior, the practice of using just a small part of the DNA sequence, even a part that does not reveal any of those things, is controversial.

**B. DNA Crime Databases**

When a sample of DNA is collected from an offender or a crime scene, numbers are used to represent the alleles present at the indexing markers.\(^\text{18}\) These numbers are then stored in a software database, for reference and comparison to other files. What happens to the actual tissue sample afterwards varies. Some jurisdictions destroy it, but some keep it in storage. Because the sample contains the entire array of DNA information, their subsequent status is a contentious topic.\(^\text{19}\) Under current profiling systems, however, the genetic information in those samples is not available to law enforcement investigators.

Criminal DNA databases are generally separated into two pieces: an offender index and a crime scene index.\(^\text{20}\) The offenders are all of the known people who have been required to submit a sample. The crime scene index holds any traces of DNA found at unsolved crime scenes. These are automatically compared against each other on a regular basis, to see if a new offender in the system matches a previously unsolved crime, or if a new crime sample

---


matches another crime sample already in the system. A match between crime scene samples allows investigators to link seemingly unrelated incidents to the same, unknown, perpetrator.

**III. Differences between the U.S. and U.K. DNA Programs**

**A. The Legal Structure**

Like many government functions in the United States, the national DNA database is a combination of state and federal programs. All 50 states now have their own DNA legislation, and each one maintains a state database in accordance with their state laws, which often vary. The FBI has developed DNA comparison software called CODIS (Combined DNA Identification System), which they license to the states. Each state uses CODIS to upload DNA profiles both to their own state database and the national database.\(^2^1\) CODIS therefore provides a hierarchical system: profiles originate at the state level, and then move up to the national index.\(^2^2\) This allows the state agencies to work within their own statutory guidelines for administration and maintain their own database, but also make comparisons against a national database of offenders.\(^2^3\) The FBI is responsible for adding federal offenders to the database, in accordance with federal law.

While every state is participating in this program, the use and effectiveness of the programs vary significantly from state to state. California has the largest state database, with 955,525 offender profiles, and has generated over 5,000 “hits” so far.\(^2^4\) Virginia, which was the first state to develop a database, has 258,816 profiles.\(^2^5\) Mississippi, on the other hand, has only 3,600 profiles in its database and has only aided eight investigations.\(^2^6\) Often low utilization is a

---


22. Id.

23. Id.


result of financial restraints, rather than lack of effective legislation. Louisiana, for example, has one of the broadest statutory mandates for collecting samples, but has only aided 586 investigations, due to lack of available resources.28

The situation in the United Kingdom is very different. The United Kingdom was the first nation to implement a DNA program, establishing the National DNA Database (NDNAD) in 1995.29 The NDNAD is operated by the Forensic Science Service, a government-owned company that provides forensic services to the police departments in England and Wales.30 There was no specific legislation that set up the NDNAD; instead, a series of amendments have been passed to the existing Police & Criminal Evidence Act. The first of these amendments, passed in 1994, allowed DNA samples to be collected and stored like fingerprints,31 and the subsequent amendments have progressively broadened this power of the police. The most recent amendment, passed in 2003, allows police to collect a sample from anyone arrested for a recordable offense, regardless of whether or not they are charged.32

In 2000, Prime Minister Tony Blair announced the DNA Expansion Programme, a £240 million effort to include every known offender in the database.33 This ambitious goal of having every active criminal in the database, combined with an early start, put the United Kingdom in a leadership position. For many years the NDNAD was the largest DNA database in world, but recently the United States' NDIS surpassed the NDNAD in size. As of July 2007, the U.S. database had 4,766,390 offenders,34 compared to 3,976,090 offenders

29. The National DNA Database, supra note 3.
in the U.K. database.\textsuperscript{35} But the United Kingdom still has the largest percentage of population profiled. The United Kingdom currently has 6.5\% of its population in NDNDA,\textsuperscript{36} while the United States has just 1.5\% of its population in NDIS.\textsuperscript{37}

