Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime?

Oliver M. Tuazon *, †

Maastricht University, Faculty of Law, Forensics, Criminology and Law Program, Maastricht 6211 LH, The Netherlands
*Corresponding author. E-mail: omtuazon@up.edu.ph

ABSTRACT

Universal forensic DNA databases are controversial privacy-wise given their omnibus scope of incorporating DNA profile data of the entire population into the system. Following the landmark decision of the European Court of Human Rights on the retention of DNA profiles in S. and Marper v. the United Kingdom, two differing opinions emerged on its application to universal databases: their acceptability and illegality. This paper makes use of the elements of the right to respect for private life (Article 8 ECHR), distilled from the Court’s jurisprudence involving collection and retention of DNA profile data, in the form of tests—preliminary interference, legality, legitimate purpose, and proportionality—in assessing the feasibility of establishing population-wide DNA databases in Europe.

KEYWORDS: DNA profile collection and retention, population-wide database, right to respect for private life, data protection, legal safeguards

† A member of the Philippine Bar, he finished his LLM in Forensics, Criminology and Law at Maastricht University, where a major part of the research for this article was conducted. He also holds a master of science degree in Microbiology under a sandwich program, where he did his course work at the University of the Philippines, and thesis work at the Massachusetts General Hospital under a professor from Harvard Medical School. He is currently an external PhD candidate at the Center for Law and Digital Technologies (eLaw) of Leiden University.
I. INTRODUCTION

Forensic DNA databases have become an integral component of criminal justice systems in many jurisdictions around the world since the successful application of DNA evidence in solving a double-murder case in England in the mid-1980s. Existing forensic databases only contain DNA profiles of convicted felons, and to some extent, arrestees. DNA databases that are used in criminal investigations and court proceedings are called ‘forensic’ DNA databases, as distinguished from ‘medical’ databases or biobanks. When they include the entire population of a given country, they are called ‘universal’ forensic DNA databases. The word ‘universal’ can be substituted with any of the followings words to refer to the same database: ‘population-wide’, ‘comprehensive’, or ‘compulsory’. For the sake of brevity, the phrase ‘universal database’ is used in this article to refer to the same concept.

In 2003, the feasibility of a universal database was proposed for the first time. These universal databases promise to yield greater investigative and deterrent capacity, reduce racial/ethnic polarization, and in the presence of strict legal safeguards, even better privacy protection than the present DNA collection and retention regimes. A renewed call for the creation of universal databases was made in 2018 with the challenge, ‘Is it time for a universal genetic forensic database?’ The topic has become a subject of debate, especially in the United States, and its theoretical application has been evaluated in Australia. But there is a dearth of research about the topic in Europe, where it is treated almost as a taboo.

When the European Court of Human Rights (ECtHR) issued its landmark decision involving DNA profiles in *S. and Marper v. the United Kingdom*, two opinions emerged as to its application to universal databases. One author claimed that ‘a database of all citizens would be acceptable’ whereas another downrightly...

---

1 J.M. Butler, *Fundamentals of forensic DNA typing* 5 (2010).
2 N. Van Camp & K. Dierickx, *The retention of forensic DNA samples: A socio-ethical evaluation of current practices in the EU*, 34 J Med Ethics 606, 607 (2008).
3 See H. Machado & S. Silva, *Public participation in genetic databases: crossing the boundaries between biobanks and forensic DNA databases through the principle of solidarity*, 41 J Med Ethics 820 (2015).
4 D.H. Kaye & M.E. Smith, *DNA identification databases: Legality, legitimacy, and the case for population-wide coverage*, 3 Wis. L. Rev. 413 (2003).
5 Id. see also D.H. Kaye & M.E. Smith, *DNA databases for law enforcement: the coverage question and the case for a population-wide database, in DNA and the criminal justice system: the technology of justice* 272 (D. Lazer ed., 2004).
6 K. Dedrickson, *Universal DNA databases: a way to improve privacy?*, 4 J. Law Biosci. 537 (2017).
7 J.W. Hazel, et al., *Is it time for a universal genetic forensic database?*, 362 Science 898 (2018).
8 Authors from both sides of the debate wrote separate chapters under Part II (Balancing Privacy and Security) in D. Lazer (ed.), *DNA and the criminal justice system: the technology of justice* (2004).
9 M. Smith, *Universal forensic DNA databases: Balancing the costs and benefits*, 43 Altern. Law J. 131 (2018).
10 Other countries like Kuwait and Saudi Arabia have also considered setting up universal DNA databases; see Hazel, et al., supra note 7, at 898.
11 The European Court of Human Rights is referred to in this article as ‘ECtHR’, or simply ‘the Court’.
12 D. Townend, *EU laws on privacy in genomic databases and biobanking*, 44 J Law Med Ethics 128, 139 (2016).
rejected universal databases as ‘illegal’ at least for Europe.13 What is the real score?

At the outset, two things are clear: first, the Court has not been asked to directly adjudicate on a case involving universal databases;14 and second, a future case involving the retention of DNA profiles in universal databases will be evaluated under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),15 also known as the right to respect private life.

In Marper, the Court found a violation of the applicants’ right to respect for private life based on the respondent state’s practice of retaining DNA profiles of suspected but un-convicted individuals. More recently, the Court found a similar violation in retaining DNA profiles—in Gaughran v. the United Kingdom16 and Trajkovski and Chipovski v. North Macedonia17—this time of convicted applicants. These cases demonstrate that the Court does not base its finding of a violation of the right to respect for private life on the conviction of the applicant. The common ratio deci dendi for the violation refers to the lack of sufficient legal safeguards in the relevant national DNA database law. Can the same judicial reasoning be applied to a universal database, which includes the DNA profiles of all the citizens of a member state?

The ECtHR has been consistent in affirming that the right to respect for private life is not an absolute right and that it is the Court’s role to balance it with other legitimate rights of individuals (private interests) and society (public interests).18 This article aims to determine on which scale the creation of universal databases would tilt using the elements employed by the ECtHR itself in adjudicating the presence or absence of a violation of the right to respect for private life, namely, the preliminary interference test, and the three main tests of legality, legitimate purpose, and proportionality. In the course of the analytical process, due consideration was given on whether legal safeguards could be formulated to allow the creation of universal forensic DNA databases following the ECtHR regime.

13 A. Santurtún, et al., Fundamental rights regarding forensic databases: Review and analysis of Kuwait’s law 78/2015, 43 Span. J. Leg. Med. 79, 84 (2017).
14 In Gaughran, the Court made an obiter dictum—since the case was on another albeit related issue—on universal databases labeling them as ‘excessive and irrelevant’; see Gaughran v. the United Kingdom, no. 45245/15 ECtHR paras. 1–103, 89 (Feb. 13, 2020). Aside from being a mere judicial opinion outside the litigated issue, the ruling includes storage of data of deceased persons which does not apply squarely to universal databases as described in this article. It would be superfluous to retain profiles of the dead since only living persons can commit crimes although they may be kept at the inception of a universal database system to help resolve outstanding cold cases.
15 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, ETS No. 5 (Council of Europe, 1950). Hereinafter referred to as ‘ECHR’ or simple, ‘the Convention’.
16 Gaughran, ECtHR.
17 Trajkovski and Chipovski v. North Macedonia, nos. 53205/13 and 63320/13 ECtHR paras. 1–59 (February 13, 2020). Note that Chipovski cites Gaughran, although they bear the same judgment date; see id. at 32.
18 European Union Agency for Fundamental Rights, Handbook on European data protection law, 37, https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed Jan. 19, 2021).
II. COLLECTION OF SAMPLES AND THE PRELIMINARY INTERFERENCE TEST

II.A. Are DNA Profiles Protected Data under ECHR?

