FOUR

Policing with Big Data: DNA Matching vs Crime Prediction

Tom Sorell

Many large data sets are relevant to the detection and prosecution of crime. For example, DNA profiles can be extracted from databases and matched with samples collected at crime scenes to aid in the identification of suspects. There is evidence that storage and matching of DNA profiles not only solves particular crimes but reduces crime rates.[1] More controversially, patterns in the intensity and spread of burglaries in a city can inform opinions about where burglaries will occur locally in the future. Since liberal democracies promise the law-abiding that they will protect them from crime, do those jurisdictions not have an obligation to use relevant data sets to prosecute, and, where possible, prevent, crime? Even if the answer is 'Yes', those obligations may be limited significantly by liberal rights. Ordinary citizens have rights to pursue law-abiding activities unmolested, and the surveillance underlying some of the relevant data collection and matching may amount to a sort of molestation or at least an invasion of privacy. Besides, pattern recognition in crime data may be affected by bias in choices of characteristics that matter to crime, and data sets are subject to theft, deletion and contamination of various kinds.

In previous work, I have defended large-scale data collection and analysis of data in the prosecution and prevention of the most serious crime, including terrorism (Sorell 2011, 2016, 2018a, 2018b). In particular, I have tended to be sceptical of objections based on privacy to large-scale collection and analysis for those purposes. But, clearly, the propriety of using big data in policing decreases the less serious the relevant crimes are, the more speculative the algorithms generating the predictions and the less well governed the databases. The use of big data is also called into question

in jurisdictions that suffer from over-criminalisation, disproportionately severe punishment and very expensive legal representation. Differently, secrecy and the relative accountability of the collectors and users of the data matter to the democratic legitimacy of uses of big data. Police forces are not meant to operate out of sight of at least a subset of democratically elected legislators and the judicial system. Nor are they supposed to operate ad lib. They are subject to protocols intended to maximise the harmless liberty of those who are policed.

In this chapter I defend the construction of inclusive, tightly governed DNA databases, as long as police can access them only for the prosecution of the most serious crimes or less serious but very high-volume offences. I deny that that the ethics of collecting and using these data sets the pattern for other kinds of policing by big data, notably predictive policing. DNA databases are primarily used for *matching* newly gathered biometric data with stored data. After considering and disputing a number of objections to this practice, I conclude that DNA databases used in this way are ethically acceptable, if not valuable, contributions to legitimate policing.

DNA Databases

In developed liberal democracies DNA databases are composed of profiles rather than samples. A DNA sample is biological material that, under the right conditions and with the right techniques, can be used to identify a unique individual. A sample is also a basis for very probable inferences about an offender's gender, certain medical conditions and physical characteristics, such as eye colour. In both the US and UK, there are severe restrictions on the retention by the authorities, including the police, of DNA samples. DNA *profiles* are different. Each profile is a set of markers of gender and Standard Tandem Repeat (STR) DNA sequences – sequences that do not code for genes (and therefore do *not* sustain the inferences just mentioned). These profiles are virtually unique to a single human being – identical twins apart – and are excellent evidence of identity if derived from uncontaminated, undegraded DNA samples.

In the UK until 2008, DNA samples could be collected without consent from anyone arrested for virtually any crime. They could be kept permanently, whether or not people whose samples were taken were subsequently convicted. A European Court of Justice ruling in 2008 prohibited the retention of DNA profiles of people with no convictions. Rules introduced relatively recently in the UK limit the periods of time profiles can be retained for non-convicts. In general, the more serious the crime for which someone with no convictions is arrested, the longer a profile taken at the point of

arrest can be retained. Retention beyond three years sometimes requires a special application to an official, and five years tends to be the limit. However, it is still customary near the time of arrest for a profile to be checked for matches with samples independently collected from scenes of crime, and with profiles of convicted offenders, lest arrestees who have convictions but who are operating under an assumed name escape detection.