\textbf{B. Arrestee Sampling}

The difference in percentage of population included in the two databases is largely a result of different laws about who can be forced to submit a sample. In the United States, the rules regarding sample collection vary from state to state. Every state requires convicted sex offenders to provide a DNA sample, and as of October 2007, 44 states take samples from all convicted felons.\textsuperscript{38} Ten states are also taking samples from persons convicted of certain misdemeanors, usually for crimes related to sex or children.\textsuperscript{39}

Where the U.S. scope of sampling differs most significantly from the U.K. is in the area of arrestees. Arrestee sampling is the collection of DNA from people who have been arrested, but not yet convicted, and in some cases not even charged, with a crime. Currently eight U.S. states, including California, have laws authorizing arrestee sampling.\textsuperscript{40} Some states wait for the indictment and only sample sex offenders; California requires a sample from anyone charged with a felony sex offense, murder, or manslaughter, or anyone who attempts to commit those crimes.\textsuperscript{41} In 2009, this will expand to arrests for all felonies.\textsuperscript{42} Because only a small number of states have started arrestee sampling, the case law is very limited, and
the constitutionality of this practice is not clear. There are only two U.S. cases that have addressed the issue, and they come to opposite conclusions.

One is a Virginia case from September 2006, Anderson v. Commonwealth. In 2001, Angel Anderson was arrested on a rape charge. Because the Virginia statute allows collection of DNA from someone arrested for rape, police took a sample from Anderson immediately after the arrest. When this sample was entered into the state database, it matched a crime scene sample from an unsolved 1991 rape. Anderson was convicted of the earlier rape, but appealed on grounds that the DNA taken after his 2001 arrest violated his Fourth Amendment rights. Specifically, he argued that taking the sample was a "suspicionless search," unrelated to the crime for which he had just been arrested.

The court disagreed. It referenced the established principle that a search incident to arrest is permissible within the Fourth Amendment, and that such a search may include an attempt to identify the arrestee. It also pointed to the 1992 Fourth Circuit case Jones v. Murray, which held the state's interest in the arrestee's identity "is relevant not only to solving the crime for which the suspect is arrested, but also for maintaining a permanent record to solve other past and future crimes."

The Minnesota Court of Appeals, however, reached the opposite conclusion on this issue only a month later. In the October 2006 case In re Welfare of C.T.L., C.T.L. was charged with assault and aiding and abetting robbery. The state ordered C.T.L. to submit a DNA sample, but he refused, arguing that the collection would violate his Fourth Amendment rights. The Court of Appeals agreed, holding that arrestee sampling, with only a judicial determination of probable

44. Id. at 709.
45. Id.
46. Id.
47. Id.
48. Id. at 710.
49. Id. at 711.
50. Id. at 710.
52. In re C.T.L, 722 N.W.2d 484, 486 (Minn. 2006).
53. Id.
cause, violates the warrant requirement of the Fourth Amendment.\textsuperscript{54} The court stated that in this situation, the privacy interest of the person who has been charged, but not convicted, is not outweighed by the state’s interest in taking a DNA sample.\textsuperscript{55}

While arrestee sampling is an unsettled legal issue in the United States, it is an accepted and widespread practice in the U.K. In 2001, the Police and Criminal Evidence Act was amended to allow the Forensic Science Service to retain a person’s sample after an acquittal or dismissal.\textsuperscript{56} In 2003, another amendment authorized the police to collect samples from anyone arrested for a recordable offense, before a person is charged.\textsuperscript{57} While the few U.S. states that permit arrestee sampling do so only after a serious offense, the British are collecting samples from people arrested for minor crimes, such as being drunk in public or panhandling.\textsuperscript{58}

The retention of these samples without a conviction was challenged in the English courts. Two cases were considered together: one involved an 11-year-old boy charged with attempted robbery, who was tried and acquitted.\textsuperscript{59} The other involved a 38-year-old man who was charged with harassment by his partner. The partner later dropped the charges.\textsuperscript{60} In both cases, police retained the DNA samples on file, pursuant to the 2001 amendment. The plaintiffs argued that, because neither of them was ever convicted of a crime, holding their DNA on file violated their privacy.\textsuperscript{61}