Given the tendency of the Court to interpret the Convention as a ‘living document’, its case law has made the concept of private life so broad and ‘not susceptible to exhaustive definition’, to which DNA profiles as protected personal data have been included. The main reason behind this classification is that DNA profiles contain ‘substantial amounts of unique personal data’, which can be used to detect possible ‘genetic relationship[s]’ among individuals—such as when familial or ethnic searching is employed—which the Court considers to be ‘highly sensitive’. The same reasoning can be easily transposed to universal databases because they are a collection of DNA profiles from the entire population. Hence, a future case on this subject will be clearly classified by the Court as protected personal data under the right to respect for private life (Article 8 ECHR).

II.B. Is There Interference in Universal Databases?

From Van der Velden (2006) to Marper (2008) and W. (2009), and later in Martens (2013) and Aycaguer (2017), up to the most recent cases involving DNA profiles, Gaughran (2020), Chipovski (2020), and Petrović (2020), the Court has consistently ruled that the collection of cellular samples amounts to an intrusion upon a person’s private life. Their systematic retention goes beyond the scope of neutral identification making it ‘sufficiently intrusive’ to constitute an interference with the right to respect for private life. In other words, individuals have a reasonable expectation of privacy when it comes to their own personal data in the form of

---

19 A.W. Heringa, Constitutions compared: An introduction to comparative constitutional law 256 (2016).
20 P.G. and J.H. v. the United Kingdom, no. 44787/98 ECHR paras. 1–96, para. 72 (Sep. 25, 2001).
21 Marper, ECHR at para. 103.
22 D.J. Harris, et al., Law of the European Convention on Human Rights 538–40 (2018).
23 Marper, ECHR at para. 75. See also Gaughran, ECHR at para. 81.
24 Van der Velden v. the Netherlands, no. 29514/05 [dec] ECHR (Dec. 7, 2006).
25 Marper, ECHR at para. 77.
26 W. v. the Netherlands no. 20689/08 [dec] ECHR (Jan. 20, 2009).
27 Peruzzo and Martens v. Germany, nos. 7841/08 and 57900/12 ECHR paras. 1–58, para. 33 (June 4, 2013).
28 Aycaguer v. France, no. 8806/12 ECHR paras. 1–47 (June 22, 2017). In this case, the Court made use of an earlier case (not involving DNA profiles) to affirm that mere storage of personal data amounts to an interference within the meaning of private life under Article 8 ECHR; see Leander v. Sweden, no. 9248/81 ECHR paras. 1–84, para. 48 (Mar. 26, 1987).
29 Gaughran, ECHR at para. 63.
30 Chipovski, ECHR at para. 43.
31 The latest decision of the Court on this issue provides this summary: ‘The taking and retention of a DNA sample has furthermore been deemed to amount to an interference with the individual’s “private life” within the meaning of the same provision . . . ’; see Dragan Petrović v. Serbia, no. 75229/10 ECHR paras. 1–98, para. 69 (Apr. 14, 2020).
32 Chipovski specified it for DNA profiles: ‘ . . . DNA profiles clearly constitute data pertaining to one’s “private life” and their retention amounts to an interference with the right to respect for one’s private life, within the meaning of Article 8 § 1 of the Convention . . . ’; see Chipovski, ECHR at para. 43.
33 Van der Velden, ECHR.
34 Although not a conclusive factor, the ‘reasonable expectations as to privacy’ of a person is evaluated to determine the existence of an interference; see P.G and J.H, ECHR at para. 59.
DNA profiles.\textsuperscript{35} Would the same apply to universal databases? If the Court found an interference when samples from arrestees and convicts were collected, \textit{a fortiori}, it is expected that the Court would find a stronger and more serious interference when samples are collected from the entire population.\textsuperscript{36} Whether such serious infringement will pass judicial muster is determined through the three tests of legality, legitimate purpose, and proportionality in the succeeding sections. Before applying these tests to universal databases, this section educes a necessary legal safeguard on the collection of DNA profiles.

\section*{II.C. Rationale on the Collection Coverage}

The Court rulings imply that collection of DNA profiles of arrestees and their retention upon conviction may constitute a lawful interference to the right to privacy when sufficient safeguards are available. But why limit the coverage to convicts? The Court appears to be following the predictivist or recidivism theory,\textsuperscript{37} that is, a person who has been convicted is more likely to commit other crimes in the future.\textsuperscript{38} In this regard, \textit{Marper} noted the utility of databases in identifying ‘future offenders’.\textsuperscript{39} More recently, the Court in \textit{Chipovski} applied the reasoning behind inclusion in a national sex offender register\textsuperscript{40} to the retention of DNA profiles in national databases claiming that it helps in ‘combating recidivism’.\textsuperscript{41} While convicts may re-offend, it does not mean that all future crimes will be committed by them.\textsuperscript{42}

\textsuperscript{35} One author actually argued that the public has no reasonable expectation of privacy regarding their DNA information given that they keep on shedding cellular material from which DNA profiles can be derived, and some police investigations have been made on these shed DNA. However, this article accepts the reasoning of the Court on this point. For that other view, see B. Quarmby, \textit{The case for national DNA identification cards}, 1 DUKE L. & TECH. REV. 1 (2003).

\textsuperscript{36} The evaluation of the existence of an interference of a fundamental right under EU law—and \textit{mutatis mutandis} under the ECHR regime—is composed of various layers, at the center of which is its essence or core, which cannot be interfered with under any circumstance, according to M. Brkan, \textit{The concept of essence of fundamental rights in the EU legal order: Peeling the onion to its core}, 14 EUR. CONST. LAW REV. 332, 332–3 (2018). See also M. Brkan, \textit{The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning}, 20 GER. LAW J. 864, 870 (2019). The effect of the collection and retention of DNA profiles on the right to respect for private life can be subjected to proportional balancing according to prevailing court practice, hence, it does not pertain to the very essence of the said right; see \textit{European data protection law handbook}, \textit{supra} note 18, at 24.

\textsuperscript{37} Kaye & Smith, \textit{supra} note 4, at 415.

\textsuperscript{38} \textit{id.} at 419. The Court noted the submission of the respondent member state that ‘retaining biometric data . . . is of value in fighting crime, in particular statistics for Northern Ireland show that a significant percentage of convicted adults are re-convicted of a further offence within one or two years’, \textit{Gaughran}, ECtHR at para. 62.

\textsuperscript{39} \textit{Marper}, ECtHR at para. 100.

\textsuperscript{40} ‘The Court cannot call into question the preventive purpose of a register . . . The aim of that register, as it has already pointed out, is to prevent crime and in particular to combat recidivism and, in such cases, to make it easier to identify offenders.’ See \textit{Gardel v. France}, no. 16428/05 ECtHR paras. 1–73, para. 63 (Dec. 17, 2009).

\textsuperscript{41} \textit{Chipovski}, ECtHR at para. 51.