Although thousands of DNA profiles in the UK are now deleted annually in order to meet the provisions of the Protection of Freedoms Act (POFA) (UK Government 2012), the DNA database in the UK remains the largest in the world, with profiles of over 5 million people (out of a UK population of around 65 million). The deletion rules under POFA defer from the 2008 European Court of Justice ruling in *S and Marper* v. *UK* (Council of Europe 2008) – according to which keeping indefinitely the DNA profiles and fingerprints of people who were once suspected of a particular crime but who have been acquitted, infringes their right to private and family life. The Court particularly objected to a police practice in England and Wales that made collection and retention of biometric data routine for adults and minors alike, regardless of the severity of the crime. (S had been a child suspect in a burglary case, and Marper was charged with harassment in a case brought by a partner who subsequently resumed a relationship with him.) The Court did not object to the general purpose of the collection and retention of biometric data, namely, the detection and prosecution of crime. Its focus was on the disproportionate effects of pursuing that policy on Marper (against whom harassment proceedings were dropped) and S, a child when arrested, who was acquitted).

The Privacy Objection

Without denying that the former collection and retention policy in the UK was heavy-handed in the case of *S and Marper*, must we say that there are objections on the basis of the value of privacy or other values to any DNA database that covers 8 per cent of the population? It is not obvious to me that we must.

Violations of privacy, as I have tried to argue in the past (Sorell 2011, 2018b; Guelke and Sorell 2017), are penetrations of zones conventionally protected from observation or reporting. The zones in question are those of the body, the home and the mind.[2] By 'the body' is meant primarily the exposed or naked human body. The conventions of covering the body or, differently, of not uncovering the body, support a convention of refraining from surveillance of the body. Looking at close quarters is intrusive unless it is invited, and so is camera surveillance, which produces pictures

simulating direct visual experience of the body. Privacy conventions put the control of exposure of the body in the hands of the self, and limit the unwanted social effects of observation or reporting about the body by others.

The home, for the purposes of this chapter, is the default location occupied daily by a person when not otherwise active. It is the zone where people rest and sleep and expect to be safe when engaged in either. There can be temporary default locations, like hotel rooms, or passenger aircraft or cars that also count as home spaces, and the conventions for not entering or inspecting the home uninvited can apply to the hotel room or one's airline seat. These, too, are normally not to be observed or reported on without the permission of the person whose space it is.

The third and most important zone of privacy is the mind, understood as the set of capacities for arriving at what to believe and what to do. The mind is not, for our purposes, private in the sense – famously called into question by Wittgenstein – of being accessible only to the subject, or being the place where 'what it is like' to experience something registers. It is *normatively* private, meaning that it is wrong to force people to disclose their thoughts or convictions or to think aloud in some substantial sense (Nagel 1998). Especially in contexts where there is some strongly enforced political or religious orthodoxy, and expectations that each person will publicly proclaim adherence, the freedom to make one's own mind up privately – *without* thinking aloud and without declaring one's possibly unorthodox conclusions – comes into its own.

More generally, the mind is the arena where, by arriving at reasons for beliefs, or beliefs on the basis of reasoning, one *makes* those beliefs one's own. In the absence of the normative privacy of the mind people are likely to be mouthpieces for the views of their parents, religious or political leaders, or their class. The normatively private mind is also in some sense the *pre-eminent* zone of privacy, because it is by using its capacities that an adult in a liberal democratic society can determine the limits of exposure of the body and public access to the home. Normative mental privacy, then, is typically a condition of an individual's governance of other normatively private zones, but not the other way round.

If privacy is what one enjoys when experiential and informational access by others to one's body, home, beliefs and choices is significantly limited, then it is easy to see that privacy facilitates the exercise of autonomy. The normative privacy of the mind helps one to think and choose for oneself, but the public conventions licensing limited access to the home also facilitate the exercise of the capacity to choose and to believe for reasons. It is at home that one can be oneself and expose oneself most easily, and the home

space therefore provides opportunities for trying on different views with one's friends and family before expressing them publicly.

Privacy is often, but disputably, connected with being in control of information about oneself. I say this is disputable, because loss of control, or absence of control, does not necessarily amount to a violation of privacy. When a powerful politician tries to prevent publication of damaging but accurate information about him- or herself – for example, the fact that he or she has taken a bribe – that is not necessarily a case of preserving the privacy of properly private information, and when, despite the politician's efforts, the information becomes generally known, that is not necessarily a violation of privacy. It could instead be a case of people finding out what a public figure is really like, which might properly affect their votes in a future election. This is because there is a legitimate public interest in news of the bribe: electors are entitled to know whether their representative's votes can be bought with money, especially where the use of paid-for influence could go against the interest of constituents.