The Court of Appeal upheld the retention of the samples, on the practical ground that a larger database is better. Lord Woolf wrote, “[t]he larger the databank, the greater the value of the databank will be in preventing crime.”\textsuperscript{62} The case was appealed to the House of Lords, which affirmed the Court of Appeal decision. Lord Steyn wrote for the House of Lords, “[i]t is of paramount importance that

\textsuperscript{54} Id. at 492.
\textsuperscript{55} Id.
\textsuperscript{56} Criminal Justice and Police Act, United Kingdom (2001).
\textsuperscript{57} Criminal Justice Act, United Kingdom (2003).
\textsuperscript{59} Regina (S) v. Chief Constable of the South Yorkshire Police; Regina (Marper) v. Chief Constable of South Yorkshire Police, 1 WLR 3223 (2002).
\textsuperscript{60} Id.
\textsuperscript{61} Id.
\textsuperscript{62} Id.
law enforcement agencies should take full advantage of the available techniques of modern technology.63 English courts seem, therefore, to value the effectiveness of a large database over privacy concerns. Why that is the case will be explored later in this note, but it is worth noting here how a policy like arrestee sampling adds to effective law enforcement.

Consider the 2001 Criminal Justice and Police Act, which allowed the Home Office to keep DNA profiles after a case was dropped or the accused was acquitted. After the law went into effect, the police were able to keep 198,000 profiles in the database that would have been destroyed under the old law.64 During the next five years, 7,591 of those profiles were matched to over 10,000 crimes, including 88 murders and 116 rapes.65 The 2003 amendment, allowing arrestee sampling, is already showing similar results. Generally, 43% of people arrested in the United Kingdom are not charged.66 During the years 2004 and 2005, samples taken from people who ended up not being charged yielded 250 matches to other crime scenes, including four murders, three rapes, and 98 burglaries.67

C. Familial Searching

In addition to taking samples from a broader range of people, the British are also using their database in more powerful ways. A notable example is the practice of “familial searching.” When investigators do not find a perfect match in their database, they sometimes look instead for a “partial” match: a profile that matches a higher-than-average number of markers. Someone who shares alleles at six or more markers may be a close relative of the actual suspect. This can be a significant lead in a cold investigation, giving investigators a place to start, or allowing them to focus on a particular suspect, saving time and resources.

The British started using familial searching in 2002.68 Since then, the Home Office has used the technique in 20 cases and solved five of them, including the rape and murder of an 86-year-old woman.69
} In March of 2003, someone threw a brick off a bridge that ran over a road. It went through a car windshield, causing the driver to suffer a fatal heart attack. There were no witnesses, but the offender left a little of his own blood on the brick. There was no match in NDNAD, but police checked for partial matches and found a close relative, who led them to Harman. When confronted, he confessed, and is now serving a six-year sentence for manslaughter.\footnote{Id.}

This method is used very rarely in the United States. Massachusetts and New York are the only states that have statutes that explicitly allow familial searching, although most states do not have a law prohibiting the practice.\footnote{Richard Willing, \textit{Suspects get snared by a relative's DNA}, USA TODAY, June 7, 2005, <www.usatoday.com/news/nation/2005-06-07-dna-cover_x.htm> (visited Oct. 1, 2007).} In Virginia, the laboratories are authorized to turn over "very, very close matches,"\footnote{Id.} but are not permitted to turn over anything short of that, despite a strong suggestion of relation.\footnote{Gareth Cook, \textit{Near match of DNA could lead police to more suspects}, THE BOSTON GLOBE, May 12, 2006, <www.boston.com/news/nation/articles/2006/05/12/near_match_of_dna_could_lead_police_to_more SUSpects/> (visited Oct. 1, 2007).} In Massachusetts, the police do not use the technique, even though it is legal, because they lack the resources.\footnote{Id.}

North Carolina may have the only successful familial search in the United States at this point. In 2002, a DNA test proved that the wrong man was in prison for a 1984 rape and murder. Police compared the original crime scene sample against their database, and, although they did not find a match, they did find someone who matched at eight of the thirteen markers. Investigators then focused on that man's brother; they analyzed a cigarette butt he dropped, and DNA on the cigarette matched the crime sample perfectly. The man confessed and is now serving a life term in prison.\footnote{Willing, supra note 69.}