\textsuperscript{42} A study on the occasion of the Court’s decision in \textit{Marper} showed that levels of subsequent criminality were similar to those convicted and those whose proceedings against them were terminated without conviction. See A. Tseloni & K. Pease, \textit{DNA retention after arrest: Balancing privacy interests and public protection}, 8 EUR. J. CRIMINOL. 32 (2010). Universal databases address the issue of discrimination felt by arrestees and convicts for being singled out with a recurring thought at the back of their minds that they
There are many predictors of crime engagement other than prior arrest and conviction.43 A universal database does not preclude the detection of first-time offenders44 who are obviously excluded from the current system.45 If everyone’s DNA profile is in the database, does it then make everyone a suspect?46 Objectively, DNA profiles will only match the equivalent number of perpetrators in the crime scene. Non-involvement in a crime will not activate one’s file in the database.47 As the Court noted, inclusion in the database produces the benefit of ‘rapid elimination’ as a suspect in a crime under investigation.48

II.D. A Side Note on the Practicality and Cost of Collection of Samples

DNA profile collection of an entire population may appear overwhelming at first sight49 but similar nationwide systems are already in place like mandatory newborn

---

43 Among these are dysfunctional families and neighborhoods, level of education, employment, age, gender, among others; see Kaye & Smith, supra note 4, at paras 420–1. Neither prior arrest nor prior conviction alone offer satisfactory bases for inclusion in databases; see id. at 421.

44 In the US, a black American is five times more likely to be put to jail than a white American thereby making the population in these databases racially distorted; see id. at 453. A more recent study shows that DNA databases in the US are racially disproportionate; see E. Murphy & J. Tong, Racial composition of forensic DNA databases, NYU SCHOOL OF LAW, PUBLIC LAW RESEARCH PAPER NO. 19–54 1, 27 (2019). Solving this racial imbalance will create an environment of mutual respect knowing that crime scene samples will be screened over the entire population, regardless of color. In the United Kingdom, a concern was also had on the disproportionate number of black males in its DNA database; see B. Blakemore & C. Blake, Can the national DNA database be effective and comply with human rights legislation?, 85 THE POLICE JOURNAL 191, 196–197 (2012). It has been argued that the current practice of collecting samples only from arrestees and convicts creates databases that are ‘skewed against the disadvantaged because they are the ones most likely to be the focus of such convictions and arrests’; see Hazel, et al., supra note 7, at 899. The author of the following article noted that one reason in support of universal databases is ‘equity’: A.O. Amankwaa, Forensic DNA retention: Public perspective studies in the United Kingdom and around the world, 58 SCIENCE & JUSTICE 455, 459 (2018).

45 R. S. Peterson, DNA databases: when fear goes too far, 37 AM CRIM LAW REV 1219, 1228 (2000). The author noted that a universal database ‘could be used to identify otherwise missed first-time offenders and to render unnecessary discriminatory dragnets’. Note that she ultimately argued against universal databases as an infringement of the Fourth Amendment of the U.S. Constitution, id. at 1238.

46 On the argument that universal databases are indicative of an ‘Orwellian society’, Kaye and Smith replied: ‘As rhetoric, this is powerful stuff, but its substance is fluffier. Privacy is an important value, but the privacy threat from digital records of DNA types that reveal nothing about a person’s nature or status is not self-evident . . . Indeed, a population-wide database should quickly limit the number of suspects—typically to a single person—in many crimes. By promptly eliminating everyone else as a viable suspect, it would reduce the burden on many individuals who would have been primary suspects.’ See Kaye & Smith, supra note 4, at 446.

47 In effect, it provides a sense of security for the innocent who will automatically be eliminated from suspicion and be spared of tedious police investigations. Overall, a higher sense of equality and trust in society is established when—like in many other government data systems like passports, tax returns and driver’s licenses—everyone is covered. There will be no discrimination based on one’s color, race or creed. Smith argued that ‘where the requirement to be included in the database applies equally to all citizens, no individual would be disadvantaged in relation to any other’, Smith, supra note 9, at 133.

48 W, ECtHR. See also Van der Velden, ECtHR.

49 One author even thinks it is ‘absurd’. See T. Simoncelli, Dangerous excursions: The case against expanding forensic DNA databases to innocent persons, 34 J LAW MED ETHICS 390, 394 (2006).
screening tests\textsuperscript{50} and passport and driver’s license applications where fingerprints and other personal data are collected and stored.\textsuperscript{51} Sample collection is even less invasive and intrusive compared to COVID-19 testing, which requires samples from both nose and throat,\textsuperscript{52} whereas a cheek swab is enough for DNA profiling. These data gathering mechanisms are possible venues for universal database sample collection.\textsuperscript{53}

Compared to COVID-19 testing, which employs similar molecular diagnostic procedures, DNA profiling is less costly since only one sample is required.\textsuperscript{54} Country-wide collection of samples for specific tests is not new.\textsuperscript{55} Using economies of scale, the overall cost is expected to decline over time with mass sample collection. This would depend on the state’s economic standing and its willingness to cover the cost or to charge it to its citizens.\textsuperscript{56}

\begin{itemize}
\item \textsuperscript{50} Peterson, supra note 45, at 1228. The following authors suggest that mandatory collection of DNA at birth instead of during one’s first point of contact with the law ‘maximizes efficiency’; see K.M. Donovan & C.F. Klahm IV, COUNTERBLAST. Prosecuting science: The rational defence of mandatory DNA databases, 48 Howard J. Crim 411, 411 (2009). In Europe, governments collect and store data related to healthcare, social security, and employment details of public servants; see M. McDonagh, Balancing disclosure of information and the right to respect for private life in Europe, 16 J. Internet L. 3, 3 (2012). Government data gathering venues are already regulated by certain privacy principles; see Smith, supra note 9, at 135.
\item \textsuperscript{51} One author even suggested the inclusion of one’s DNA information in their national identification card; see Quarmby, supra note 35, at 1. Another author suggested that samples can be obtained during the routine vaccination of children or when couples apply for marriage licenses; see Peterson, supra note 45, at 1228.
\item \textsuperscript{52} Government of the Netherlands, Testing for COVID-19 from the Ministry of Health, Welfare and Sport, National Institute for Public Health and the Environment, www.rivm.nl/en/novel-coronavirus-covid-19/testing-for-covid-19 (accessed June 16, 2020).
\item \textsuperscript{53} The time for collection may vary from state to state, but at the minimum, it should not be later than the age of criminal liability under national law.
\item \textsuperscript{54} Id. A person’s DNA is known to be stable, and the same test can be applied to the entire population without the attached burden of mutation—hence, variation of the test—in a virus like COVID, thereby making DNA profiling less costly. In fact, the EU guidelines on COVID-19 testing considers the capability of the virus to mutate, amounting to additional diagnostic costs, which does not apply to DNA profiling; see Guidelines on COVID-19 in vitro diagnostic tests and their performance, OJ C 122 1/1 4 (European Commission, 2020).
\item \textsuperscript{55} The current trend is for states to make COVID-19 testing available for their whole population; see W.A. Haseltine, Tests for COVID-19 are expensive, but they don’t have to be, FORBES, www.forbes.com/sites/williamhaseltine/2020/04/08/pricing-and-profiteering-from-covid-19-tests/ (accessed Apr. 28, 2021). A similar country-wide testing for Hepatitis C has been done in Egypt where free testing was offered to the entire population. To date, some 68 million Egyptians have been screened for the virus. Mutatis mutandis a much simpler DNA profiling test is more doable for an entire population than the more complex viral tests for COVID-19 and Hepatitis. See W.A. Haseltine, Universal disease screening and treatment—the Egyptian example, 382 New England Journal of Medicine 1081 (2020).
\item \textsuperscript{56} Some states may view it as an investment. Its ‘contribution to crime control and public safety would justify the financial investment and offer a proportionate benefit to any loss of privacy’. See Nuffield Council on Bioethics, The forensic use of bioinformation: Ethical issues, para. 4.74, www.nuffieldbioethics.org/assets/pdfs/The-forensic-use-of-bioinformation-ethical-issues.pdf (accessed Apr. 28, 2021). Note, however, that in para. 4.76, it was argued that ‘the increased risk to civil liberties would be compensated by only a negligible increase in public safety’. Details of this matter are beyond the coverage of this article but suffice it to say that testing during current pandemic only shows the feasibility of the measure. A case in point: the Netherlands uses the CODIS system developed by the US, whose current database population is almost equal to the entire population of the Netherlands. The combined state and federal DNA databases in the US amounts to 16.5 M samples; see Hazel, et al., supra note 7, at 898.
\end{itemize}
II.E. Preliminary Safeguard: Limiting Sample Collection to DNA Profiles