On the other hand, publishing photographs of the interior of the politician's home to satisfy newspaper readers' curiosity about what it looks like is a violation of privacy quite apart from the politician losing control of the information in the photos. This is because of conventions that define the privacy zone of the home are so well entrenched in everyone's thinking about privacy.

How do DNA samples and DNA profiles fit into this picture of the protected zones? DNA *samples* certainly give a scientifically trained third-party insight into a person's body and even the bodies of members of that person's biological family, their parents in particular. Publicising some of this information could disadvantage those with identifiable genetic predispositions to expensive and hard to insure, or stigmatised, medical conditions. Even if the information were not public but were disclosed only to the person whose DNA it is, knowledge of the condition could drastically reduce quality of life. These adverse consequences of the availability of DNA samples do not show that DNA samples should never be taken or be the subject of published research. At most they call attention to the importance of insurance safety nets and the difficulty of adjusting to news that indicates one's days are numbered.

What about the fact that information derived from a DNA sample is for all intents and purposes *uniquely* identifying? What does this have to do with privacy? Claims that DNA is essential to a person's *identity* do not mean that sequencing or collecting DNA is more intimate than collecting, say, information about a person's preferred sexual practices or their sexually transmitted diseases, which are often *not* uniquely identifying.

It is true, as already acknowledged, that genetic information may need protection or rationing for communicative purposes, for example, because it will trigger prejudices and disadvantage someone. But this is not to say that just any disadvantageous information about a person is therefore private and incommunicable. The fact that someone has been convicted of murder is normatively public (because the result of a normatively public trial), *not* private.

The collection of uniquely identifying information, including genetic information, is not necessarily more of an intrusion than the confiscation of a diary. On the contrary, it can be entirely non-intrusive, because the information in question is not personally revealing. For example, the fact of being female and winning two Nobel prizes uniquely identifies Marie Curie (so far), but a contemporary of Marie Curie who knew only this fact did not come close to knowing Marie Curie 'personally', and fell even further short of being aware of private information about her. The same, I think, is true of knowing the results of the sequencing of one's own DNA. To know this sequence is to have impersonal knowledge, albeit biologically revealing knowledge, of someone. This is not necessarily private in the sense of penetrating a protected zone.

The fact that DNA is uniquely identifying does not show that it is tied to no-one else. If it is private or private property, it is private property shared by someone with their genetic parents, siblings and children. So not only is the inference from

(1) X uniquely determines the identity of person P

to

(2) X is private to person P

disputable,[3] in view of the inheritance of half of one's genetic material from each of one's parents. So, too, is the inference from (1) to

(3) Third-party collection of X violates P's privacy, *ceteris paribus*.

But, in any case, most DNA databases are *not* collections of DNA samples but of DNA *profiles*, which are much less revealing than DNA samples even if, for all intents and purposes, uniquely identifying.

The Suspect Population Objection

A second objection to large-scale collection and storage of DNA profiles arises from the size of the DNA database when it contains, as it does in the

UK, profiles of around 8 per cent of a large population. This time the problem concerns the relation between police and citizens in a liberal democracy. A citizenry is supposed to control and authorise the actions of police through representatives who legislate in the interests of everyone or most people in the jurisdiction. When law enforcement holds potentially incriminating information on so many, is not the direction of the control reversed, so that police and not citizens have the whip hand?

A related question is asked about the use by the police of large-scale closed circuit television systems whose cameras are openly trained on large public spaces. Does not this kind of surveillance either make a population suspect or help to keep them under the thumb of the authorities? Granted that the police are not *actively* targeting each person in those large spaces for attention, is not the indiscriminate retention of the images of so many, and in places where levels of crime may not be high, an expression of distrust or suspicion of the population? It is no more an expression of distrust or suspicion than the fact that everyone is now checked at airports before boarding. The authorities know that very few people come to the airport with concealed explosives or weapons. Still, the consequences, if just a few people are successful, are so great in lives lost, injury suffered and fear created, that sweeping searches are arguably not disproportionate. Nor are they discriminatory, since the premise of the argument that they *are* disproportionate is that *everyone* is treated the same way.