This example is one of a kind, however. Most states are not pursuing familial searching right now, despite the absence of any explicit prohibition against it. There may be a variety of reasons for this. Familial searching often requires substantial resources, because
a partial match may or may not be a relative of the target. Investigators must first determine if the person is a relative, and then investigate any connections between his family members and the crime. This can be an expensive, and fruitless, process. But familial searching can in some situations be helpful, depending on the genetic profiles involved and the nature of the investigation. The fact that this method goes almost entirely unused in the United States right now suggests that cost is not the only barrier, and that the Fourth Amendment is a potential barrier as well.

The collection of DNA samples implicates the Fourth Amendment because the blood extraction constitutes a search.\textsuperscript{77} Generally, the Fourth Amendment requires that a search be supported by some reasonable suspicion that an individual has committed a crime.\textsuperscript{78} But courts have also found many situations that allow for a “suspicionless search.” Some of these apply to exempted areas, such as airports and border crossings, and some of them qualify as “special needs.”\textsuperscript{79} Examples of special needs have been highway sobriety check points\textsuperscript{80} and random, suspicionless drug testing.\textsuperscript{81} But the ultimate issue with any warrantless search is whether it is “reasonable,” because the Constitution only protects citizens against unreasonable searches.\textsuperscript{82} And the reasonableness of a search is determined by balancing the state interest involved against the degree of intrusion on the citizen’s privacy.\textsuperscript{83}

The U.S. courts of appeals are unanimous that DNA collection statutes are constitutional, but they are split as to whether the issue falls under special needs analysis or the traditional balancing test. The Second, Seventh, and Tenth Circuits apply a balancing test only after finding the statute serves some special government need.\textsuperscript{84} The Fourth, Fifth, Ninth, and Eleventh Circuits apply the traditional

\textsuperscript{78} Terry v. Ohio, 392 U.S. 1, 27 (1968).
\textsuperscript{79} U.S. v. Kincade, 379 F.3d 813, 822-823 (9th Cir. 2004).
\textsuperscript{81} Board of Education v. Earls, 536 U.S. 822 (2002).
\textsuperscript{82} Skinner, 489 U.S. at 619.
\textsuperscript{83} Id. at 618.
\textsuperscript{84} See Roe v. Marcotte, 193 F.3d 72 (2d Cir. 1999) (upholding Connecticut DNA statute); Green v. Berge, 354 F.3d 675 (7th Cir. 2004) (upholding Wisconsin DNA statute); United States v. Kimler, 335 F.3d 1132 (10th Cir. 2003) (upholding the DNA Analysis Backlog Elimination Act of 2000).
balancing test without finding a special need. Despite these divergent analytic approaches, the constitutionality of DNA collection is always ultimately a balance between the state interest and the privacy interest. Common considerations that courts weigh in the balance are the minimally invasive nature of collecting blood samples, the offender’s reduced expectation of privacy, the strong state interest in public safety, and the exceptional reliability of DNA evidence for identification.

The issue of whether familial searching would alter that balance has never come before a U.S. court, but it seems possible that it could affect the constitutionality of a DNA database program. Some courts have identified the offender’s reduced expectation of privacy as one of the factors in the balancing test, but a familial search begins to implicate the privacy rights of the relative, and the constitutional significance of that is unknown right now. Some states may therefore be reluctant to pursue familial searching because doing so could upset the constitutional status of their investigation.

Arrestee sampling and familial searching are two prominent examples of how these programs differ in the United States and the United Kingdom, but there are others. DNA “dragnets” are also more common in the United Kingdom. This is a police tactic of encouraging all members of a community to provide DNA samples to aid an ongoing investigation, without suspicion of any one person. These occur in both countries, but are more common and accepted in the United Kingdom.

All of these examples demonstrate that the U.S. and U.K. legal regimes are evolving differently, both in regard to whose data is in the database, and what can be done with the information once it is there.