DNA profiles in their simplest form are numerical figures that represent the variations of alleles found in each locus making them analogous to bar codes.\(^{57}\) They only provide limited information necessary to identify an individual compared to cellular samples, which can be fresh sources of DNA for the generation of a lot more information, which may have deeper privacy repercussions, such as ethnic and familial tracing and predisposition to genetic diseases. Although the Court acknowledged the wealth of health and genetic information that can be generated from cellular samples—without acknowledging the same on DNA profiles—it afforded the same protection to both.\(^{58}\) However, limiting sample collection to DNA profiles provides a sufficient safeguard for the protection of privacy given their narrower use for identification purposes. An appropriate legal safeguard would be to require the destruction of cellular samples and DNA extracts right after the production of DNA profiles. This safeguard will limit the seriousness of the interference to a set of numerical figures representing a person’s DNA profile.\(^{59}\)

III. LEGALITY TEST AND POLICE INVESTIGATION TECHNIQUES

Related laws promulgated by the Council of Europe are evaluated in this test given the scope and nature of this article where a universal database legislation has not yet been created. The legality test has two main requirements:\(^{60}\) 1. the interference or measure should have some basis in the domestic law of a member state; and 2. the law must be ‘clear, foreseeable, and adequately accessible’ (quality of the law). This test is so crucial such that its violation would immediately allow the Court to declare a violation of Article 8 ECHR without having to perform the legitimate purpose and proportionality tests.\(^{61}\)

---

57 A person’s DNA is extracted from any cellular sample (skin, hair, cheek cells, etc.); from this DNA extract, a DNA profile is generated depending on the STR method used. The resulting data are in the form of numerical figures representing the profile and so they cannot be used to generate another DNA profile, unlike cellular samples and DNA extracts. As to the DNA-STR profiles, each person has two alleles for each locus, one inherited from the mother and the other from the father. If the same allele is inherited from both parents, the locus is homozygous; if they are different, it is heterozygous. See B. Alberts, et al., Molecular Biology of the Cell 547 (2008).

58 See Marper, ECHR at para. 120. Both cellular samples and DNA profiles were collected and retained in van der Velden and Marper, whereas in Gaughran, the focus was on DNA profiles because the applicant’s cellular sample was previously destroyed.

59 This legal safeguard will also prevent further phenotypic DNA profiling that may be performed on the cellular material—one of the fears generated by expanding DNA databases. See P. Gorkic, Judicial oversight of the (mass) collection and processing of personal data, in Big DATA, CRIME AND SOCIAL CONTROL 193 (A. Završnik ed., 2018).

60 PG and JH, ECHR at para. 61. In Marper, the Court explained that ‘the wording “in accordance with the law” requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8,’ at para. 95.

61 After the Court found a violation of the legitimacy test in Petrović, it ruled that it was ‘unnecessary for the Court to examine whether it [the collection of DNA samples] was undertaken in pursuit of a “legitimate aim” and was “necessary in a democratic society”, within the meaning of Article 8 of the Convention.’ See Petrović, ECHR at para. 84.
III.A. Basis in Domestic Law

1. Convention 108+ of 2018

Article 6 of Convention 108+ enumerated a number of ‘special categories of data’ where DNA profiles may be classified: either as ‘genetic data’ or ‘biometric data uniquely identifying a person.’ The processing of both data is not prohibited as long as ‘appropriate safeguards’ are provided in the enabling law. The Court in Marper referred to the Data Protection Convention of 1981 (Convention 108). Although the newer Convention 108+ was already effective during the promulgation of the Gaughran decision, the Court continued to refer to the older Convention. The ECtHR judges may need some updating on the prevailing law at the time of their decision and not merely make a blind reference to related but outdated paragraphs in its previous rulings. They would have enriched jurisprudence by making a classification of DNA profiles according to the terminologies of the updated law. In any case, there is nothing in the updated legislation that directly prohibits the creation of universal databases.

2. Recommendation No. R (87) 15

The specific provisions under Recommendation No. R (87) 15 on the use of personal data in the police sector that were made applicable in both Marper and Gaughran were Principles 2, 3 and 7 specifying the following safeguards: (1) collection is limited to what is necessary for ‘the prevention of a real danger or the suppression of a specific criminal offence’ (Principle 2); (2) storage is ‘limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks’ (Principle 3); and (3) personal data that are ‘kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored’ (Principle 7). Recommendation No. R (87) 15 does not prohibit universal databases as long as their use is limited to the purposes of their creation and the enumerated safeguards are in place.

62 Convention 108+: Convention for the protection of individuals with regard to the processing of personal data, 128th session of the Committee of Ministers (Council of Europe, 2018).
63 id. at Article 6(1).
64 This is understandable given that the Marper decision was promulgated during the effectivity of Convention 108 and before the effectivity of Convention 108+.
65 Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, ETS No. 108 (Council of Europe, 1981).
66 Gaughran was decided two years after the promulgation of Convention 108+.
67 It merely gave reference to paragraph 41 of Marper, which refers to the older convention. See Gaughran, ECtHR at para. 50. It made reference to Marper, ECtHR at paras 41–53.
68 Article 6 in the old law (Convention 108) does not distinguish genetic from biometric data. The Court missed the opportunity in Gaughran to provide guidance on this legal topic given the new classification of data in the updated version of the law (Convention 108+).
69 Recommendation No. R (87) 15: On regulating the use of personal data in the police sector, 410th meeting of the Ministers’ Deputies (Council of Europe, 1987).
70 Marper, ECtHR at para. 42.
71 Gaughran, ECtHR at paras 50–1.
3. Recommendation No. R (92) 1

The more specific legal instrument concerning DNA analysis in the criminal justice system is Recommendation No. R (92) 1. Marper highlighted provisions 3, 4 and 8 of the Recommendation, while Gaughran only underscored provision 8. In both cases, the said provisions do not prohibit the creation of universal databases as long as the following safeguards are in place: (1) their use is limited to the ‘investigation and prosecution of criminal offence’ or if they are used for research and statistical purposes, the identity of their sources cannot be ascertained (provision 3); (2) taking of samples is limited to what the domestic law provides (provision 4); and (3) data are deleted after their purpose has been achieved (provision 8). Overall, none of the existing legal instruments of the Council of Europe directly prohibit the creation and maintenance of universal databases.

III.B. Quality of the Law

In measuring the quality of the law, its accessibility, clarity, foreseeability with respect to persons concerned are evaluated.

Accessibility of the law. There has been no case questioning the accessibility of the law before the ECtHR. Each member state has developed a system by which new laws are made accessible to all its citizens. This usually comes in the form of publication of the law in a manner specified by national practice. The same system of dissemination can be applied to universal databases.