In the case of the national DNA database in the UK, there is no question of the collection of data turning people *into* suspects, as allegedly happens with mass surveillance. If anything, it is the other way round: only if someone is already officially suspected for some crime inasmuch as they have been *arrested*, does their profile get added to the database. Against this background, the collection of DNA samples is far less indiscriminate than the collection of CCTV images, and might for that reason be more proportionate as well.

Not only must subjects of DNA profiles reach a non-trivial threshold – arrest – to be included at all in the UK national DNA database, further non-trivial conditions need to be met if those profiles are to be retained for more than three years. There are three kinds of relevant suspects: (a) convicted; (b) unconvicted but charged with a relatively serious or 'qualifying' offence under the Protection of Freedoms Act; and (c) those charged with or arrested for a relatively minor offence. There is no retention in type (c) cases except by permission of the UK Biometrics Commissioner. Type (b) cases involve the retention of profiles for three years with the possibility of applying to the Biometrics Commissioner for a two-year extension. Type (a) cases call for indefinite retention of profiles. There is more lenient

treatment for offenders under 18 with a single conviction, and guidelines for early deletion of profiles in a range of special cases (UK Government 2016: 30–1, table 6a).

The large size of the UK DNA base notwithstanding, the current restrictions on inclusion and retention of profiles seem sufficient to rebut the charge that it is an instrument for making a whole population suspect. Indeed, the restrictions rebut the charge that the DNA regime is disproportionately unforgiving of the population of arrested people or the population of previously charged people.

Whole Population DNA Profiling

I have argued that collecting DNA profiles of arrestees falls well short of making a whole population suspect. Would collecting DNA profiles not involve injustice, however, if arrestees, and therefore profiles, were overwhelmingly from a section of the population who was despised, or subject to some kind of prejudice? Here the answer is 'Yes'. In the UK, as it happens, profiles are currently in proportion to the ethnic mix of the country, with, in particular, the majority white population being reflected in the proportion of white people's profiles in the DNA database (UK Government 2016: 11, fig. 3b). It has not always been this way (*Independent* 2007). Indeed, it is conceivable that in another jurisdiction, or even in a possibly illiberal future UK, arrests and convictions would start conspicuously to disadvantage minority or ethnic populations. In jurisdictions of that kind, there would be an argument for reforming conditions under which someone could be arrested.

But would there not also be an argument for treating majority and minority populations alike by collecting DNA profiles of *everyone*? This would counteract some effects of prejudice in arrests, and would obviate the singling out of arrestees for DNA profiles. But would not *that* have the effect precisely of making a whole population suspect, if what the profiling was for was to find those guilty of any crime? And what if the jurisdiction in question were characterised by over-criminalisation and unduly severe sentences?[4] Would not universal collection of DNA profiles make it easier for unjust governments to convict anyone of offences that should not exist in the first place?

Let us for now leave aside special issues arising from over-criminalisation and unduly severe sentences: is there anything wrong with collecting profiles of everyone in a jurisdiction in which criminalisation and sentencing do seem proportionate, and arrests are not discriminatory? For example, if we hold constant the current range of criminal offences, sentences and investigatory techniques in the UK, what would be wrong with trying to

match crime scene profiles with the profiles of 65 million people rather than 5 million profiles? (Smith 2006; Seringhaus 2009).[5] Unless one thinks (incorrectly, in my view) that knowledge of a DNA profile gives whomever has it dangerously direct access to the profile-owner's identity, allegedly the most private information of all, I do not see what is morally wrong with this idea on its face. Universal DNA profiling would support both law enforcement and the rule of law. It would treat everyone the same. If the current UK rules for accessing the database were preserved, the number of officials able to get at it would be extremely small.

Would universal profiling make a whole population suspect? That depends on whether inclusion in a universal database is enough to make one a suspect. I have already expressed scepticism about the related idea that the policy of checking every airline passenger for dangerous implements makes every airline passenger a suspect: a person can be checked just because checking everyone is thought to be the best (fairest and most thorough) way of finding dangerous substances or devices. Such a regime is compatible with checks on people who are regarded by the checkers and everyone else as very improbable potential terrorists. Universal checks in the *absence* of universal suspicion is what we find in airports.