85. See Jones v. Murray, 962 F.2d 302 (4th Cir. 1992) (upholding Virginia DNA statute); Groceman v. United States, 354 F.3d 411 (5th Cir. 2004) (upholding the DNA Analysis Backlog Elimination Act of 2000); United States v. Kincade, 379 F.3d 813 (9th Cir., 2004) (en banc, five judges endorsing the reasonableness standard; one, the special needs exception; and five dissenting); Padgett v. Donald, 401 F.3d 1273 (11th Cir. 2005).
87. Id.
88. Roe v. Marcotte, 193 F.3d 72, 78 (2d Cir. 1999).
IV. Why the Law Is Evolving Differently

A. The Fourth Amendment

Clearly a large factor in these differing practices is the Fourth Amendment to the U.S. Constitution. The British are legislating DNA collection programs without a comparable constitutional constraint. But the Fourth Amendment does not fully explain the difference. There has never been a U.S. court case on familial searching, let alone a case that held that it violates the Fourth Amendment. Arrestee sampling is just starting to be discussed in the courts, but several states are already doing it successfully. Nonetheless, most states are not using either of these practices. While this may be attributable in part to disparities of state resources, it may also reflect the fundamentally different understanding of privacy in the United States and the United Kingdom. Before looking at our understandings of privacy, it is worth considering what about DNA databases makes privacy a controversial issue.

B. Privacy Concerns

Privacy is implicated by DNA evidence in several ways. First, there is the concern over the vast amount of information that DNA contains about a person. DNA may function in some ways like a fingerprint, but of course it is much more than that. Precisely what a person's DNA reveals about him is debated, but it certainly includes genetic defects, predisposition to disease and possibly the propensity to engage in certain behavior. Proponents of DNA databases point out that the current profiling systems do no use any of that information. Systems like CODIS only include numbers generated from alleles in "junk DNA," pieces of the genome that are useful for identification but nothing else.

Some privacy advocates are not assuaged by that response. They point to research that indicates this so-called "junk" DNA may in fact contain useful genetic information. Furthermore, the state and federal laws that authorize the collection of DNA generally do not require that tissue samples be destroyed after the numerical profile is created. The state is often keeping a complete genetic sample of

91. Kincade, supra note 17, at 850.
92. Gibbs, supra note 17, at 29. See also Steinhardt, supra note 19, at 173.
93. Steinhardt, supra note 19, at 190.
these people, even if it is not using it. But current law enforcement methods of DNA comparison and investigation do not involve any of this genetic information. DNA collection statutes in both the United States and United Kingdom only allow investigators to look at numeric representations of the markers for the sole purpose of solving crimes. So the question of what other information may be available in a tissue sample, or in "junk" regions of the genome is largely irrelevant.

Regardless of how well genetic privacy is being maintained today, another common concern is how the government might use this genetic information in the future. In March of 2000, the House Judiciary Subcommittee on Crime held hearings regarding CODIS and the use of DNA databases in criminal investigations. Barry Steinhardt, who is the Director of the Technology and Liberty Program at the American Civil Liberties Union (ACLU), testified on behalf of the ACLU and described one of the organization's concerns about DNA database programs: "While a DNA data bank for criminal identification purposes may have legitimate uses, I am skeptical that we can hold the line and ward off the temptation to expand its use to non-forensic purposes." Steinhardt pointed the Subcommittee to two previous examples of what he called "function creep" in other government database programs. One was social security numbers, which the government stated in the 1930s would only be used to facilitate a new retirement program, and the other was census records, which were used during World War II to round up Japanese Americans for internment camps, despite their original, benign, statistical purpose.