Clarity of the law. Clarity refers to the ‘scope of discretion exercised by public authorities’ when it comes to the implementation of the law. There should be ‘reasonable clarity’ as to the ‘scope and manner’ of this discretion to provide people with ‘minimum degree of protection’. This can be measured through legal safeguards in the enabling universal database law to prevent arbitrariness on the part of law enforcers, thereby making the implementation of the law predictable to everyone concerned.

Sufficient foreseeability. In Petrović, the Court declared that the collection of DNA samples was not ‘in accordance with the law’ because the ‘domestic legal provisions in question should, inter alia, have been “foreseeable as to [their] effects” for the applicant’. The respondent state relied upon the law’s ‘other medical procedures’ clause to justify DNA sample collection but the Court ruled that a ‘specific reference . . . to the taking of a DNA sample’ is necessary. This element of foreseeability is intimately linked with the previous element of ‘clarity of the law’. Legal protection should be

---

72 Recommendation No. R (92) 1: On the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system, 470th meeting of the Ministers’ Deputies (Council of Europe, 1992).
73 Marper, ECtHR at para. 43.
74 Gaughran, ECtHR at para. 50.
75 European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, paras 14–20, https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (accessed April 28, 2021).
76 Id.
77 Id.
78 ECHR Article 8 Guide, supra note 75, at paras 16–17.
79 Petrović, ECtHR at para. 80.
80 Id. at para. 81.
present in the law against arbitrary interferences by public authorities.\footnote{Krušlin v. France, no. 11801/85 ECHR paras. 1–40, para. 30 (Apr. 24, 1990).} It must be sufficiently foreseeable such that the people concerned know the circumstances and conditions where authorities are entitled to take action on matters that affect their rights.\footnote{ECHRArticle 8 Guide, supra note 75, at para. 17.} It must allow people to determine to a reasonable degree if they are covered by the law\footnote{Id.} and its provisions should be ‘foreseeable as to their effects’\footnote{Petrović, ECtHR at para. 80.} to the applicant. In universal databases with sufficient legal safeguards, it is clear that the entire population is covered.

### III.C. Legality, Identification and Police Investigative Practices

#### 1. Identification Conundrum

The Court understood correctly that DNA profiles are generated from DNA that is extracted from cellular samples.\footnote{Three different types of forensic samples were involved in \textit{Marper}, namely, cellular samples, DNA profiles and fingerprints. The same samples were involved in \textit{Gaughran} although the cellular samples were destroyed after the DNA profiles were generated; see \textit{Gaughran}, ECtHR at para. 9. This article focuses on DNA profiles because they are the ones that are retained in DNA databases.} While it acknowledged that the personal information they contain is ‘more limited’ and its information is in ‘coded form’, it claims that the automated processing of these data permit authorities to ‘go well beyond neutral identification.’\footnote{\textit{Marper}, ECtHR at paras 74–75.}

The Court appears to be confusing the three meanings of identification as previously clarified by Kaye:\footnote{D.H. Kaye, \textit{Response. Maryland v. King: per se unreasonableness, the golden rule, and the future of DNA databases}, 127 Harv. Law Rev. 39, 44–5 (2013). See also E. Murphy, \textit{License, registration, cheek swab: DNA testing and the divided court}, 127 Harv. Law Rev. 161, 179–80 (2013).} 1. \textit{authentication}-identification, where a person’s identity is determined through a mark or token, like a DNA profile; 2. \textit{association}-identification, where a known individual’s DNA profile is associated with their profile in a database; and 3. \textit{trait}-identification, where an individual’s health, character, ethnicity, etc. are described.\footnote{For example, it is the ‘trait-identification’ feature that allows the use of a DNA profile to determine if a person has a propensity to acquire a genetic disease or even a criminal tendency.} It is the third meaning of identification that has ‘much more serious implications for personal privacy’,\footnote{Kaye, supra note 87, at 45.} and its confusion with the first two meanings is a cause of great fear as to the alleged privacy overreach of these databases.\footnote{‘To some extent, \textbf{the decision in Marper is based on fear} that those in the database will be associated with criminality . . . the criminal stigma of being in a database is eliminated if everyone’s DNA is acquired,’ (emphasis supplied) see Hazel, et al., \textit{supra} note 7, at 899.} The objections enumerated by the Court—such as the use of DNA profiles in familial searching\footnote{For this procedure, see H. T. Greely, et al., \textit{Family ties: the use of DNA offender databases to catch offenders’ kin}, 34 J Law Med Ethics 248 (2006).} or in identifying a person’s ethnic origins—belong to the meaning of \textit{trait}-identification.

Since DNA profiles are susceptible to automatic processing, and such data are used for criminal investigations by the police,\footnote{\textit{Marper}, ECtHR at para. 103.} one legal safeguard is to limit their use to
authentication- and association-identification. This safeguard removes the possibility of function creep, prevents comparison with other datasets, and it appears to provide even greater protection to informational privacy compared to current practices in criminal investigations.

2. Streamlining Investigations

When crime scene samples do not show a match in existing forensic databases, police officers tend to request for judicial warrants to compare their samples to other databases like those used for medical and health research. A subpoena of medical records may also be requested—a practice that raises more privacy concerns given the presence of other personal data in those medical files. In the US, a cold case was resolved by the police using a private direct-to-consumer (DTC) genetic database. It has sparked privacy concerns over the use of non-governmental facilities for criminal investigations. Universal databases entirely make these practices obsolete since everyone's DNA profile is already in the system.

93 The authors of the following article argue that there is no federal limit on the use of information from DNA databases: M.A. Rothstein & M.K. Talbott, The Expanding Use of DNA in Law Enforcement: What Role for Privacy?, 34 J LAW MED ETHICS 153, 159 (2006). It is precisely the argument of this present article that the legislation of universal DNA databases will be a venue for the institution of those limits by law and not by mere regulation subject to the prerogative of the police.

94 ‘Function creep refers to changes in, and especially additions to, the use of a technology’, J.Y. Dahl & A.R. Sætnan, ‘It all happened so slowly’—On controlling function creep in forensic DNA databases, 37 INT J LAW CRIME JUSTICE 83, 83 (2009). See also P. Monteleoni, DNA databases, universality, and the Fourth Amendment, 82 N.Y.U. L. REV. 247, 259 (2007).

95 Other datasets include Single Nucleotide Polymorphisms (SNPs). In a study using linkage disequilibrium, record matching among separate sets of databases was shown to be possible even when the data do not have shared markers. Scientists matched two types of genotype datasets: SNPs and forensic STR markers. They showed that 90–98% of the STR profiles can be connected to corresponding SNP records and vice versa. The accuracy of the match goes up to 99–100% when the STR loci was increased to around 30. This means that analysts who have access to both datasets could use those profiles for trait identification including data related to ancestry and health, and could make possible predictions of genetically influenced phenotypes. For details, see M.D. Edge, et al., Linkage disequilibrium matches forensic genetic records to disjoint genomic marker sets, 114 PNAS 5671 (2017).

96 The following author argued that any possible violation of restrictions in this day and age would lead to the further tightening of security: ‘After all, we do not shut down other basically beneficial systems, from airline traffic to courts, because some mistakes occur. Making policy based on horror stories is a horrible idea’; see A. Etzioni, DNA tests and databases in criminal justice: Individual rights and the common good, in DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 211 (D. Lazer ed., 2004).

97 It has been argued that currently, law enforcement officials use electronic medical records as their ‘de facto’ universal database, which exposes more sensitive personal information than a DNA profile would; see Dedrickson, supra note 6, at 646.