What about being included in a universal DNA database? In some ways this is much *less* likely to trigger suspicion than being a traveller at an airport: the threshold for being singled out for investigation is much higher than in an airport where everyone is put through a scanner individually and sometimes searched. Most profiles in a universal database would lie permanently inert and unexamined on the database. Only a small minority would get attention, and only when a profile derived from a crime scene was run through the system and got a match. Until that occurs, a universal DNA database with a capacity for matching makes *no one* a suspect.

Furthermore, and just as important, the matching procedure is able to establish conclusively, and without the intervention of interested parties, including police with strong hunches, that someone's DNA does *not* match crime scene DNA. In this way, it can counteract the unreasonable suspicions, or the reasonable but mistaken suspicions, of investigating officers. A burglary may look to a policeman to be the characteristic work of X, whom the policeman has arrested many times, but if the profile extracted from the DNA found at the scene fails to match X's profile, then the work of showing X is the culprit gets harder, not easier. In conjunction with the presumption of innocence, a failure to match is a strong basis for reasonable doubt in the absence of other compelling evidence.

I am claiming that universal searches of people's bags and clothing at airports are more likely to be heavy-handed and clouded by prejudice than

inclusion in a DNA database capable of identifying matches. This is precisely because the threshold for becoming a suspect is a DNA match and *not* mere inclusion on a database. In the airport case, merely starting the process of moving to a boarding area is enough for being searched. But in the universal DNA collection case, according to me, there is no counterpart of this low threshold for attracting the individual interest of the authorities.

In American jurisprudence my claim would be challenged, because taking a DNA sample is itself construed as a search under judicial interpretation of the Fourth Amendment to the US Constitution. American jurisprudence calls for a search to be reasonable, and although taking DNA through a mouth swab might be reasonable in the context of a reasonable arrest (US Supreme Court 2013) – for the purpose of collecting uniquely identifying information about the arrestee – search under a policy of taking DNA from everyone – whether arrested or not – would *not* count as reasonable. DNA would be taken not for the legitimate purpose of investigating a particular crime, but for the allegedly questionable purpose of eliminating most people from enquiries into any crime for which DNA evidence existed.

Does a buccal swab for DNA amount to an unreasonable search when such swabs are taken from everyone? That depends on the acceptability of treating DNA sample-taking as a 'search' in any sense of that term. A 'search' in the primary sense is systematic examination of the contents of a place. Presumably, taking a DNA sample is, in some metaphorical sense, a 'search' of a person or a person's body or a person's genome. But is it literally a search of this kind? It is not.[6] Taking the DNA sample is not necessarily a step in sequencing a person's genome, and the profile used in matching does not code for genes connected to a person's physical characteristics. At most it is a search in someone's 'junk' DNA for standard tandem repeats.

Although distinctive for each person, making a profile from STR does not seem to involve intrusion in the sense of revealing something incriminating, secret, hidden, embarrassing, deeply felt, deeply considered or deeply valued. Again, submitting to a buccal swab for a DNA sample is not to undergo a search of one's body or person except on some false assumptions about the relation of a profile to a body or a person. So the usual moral connotations of 'unreasonable search' in the ordinary sense of 'search' are missing.

If all this is right, it is not clear that universal data-profiling does involve unreasonable searches on a large scale. It is also not obvious (at least to me) that there would be much wrong with permanent retention of DNA profiles, if that practice extended to everyone rather than arrested people and convicts only. It is true that it is difficult now to remove the associations with suspects and convicts of retained DNA profiles, so that extending

profile collection and retention to everyone would probably be construed now by the public as treating a whole population as criminals. I do not deny that this is probable or that it counts against a universalisation of profile collection and retention starting now. What I do deny, for reasons already given, is that is universal profile collection and retention actually criminalises a population.