It should be noted that most of these privacy concerns involve future, hypothetical scenarios. In their current implementations, DNA database programs do not reveal anything about the subjects other than their gender. Proponents of these databases argue that DNA is a uniquely powerful investigative tool, which should not be underutilized because of theoretical concerns about possible future use or misuse. As their current use is permitted narrowly by statute,  


95. Id.
any new use would have to be legislated as well.

C. Different Legal and Cultural Understandings of Privacy

Privacy has become an integral part of American constitutional rights, despite the absence of the word "privacy" anywhere in the text of the Constitution. While the contours of this right are debated, it exists firmly in at least two places. One is the freedom under the Fourth Amendment to be free from unreasonable searches and seizures, which turns on the "expectation of privacy" that Justice Harlan famously described in his concurrence in *Katz v. United States*. 96 The other is the right to personal autonomy, which began in the contraception case *Griswold v. Connecticut*, 97 wound its way through the abortion cases, 98 and recently reappeared in the sodomy law case of *Lawrence v. Texas*. 99

A right to privacy in the United Kingdom, on the other hand, is a very recent idea, emerging only in the last 10 years. The English Bill of Rights, passed by Parliament in 1689, included a few of the ideas in the American Bill of Rights, such as due process and freedom from cruel and unusual punishment. 100 But the act was really an assertion of parliamentary rights against the King, rather than an assertion of individual rights against Parliament. 101 For most of modern history, the concept of individual rights simply did not exist in England. 102

Shortly after World War II, however, the idea of a right to privacy began to emerge in Europe. As a response to the lessons of Nazi Germany, several European nations, including the United Kingdom, passed the European Convention on Human Rights (ECHR). 103 Among other basic rights, the Convention acknowledged a "respect for... private and family life." 104 But unlike firm rights

---

100. Bill of Rights, United Kingdom (1689).
102. Id.
like freedom of thought and religion, the right to privacy was cast in flexible terms. Under the ECHR, the right to a private life could be limited in the interests of “national security, public safety or . . . the prevention of disorder or crime.” Furthermore, this right was not even enforceable in British courts.

This changed, however, in 1998, when the newly elected Labour Party passed the Human Rights Act, making the European Convention rights enforceable in U.K. Courts. Geoffrey Marshall, a British Constitutional law scholar, describes the Human Rights Act as the first attempt at a modern bill of rights for U.K. subjects. But it is important to note how this Act relates to other British laws. Unlike the U.S. Bill of Rights, which can be used to declare a law unconstitutional, the U.K. Human Rights Act is only a guide for interpreting ambiguous legislation. Courts are not authorized by the Act to strike down legislation that conflicts with an individual right; instead they are encouraged to interpret laws, when possible, to accommodate its principles. When a statute conflicts with the Human Rights Act, but is clear in its meaning, it must be upheld.

This means that British subjects lack a meaningful remedy when the government invades their privacy. A subject who convinces a court that a British law violates her rights is not entitled to an automatic reversal of the law. All the court can do, under the Human Rights Act, is make a declaration that the law is “incompatible” with her rights. It is then left up to the government minister to do something about that, or not. This is small vindication for a successful plaintiff.

A look at recent cases confirms this. In the 1991 case Kaye v. Robertson, journalists went into the hospital room of a famous television actor who was recovering from a severe head injury. They ignored staff requests to leave and took photographs of the actor, who was incoherent at the time. The courts, while disgusted by the behavior of the reporters, lamented the lack of any remedy. In the court’s opinion, Lord Justice Glidewell stated: “It is well known

105. Id.
107. Id.
108. Id. at 113.
110. Id.
that in English law there is no right to privacy." Lord Justice Bingham agreed, stating "the case highlights, yet again, the failure of [British law] to protect in an effective way the personal privacy of individual citizens."

But a more recent case shows that the Human Rights Act is starting to change the landscape. In 2001, Michael Douglas and Catherine Zeta-Jones sued the magazine *Hello* over unauthorized photos of their wedding that appeared in the magazine. Their claims included one for breach of privacy, which was largely a test case for the new privacy protections of the HRA. And indeed, the court recognized, for the first time, a duty under the HRA to protect the privacy of an individual against the actions of another person.

While this is a significant development for British privacy rights, it should be noted that this applies only to horizontal claims between private parties, which has limited implications for challenging DNA collection laws. In theory, a British subject could bring a claim against the Forensic Science Service, the corporation that does the testing for the Home Office. But the right to privacy, as described in the European Convention, can be limited for "the prevention... of crime." And there is no legal avenue for a subject to have any provision of evidence law invalidated on privacy grounds. This stands in stark contrast to the system in the United States, where any defendant can challenge existing legislation under the Fourth or Fourteenth Amendments.