98 This practice may expose other personal data found in those databases and even create a certain level of stigmatization—unwarranted for a health research database—should a match be found. See separate discussion on the risk of stigmatization, infra.

99 Hazel, et al., supra note 7, at 900.

100 In the Golden State killer case, the government justified the use of a private DNA database for familial searching due to its accessibility to the public. These private databases are maintained by direct-to-consumer (DTC) companies like GEDMatch, 23andMe and Ancestry.com. Universal DNA databases ‘virtually erase the government’s incentive to conduct long-range familial DNA searches of the type used in the Golden State Killer case’; see id. at 898–9.
3. Shed DNA and DNA Dragnets

Universal databases would also deter the police practice of gathering 'shed DNA'\textsuperscript{101} — DNA extracted from cellular material that a 'suspect' leaves behind\textsuperscript{102} — which raises some privacy concerns.\textsuperscript{103} This practice does not provide safeguards for suspects as it is mainly based on the prerogative of the investigator. Universal databases would also halt expensive, inefficient, and often racially biased\textsuperscript{104} DNA dragnets — where members of a given population with defined characteristics in the area of a crime or its environs are sampled — as everyone is already in the database. Besides, police officers tend to obtain warrants to sample those who refuse to participate in these dragnet procedures\textsuperscript{105} — a superfluity in the presence of universal databases. Hence, these current investigative practices that raise privacy concerns will be avoided.\textsuperscript{106}

IV. LEGITIMATE PURPOSE TEST AND FORENSIC REPORTING

The question on whether the impugned measure at issue serves a legitimate purpose has been the easiest to answer in the affirmative as can be deduced from the cases involving DNA profiles that have reached the Court. This test is rather straightforward: the impugned measure should fall within any of the aims enumerated in Article 8 § 2 of the Convention. These include the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others.\textsuperscript{107} The standard Court practice is to be 'quite succinct when it verifies the existence of a legitimate aim'\textsuperscript{108} within the meaning of Article 8 § 2 of the Convention. The burden falls upon the government to demonstrate that the interference is in pursuit of such legitimate aim.\textsuperscript{109}

IV.A. Legitimate Purpose under Article 8 § 2 ECHR

All the cases involving DNA profiles have been classified under the legitimate aims of prevention of crime and protection of the rights and freedoms of others.\textsuperscript{110} The Court noted that these legitimate aims stand even if the DNA ends up not playing a role in the criminal investigation.\textsuperscript{111} The Court in \textit{Marper} also acknowledged the importance of

\textsuperscript{101} Quarmby, supra note 35.

\textsuperscript{102} For example, the police may collect epithelial cells from drinking glasses or cigarette butts that are left behind in a restaurant or public space.

\textsuperscript{103} Dedrickson calls these 'abandoned DNA'; see Dedrickson, supra note 6, at 645. For various police techniques in gathering these samples, which raises questions of privacy, see id. at 645–6.

\textsuperscript{104} See Peterson, supra note 45, at 1227.

\textsuperscript{105} Id.

\textsuperscript{106} It has been argued that universal DNA databases 'may even increase privacy by decreasing more invasive investigative techniques, exonerating the innocent, and deterring crime'; see Dedrickson, supra note 6, at 638 & 645–7.

\textsuperscript{107} Article 8 § 2 ECHR.

\textsuperscript{108} See also S.A.S. v. France, no. 43835/11 ECtHR paras. 1–163, para. 114 (July 1, 2014).

\textsuperscript{109} ECtHR Article 8 Guide, supra note 75, at para. 21.

\textsuperscript{110} Dedrickson also argued for the legitimate purpose of public safety which may be read into one of these purposes: 'A universal DNA database’s benefits in efficiently and effectively solving crimes, exonerating the innocent, and decreasing racial disparities in law enforcement, however, make such a database immensely appealing from a public safety and criminal justice perspective'; see Dedrickson, supra note 6, at 637.

\textsuperscript{111} Van der Velden, ECtHR.
retaining DNA information for the identification of future offenders.\textsuperscript{112} This reasoning was adapted recently in \textit{Gaughran} in this wise:\textsuperscript{113}

‘While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of persons who may offend in the future.’\textsuperscript{114}

That statement is easily transposable to universal databases whose main objective is to assist in the identification of future offenders. A legal safeguard is to use them strictly for such purpose. As Lord Justice Sedley put it, they are ‘for the absolutely rigorously restricted purpose of crime detection and prevention.’\textsuperscript{115} The subsequent subsections illustrate this point.

\section*{IV.B. Legitimate Purpose and Forensic Reporting}

\subsection*{1. Accuracy of Forensic Reporting using DNA Profiles}

The current system of reporting DNA profile matches is in the form of random match probabilities and likelihood ratios. These are computed based on the statistical frequency of a given STR allele within the populations represented in the database.\textsuperscript{116} While the statistical method employed is based on sound science,\textsuperscript{117} it is primarily based on probabilities generated from a select portion of a given population. On the other hand, universal databases create a one-to-one correspondence with the sample being matched. Scientific reporting will no longer be based on match probability,\textsuperscript{118} but on person-specific matches. A match to more than one person is extremely rare\textsuperscript{119} but its eventuality would help further elucidate the accuracy of DNA profiling.\textsuperscript{120} In

\begin{footnotesize}
\begin{enumerate}
\item Marper, ECtHR at para. 100.
\item Gaughran, ECtHR at para. 75.
\item The ruling in \textit{Chipovski} is essentially the same: ‘While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the future identification of offenders.’ See \textit{Chipovski}, ECtHR at para. 49.
\item Note that this statement was made prior to Marper. Lord Justice Sedley was one of the proponents of a universal DNA database in the United Kingdom. See C. Dyer, \textit{Anger over call to widen DNA database}, \textit{THE GUARDIAN}, www.theguardian.com/uk/2007/sep/06/ukcrime.prison and probation (accessed Apr. 28, 2021).
\item Discrepancies have been observed on individual alleles at several loci between reference and casework databases. See R. Hedell, et al., \textit{Discrepancies between forensic DNA databases}, 3 \textit{FORENSIC SCI INT GENET. e135} (2011).
\item S.J. Walsh, et al., \textit{Modeling forensic DNA database performance}, 55 \textit{J. FORENSIC SCI} 1174 (2010).
\item The prevailing scientific method of forensic reporting makes use of the Bayesian approach. See M. Giacalone, et al., \textit{DNA test to assess criminal responsibility: a Bayesian approach}, 52 \textit{QUAL QUANT} 2837 (2018). See also D.H. Kaye, \textit{Identification, individualization and uniqueness: What’s the difference?}, 8 \textit{LAW PROBAB RISK} 85 (2009).
\item Smith, supra note 9, at 135.
\item At this point, this is just based on conjecture given that no universal database has ever existed yet. See S.J. Walsh, et al., \textit{Comparing the growth and effectiveness of forensic DNA databases}, 1 \textit{FORENSIC SCI. INT. GENET. SUPPL. SER.} 667 (2008). A subsequent study has shown that expanding the coverage of a DNA database does not necessarily yield a significantly higher output performance; see F. Santos, et al., \textit{Forensic DNA databases in European countries: Is size linked to performance?}, 9 \textit{LIFE SCI. SOC. POLICY} 1 (2013). However, the article only covered DNA databases that included a subset of the entire population. The seeming disparity between size and performance is no longer a question in universal databases as explained in this sub-section.
\end{enumerate}
\end{footnotesize}
any case, a double match would lead investigators to a more informed evaluation of the other pieces of evidence available to them.\textsuperscript{121} Should there be no direct match, investigation may lead to persons outside the database population, such as foreigners. It effectively directs investigators and prosecutors to use their limited time, energy, and resources to investigative leads, which they would not have immediately discovered otherwise.