So there is nothing necessarily wrong, according to my account, with universal DNA profile collection. This is different from saying that things never do or would go wrong if everyone's profiles were collected. In developed liberal, criminal jurisdictions, profile-matching produces a few false positives, and it can give erroneous results when DNA samples are contaminated or minute. A high false positive rate can and ought to undermine the use of a forensic technique. The more common it is for erroneous results to be produced in a jurisdiction, the more formidable the problems with convicting on the basis of DNA evidence. It is also true that false inferences can be drawn from the actual presence of someone's DNA at a crime scene. Mere presence at a scene is a ground for further investigation of the person whose DNA it is, but not necessarily for charges or a conviction. In addition, I have already conceded that in jurisdictions which suffer from overcriminalisation and disproportionately severe penalties, convictions should not necessarily be made easier by resort to DNA collection for *every* crime. The moral necessity of reducing the crime rate varies with the degree to which criminalisation and sentencing are reasonable and liberal democratic protections for suspects are in force. These are risks, but unless there is a high probability of their being realised, they do not rule out universal DNA databases in jurisdictions with the usual due process protections.

Repurposing Data

DNA can be collected for one purpose and used for another. It can be collected from someone arrested on suspicion of a particular crime and yet be used in an investigation of that suspect's family when a crime scene sample throws up a partial match. Is repurposing a risk particularly associated with DNA databases? Elizabeth Joh (2014) has suggested as much. She thinks that this risk arises particularly in big data research, because, according to her, big data research departs from standard methods of collecting data for research purposes. She claims that, standardly, researchers form hypotheses and selectively collect data that would confirm or falsify them. With big data, it is the other way round. It starts with comprehensive collection, and then identifies patterns that it interrogates for commercial, forensic or other purposes. For example, a sudden increase in Google searches for cold and

'flu symptoms might give early warning of a 'flu epidemic. If search data were correlated with location data for those searching, it might be possible to map the spread of the epidemic.

As this example shows, not all repurposing of data is sinister or in the service of some narrow self-interest. So, why should repurposing in general be flagged up as a danger? Again, *is* it true that research outside big data research – standard research – takes account only of data collected by researchers for the confirmation and disconfirmation of hypotheses arrived at by those researchers? To take this last question first, the answer is a clear 'No'. Data sets are often comprehensive and made available as a national research resource to answer questions that did not originally generate the data sets. For example, the British Household Panel Survey (BHPS 2018) is a multi-purpose study stretching over nearly thirty years, and is both usable and used for spotting patterns in much the way that more quickly collected and analysed internet-derived data sets are.

There are many repurposings of data sets that seem to me to be unobjectionable, because a new purpose served is a legitimate purpose, including a criminal justice purpose. CCTV camera output is a case in point. It is collected from many different cameras, installed for different purposes. For example, in petrol stations, cameras collect number plate data and images of customers, in case drivers fill up and drive off without paying. But the same images can establish where and when a victim was last seen in a murder investigation. Relatedly, data collected from mobile telephone masts can establish locations of mobile telephones and their users in a murder investigation. Surely these repurposings are entirely in order? The seriousness of the crime and the urgency of identifying, arresting and prosecuting culprits trumps privacy interests related to telephone location data and images of people in public places.

The less serious the crime, the less might be the moral justification for using CCTV camera footage collected for one purpose and used for another purpose.[7] For example, burglary is a less serious crime than murder: it does less harm to its victims, other things being equal. But it is a very high-volume crime: there are many burglaries in many places doing considerable harm, though not usually fatal harm, to many victims. The volume of this kind of crime counts towards it being classified as relatively serious, and towards the repurposing of CCTV camera data or other data, for the solution of burglaries.

Although Joh approvingly quotes David Lazer and Viktor Mayer-Schonberger as saying that the DNA samples from which profiles are derived *invite* repurposing (Joh 2014: 53–4), in the UK at least they are mostly destroyed

very soon after a profile is derived. Since repurposing requires the preservation of these samples, the 'invite' claim seems tendentious, at least in relation to Great Britain.

Conclusion

Big data in policing does not always constitute a risk to a policed population. The use of DNA databases seems to me to be both relatively non-intrusive and reliable in the identification of suspects for elimination from enquiries. Other big data applications are more questionable the more they have pretensions to predict and profile accurately. Overall, big data is not making whole populations suspect in democracies. Nor do certain kinds of big data reach right into the essence of an individual identity. The real risks are closer to the surface: high false positive rates for some methods of biometric identification, and questionable assumptions associated with certain algorithms that aspire to the prediction of crime.