The divergent legal status of privacy rights in the United States and United Kingdom does not fully explain our varied approaches to DNA databases, however, for at least two reasons. First, while British subjects lack a direct means of challenging the laws as privacy violations, they still live in a representative democracy. The Home Office has been pursuing aggressive DNA collection for 13 years; if these tactics violated a deep sense of privacy held by a majority of the population, we would be seeing a strong attempt to limit them through political channels. Second, as noted earlier, the United

111. *Id.*
112. *Id.*
114. *Id.*
States is barely pursuing arrestee sampling and familial searching, despite any case law that prohibits it.

It may be that the British are more aggressive with their DNA programs, and the Americans more restrained, because aside from our legal understandings of privacy, our cultures fundamentally value privacy differently. This is a difficult quality to measure objectively, but evidence is frequently seen in the rhetoric of this debate, on both sides. Christopher Asplen, Executive Director of the National Commission on the Future of DNA Evidence, has said “[The British] system makes a tremendous amount of sense . . . but in the United States we have a different perspective on privacy and on the extent to which we would be willing to depend on a database.”

Baroness Helena Kennedy, Chair of the U.K. Human Genetics Commission, described the British reaction this way at a 2002 meeting of the U.S. President’s Council on Bioethics: “We are a rather passive, gentle nation it seems, because nobody has become particularly alarmed enough to make enough of an issue of this.” The psychological character of the British people is beyond the scope of this paper and the expertise of this author (as, for that matter, is the psychological character of Americans), but the point is that the difference between U.S. and U.K. DNA database programs is a product of more than just the structure of our constitutions and privacy laws.

Consider the use of closed-circuit television (CCTV) cameras in the United Kingdom for fighting crime and terrorism. The United Kingdom is the world leader in the use of public surveillance devices, particularly CCTV cameras. With over 2.5 million CCTV cameras in public places, the United Kingdom captures the average British subject on camera 300 times a day. Many of the CCTV cameras in the United Kingdom are able to compare the captured images against

a database of faces of people who are being sought by the police.\textsuperscript{121} The United States, on the other hand, is far behind the United Kingdom in public video surveillance and facial recognition technology.\textsuperscript{122} It seems unlikely, however, that the respective legal understandings of privacy explain this disparity. Surveillance of public places with CCTV cameras is clearly legal in the United States, because the technology is in use in several American cities, albeit on a smaller scale than in the United Kingdom.\textsuperscript{123} Yet Americans have been unwilling to accept public surveillance to the same degree as the British, despite the fact that fighting terrorism is a high priority for both countries.

There appears to be a general willingness among British subjects to sacrifice personal privacy in the interest of state security that Americans simply do not share, regardless of whether the security measure is constitutional. This is apparent not only in the current use of technologies like CCTV cameras and DNA databases, but also in the political discourse about the future of these programs. In October 2006, Prime Minister Tony Blair began calling for a DNA database profile of every British subject.\textsuperscript{124} It seems unimaginable that a candidate in the 2008 American presidential race would suggest such a thing.

V. Conclusion

The laws in this area are changing rapidly, and the coming years will likely show significant changes on both sides of the Atlantic. Arrestee sampling and familial searching are just getting started in the United States, and the British are only beginning to experiment with their newly enforceable privacy rights. But the differences that exist in our DNA database programs so far reveal more than the structure of our respective constitutions. The debate whether law shapes culture or culture shapes law is an old one, but it remains clear that Americans and British have very different cultural notions about

\begin{footnotes}
\item[122] Luk, \textit{supra} note 121, at 256.
\item[123] Donahue, \textit{supra} note 119, at 1188.
\end{footnotes}
privacy, and about the extent to which they will give up their privacy for effective law enforcement. And this should not come as a surprise, given our respective histories. The American Constitution was explicitly built to differ from the British model, and we continue to see the implications of that departure, even in cutting-edge law enforcement technologies of the 21st century.