2. Scientific Appreciation of Forensic Reports

Forensic reporting makes use of probability statements and statistical figures, which may confound the trier of fact. It has been shown that jurors do not have a proper understanding of likelihood ratios when presented with forensic reports\textsuperscript{122} and that even forensic experts themselves make mistakes in their conclusions about DNA profile matches.\textsuperscript{123} Forensic reports vary from one forensic laboratory to another and their impact may affect an acquittal or conviction.\textsuperscript{124} An ‘allegiance effect’ has been shown where experts tend to assign more favorable reports to the side that retained them, either the prosecution or the defense.\textsuperscript{125} These problems will be inexistennt in a universal database system since its comprehensive coverage will generate person-specific matches, and not matches based on statistical probability.\textsuperscript{126}

3. Database Size and Data Anonymization

The ‘sole reason’\textsuperscript{127} why the United Kingdom wanted to keep the DNA profiles in \textit{Marper} was to increase the size and use of their database, that is, the bigger the population, the higher the chances of producing a match.\textsuperscript{128} That argument no longer applies in a universal database because there is no need to increase the sample population to produce a more statistically sound result.\textsuperscript{129} Moreover, there is no need to keep the profiles after death.\textsuperscript{130} There is also no need to anonymize\textsuperscript{131} DNA profiles so that they could be kept in the databases after acquittal or death\textsuperscript{132} in order to increase the

\begin{itemize}
\item Adventitious matches are chance matches between DNA profiles. They tend to increase as the number of profiles in the databases increase; see J. Ge, et al., \textit{Future directions of forensic DNA databases}, 55 CROAT MED J 163, 163 (2014). This problem is addressed by universal databases as explained in this paragraph.\textsuperscript{121}
\item J.W. De Keijser & H. Elffers, \textit{Understanding of forensic expert reports by judges, defense lawyers and forensic professionals}, 18 PSYCHOL CRIME LAW 191 (2012). For a study made on mock jurors, see N. Scurich & R.S. John, \textit{Trawling genetic databases: When a DNA match is just a naked statistic}, 8 J. EMPIR. 49 (2011).\textsuperscript{122}
\item De Keijser & Elffers, \textit{supra} note 122, at 205–6.\textsuperscript{123}
\item J. W. De Keijser, et al., \textit{Differential reporting of mixed DNA profiles and its impact on jurors’ evaluation of evidence. An international analysis}, 23 FORENSIC SCI INT GENET 71 (2016).\textsuperscript{124}
\item D.C. Murrie, et al., \textit{Are forensic experts biased by the side that retained them?}, 24 PSYCHOL. SCI 1889 (2013).\textsuperscript{125}
\item For more studies on the level of understanding of these forensic reports, see Smith, \textit{supra} note 9, at 134.\textsuperscript{126}
\item \textit{Marper}, ECHR at para. 123.\textsuperscript{127}
\item The value of a database is believed to be directly related to the number of profiles stored. See P. M. Schneider & P. D. Martin, \textit{Criminal DNA databases: The European situation}, 119 FORENSIC SCI INT 232, 233 (2001).\textsuperscript{128}
\item The authors of the following article discuss the sampling of populations using the current database system: C. D. Steele & D. J. Balding, \textit{Choice of population database for forensic DNA profile analysis}, 54 SCI JUSTICE 487 (2014).\textsuperscript{129}
\item \textit{Marper}, ECHR at para. 48. \textit{See also Gaughran}, ECHR at para. 53.\textsuperscript{130}
\item Data anonymization or pseudonymization may be relevant when samples are collected by a state prior to the age of criminal liability as mandated by its domestic law. See relevant discussion on the retention of data of minors, infra.\textsuperscript{131}
\item Currently, Dutch law specifies the longest retention period of twenty years from the date of death for serious offences, with decreasing periods for less serious offences. \textit{See Gaughran}, ECHR at para. 53.\textsuperscript{132}
\end{itemize}
statistical valuation of the DNA match reports. A comprehensive database will make that exercise superfluous.

4. Avoidance of False Confessions
It has been shown that some people tend to confess to a crime they did not commit, especially when police officers claim that their DNA profile matched with that of a crime scene sample. The current system produces such matches based on the available profiles in the system, which are mainly from previously convicted individuals. The tendency of police officers to induce convicts to confess to a crime they did not commit—due to a supposed DNA profile match—will be reduced if not completely eliminated because matches in universal databases are actual matches, not probable matches. Universal databases will make everyone aware of how DNA profile matching works and can demand actual match reports from police investigators. The heightened awareness of how universal databases work increases the level of scientific culture of the population and lends more objectivity to criminal investigations—at least as far as DNA evidence is concerned—making them less prone to abuse.

V. PROPORTIONALITY TEST AND LEGAL SAFEGUARDS
The final and most important test is the Court’s way of measuring whether the impugned law is necessary in a democratic society. For an interference to be considered ‘necessary in a democratic society’, it has to answer a ‘pressing social need’, and in particular, it has to be ‘proportionate’ to the legitimate aim that is being pursued and the reasons for its justification are ‘relevant and sufficient’.

V.A. Whether it Answers a Pressing Social Need
The initial assessment as to the existence of a ‘pressing social need’ is a function of the member states given their margin of appreciation subject to the final review of the Court. Following previous case law, Gaughran affirmed that the ‘breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference’. Further, this margin tends to be ‘narrower where the right at stake is crucial to the individual’s effective enjoyment of intimate or key rights’ and where ‘a particularly important facet of an individual’s existence or identity is at stake, the margin allowed to the State will be restricted’.

---

133 It has been shown that bluffing techniques (pretending to have evidence) employed by interrogators may cause innocent people to confess to a crime they did not commit. See S.M. Kassin, False confessions: Causes, consequences, and implications for reform, 1 POLICY INSIGHTS BEHAV BRAIN SCI 112, 116 (2014). In one case, a man confessed to a murder he did not commit after the lead investigator pretended to call from the crime laboratory to report that his DNA profile matched with that found in the crime scene. See S.A. Drizin & R. Leo, The problem of false confessions in the post-DNA world, 82 N.C. L. REV. 891, 969–70 (2008).

134 Marper, ECtHR at para. 101. The application of this test in the case law of ECtHR has been inconsistent and non-transparent; see J. Gerards, How to improve the necessity test of the European Court of Human Rights, 11 INT J CONST LAW 466, 467–8 (2013).

135 ECHR Article 8 Guide, supra note 75, at para. 26.

136 Gaughran, ECtHR at para. 77.

137 Id.
The Court considers that ‘personal data is of fundamental importance to a person’s enjoyment of their right to respect for private and family life.’\(^{138}\) It follows that for universal databases, the margin of appreciation afforded to member states is restricted.\(^{139}\) There is one window where this margin could be wider: when ‘there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it.’\(^{140}\) At this point, it is difficult to predict the presence or absence of consensus for universal databases in Europe.\(^{141}\) But if one extrapolates it from recent ECtHR case law on mere retention of DNA profiles of convicted persons, the margin of appreciation would still be narrow.\(^{142}\)

V.B. Whether it Is Proportionate to the Legitimate Aim Pursued

In the two major ECtHR cases concerning DNA profile retention where both convicted and un-convicted applicants are involved,\(^{143}\) the Court found a violation of the applicants’ right to respect for private life mainly because the applicable laws did not provide sufficient safeguards for the protection of such right. On the other hand, in Martens, the Court found a ‘proportionate interference’ to the said right due to the presence of sufficient safeguards in the domestic law.\(^{144}\) In the enabling legislation for universal databases, the provision for sufficient safeguards is crucial to show the existence of a fair balance\(^{145}\) between competing public and private interests.\(^{146}\)

1. Presumption of Innocence and Risk of Stigmatization

DNA profile retention in databases is argued to be violative of a person’s right to presumption of innocence.\(^{147}\) Corollary to that right, the retention of DNA data of

\(^{138}\) Marper, ECtHR at para. 103.