Notes

1. See Doleac, Anker and Landerso (2017). The criteria used to judge a DNA database as 'effective' are themselves fairly crude. See Walsh, Curran and Buckleton (2010).
2. The next nine paragraphs are adapted from Sorell (2018a, b).
3. I disagree with the view that is attributed to Baroness Hale of Richmond in the judgement in *S and Marper v UK*: 'Baroness Hale of Richmond disagreed with the majority considering that the retention of both fingerprint and DNA data constituted an interference by the State in a person's right to respect for his private life and thus required justification under the Convention. In her opinion, this was an aspect of what had been called informational privacy and there could be little, if anything, more private to the individual than the knowledge of his genetic make-up' (Council of Europe 2008: 5).
4. As Douglas Husak has argued is the case in the US (Husak 2008).
5. In the UK Lord Justice Sedley was a proponent of a universal database in 2007, when certain racial groups were over-represented in the profiles. As he understood it, visitors as well as UK residents or nationals would have profiles on the database (Independent 2007).
6. For further criticisms of anachronistic understandings of informational technology in Fourth Amendment jurisprudence, see Kerr (2004) and Solove (2002).
7. For a criterion of serious crime, see Sorell (2016).

References

BHPS, *British Household Panel Survey* (Colchester: University of Essex), 2018, available at: https://www.iser.essex.ac.uk/bhps, last accessed 22 May 2018.

Council of Europe, Case of *S and Marper* v. *The United Kingdom*, 2008, available at: https://rm.coe.int/168067d216 p.5, last accessed 22 May 2018.

Doleac, J., A. S. T. Anker and R. Landerso, 'The Effects of DNA Databases on the Deterrence and Detection of Offenders', 2017, available at: http://jenniferdoleac.com/wp-content/uploads/2015/03/DNA_Denmark.pdf, last accessed 22 May 2018.

Guelke, J. and T. Sorell, 'Violations of Privacy and Law: the Case of Stalking', *Law, Ethics and Philosophy* 4 (2017): 32–60.

Husak, D., *Overcriminalization* (Oxford University Press, New York, 2008).

Independent, The, 'Top Judge: Put Everyone on DNA Database', *Independent*, 5 September 2007, available at: http://www.independent.co.uk/news/uk/crime/top-judge-put-everyone-on-dna-database-401447.html, last accessed 22 May 2018.

Joh, E., 'Policing by Numbers: Big Data and the Fourth Amendment', *Washington Law Review* 89 (2014): 35–68.

Kerr, O. S., 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution', *Michigan Law Review* 102 (2004): 801–88.

Nagel, T., 'Concealment and Exposure', *Philosophy & Public Affairs* 27(1) (1998): 3–30.

Seringhaus, M. R., 'Forensic DNA Profiles: Database Expansion, Familial Search, and a Radical Solution', *Association for the Advancement of Artificial Intelligence*, 2009, 150–4, available at: https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1187/1503, last accessed 22 May 2018.

Smith, M. E., 'Let's Make the DNA Database as Inclusive as Possible', *Journal of Law, Medicine and Ethics* 34 (2006): 385–89.

Solove, D., 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy', *California Law Review* 75 (2002): 1083–167.

Sorell, T., 'Preventive Policing, Surveillance and European Counter-terrorism', *Criminal Justice Ethics* 30 (2011): 1–22.

Sorell, T., 'The Scope of Serious Crime and Preventive Justice', *Criminal Justice Ethics* 35 (2016): 163–82.

Sorell, T., 'Organized Crime and Preventive Justice', *Ethical Theory and Moral Practice* 1 (2018a): 137–53.

Sorell, T., 'Bulk Collection, Intrusion and Domination', in A. I. Cohen (ed.), *Essays in Philosophy and Policy* (Lanham, MD: Rowman & Littlefield, 2018b).

UK Government, 'Protections of Freedoms Act', 2012, available at: http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted, last accessed 22 May 2018.

UK Government, 'National DNA Database: Annual Report 2015–2016', 2016, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594185/58714_Un-Num_Nat_DNA_DB_Accessible.pdf, last accessed 22 May 2018.

US Supreme Court, *Maryland* v. *King*, 2013, available at: https://www.supremecourt.gov/opinions/12pdf/12-207_d18e.pdf, last accessed 22 May 2018.

Walsh, S., J. Curran and J. Buckleton, 'Modelling Forensic DNA Database Performance', *Forensic Sciences* 55 (2010): 1174–83.