\(^{139}\) Even at the level of consensus among member states in the Council of Europe, the Court has previously ruled that the margin of appreciation was deemed to be narrow in cases involving DNA profile retention; see id. at para. 112. See also Gaughran, ECtHR at para. 84.

\(^{140}\) Gaughran, ECtHR at para. 77.

\(^{141}\) This may be due to the perception that they are illegal; see Santurtún, et al., supra note 13, at 84.

\(^{142}\) ‘[T]he Court cannot conclude that the State’s margin of appreciation is widened in the present case to the extent claimed by the Government. The United Kingdom is one of the few Council of Europe jurisdictions to permit indefinite retention of DNA profiles... The degree of consensus existing amongst Contracting States has narrowed the margin of appreciation available to the respondent State in particular in respect of the retention of DNA profiles . . . ’; see Gaughran, ECtHR at para. 84.

\(^{143}\) Marper, ECtHR at para. 10. Gaughran, ECtHR at para. 7.

\(^{144}\) The applicants had been repeatedly convicted of serious offences and the retention of their DNA profiles were subject to the safeguard of periodic review; see Martens, ECtHR at paras 44–9.

\(^{145}\) It is acknowledged that experts disagree on how to strike this fair balance. See V. Mayer-Schönberger, Strands of Privacy: DNA Databases, Informational Privacy, and the OECD Guidelines, in DNA and the Criminal Justice System: The Technology of Justice 225–245 (D. Lazer ed., 2004).

\(^{146}\) Marper, ECtHR at para. 118. The creation of legal safeguards could be the most crucial factor in the acceptance of universal databases. In one study, although more people were willing to donate their samples for inclusion in DNA databases, the overall concern generated is the possible lack of control and insufficient safeguards in the system. See H. Machado & S. Silva, "Would you accept having your DNA profile inserted in the National Forensic DNA database? Why?" Results of a questionnaire applied in Portugal, 8 Forensic Sci Int Genet 132 (2014).

\(^{147}\) The reasoning employed in Marper on the question of presumption of innocence has sparked interest even outside Europe; see M. Lwin, Privacy issues with DNA databases and retention of individuals’ DNA information by law enforcement agencies: the holding of the European Court of Human Rights case S and Marper v. United Kingdom should be adapted to American Fourth Amendment jurisprudence, 19 Inf. Commun. Technol. Law 189 (2010).
Universal forensic DNA databases

un-convicted suspects was thought to expose them to the risk of stigmatization.\textsuperscript{148} In \textit{Gaughran}, the Court underlined that the risk of stigmatization is ‘not the same’ for convicted persons although the margin of appreciation for the retention of their DNA profiles remains to be narrow.\textsuperscript{149} The Court earlier ruled in \textit{Rushiti} that no suspicion regarding the innocence of the accused may be voiced after their acquittal.\textsuperscript{150} This includes the perception that they are not being treated as innocent due to the indefinite retention of their data.\textsuperscript{151} In \textit{Gaughran}, the prohibition against indefinite retention of DNA profile data was extended to convicts in the absence of specific retention criteria in the domestic law.\textsuperscript{152} Universal databases uphold everyone’s presumption of innocence because inclusion in the database would no longer amount to suspicion of commission of a crime. Consequently, any risk of stigmatization will be inapplicable when the law treats each one in the same way without any discrimination.\textsuperscript{153}

\textbf{2. Nature or Gravity of the Offence}

The nature of the offence at issue is one of the factors considered by the Court in determining the appropriateness of a retention measure. In \textit{Marper}, a violation was found because DNA profiles were ‘retained irrespective of the nature or gravity of the offence’.\textsuperscript{154} The same line of reasoning was used in \textit{Gaughran} where the applicant was convicted for a minor recordable offence.\textsuperscript{155} In \textit{Martens}, however, the state’s power of retention was upheld given that the applicants were repeated offenders of serious crimes.\textsuperscript{156} Applying these case laws to universal databases would mean their rejection by the Court due to their very essence: the collection and retention of DNA profiles from the entire population \textit{regardless} of the commission of any offence. They can be considered only if the Court uses a different set of lens in adjudicating a violation where prior commission of a crime is not a factor. The Court can evaluate the power of universal databases rather on their ability to provide equal protection to the entire population where everyone is treated equally.\textsuperscript{157} As long as the Court includes prior

\begin{itemize}
\item \textsuperscript{148} \textit{Marper}, ECtHR at para. 122. See also L. Campbell, ‘Non-conviction’ DNA databases and criminal justice: a comparative analysis, \textit{J Crim Law Criminol} 55, 72 & 77 (2011).
\item \textsuperscript{149} \textit{Gaughran}, ECtHR at para. 88.
\item \textsuperscript{150} ‘The Court, thus, considers that once an acquittal has become final—be it an acquittal giving the accused the benefit of the doubt in accordance with Article 6 § 2—the voicing of any suspicions of guilt, including those expressed in the reasons for the acquittal, is incompatible with the presumption of innocence.’ See \textit{Rushiti v. Austria}, no. 28389/95 ECtHR paras. 1–39, para. 31 (June 21, 2000).
\item \textsuperscript{151} \textit{Marper}, ECtHR at para. 122.
\item \textsuperscript{152} \textit{Gaughran}, ECtHR at para. 96.
\item \textsuperscript{153} A civil rights lawyer with more than 40 years of experience, Benedict Birnberg, claimed that universal databases ‘would remove the taint of discriminatory selection, of some people being stigmatized because their bioinformation and not others was held’, Nuffield Bioethics Council, \textit{supra} note 56, at para. 4.74. Note that in para. 4.77, it was argued that ‘[t]here is little reason to believe that the establishment of a population-wide database would in itself prevent discrimination in policing practice (eg in arrests and in taking samples) against certain vulnerable groups.’
\item \textsuperscript{154} \textit{Marper}, ECtHR at para. 119.
\item \textsuperscript{155} \textit{Gaughran}, ECtHR at para. 96.
\item \textsuperscript{156} \textit{Martens}, ECtHR at para. 44 in relation to 49.
\item \textsuperscript{157} This is admittedly a thorny issue. The focus of this subsection is its relation to the aspect of ‘nature or gravity of the offence’. It has to be read in conjunction with the discussion on equality and presumption of innocence.
\end{itemize}
existence of an offence to it balancing exercise, there is no way for universal databases to find fruition in Europe.

3. Retention Period
The practice of member states is varied when it comes to retention periods in their national databases. The Court found violations only when there was no retention limit even if such limit happens after death. The Court found a violation in Marper because DNA profiles may be ‘retained indefinitely whatever the nature or seriousness of the offence’ under suspicion.158 It is such ‘open-ended’ retention regime that invited the Court to make a careful scrutiny of the case.159 The Court argued that mere retention of DNA profiles has a ‘direct impact on the private-life interests’ of the person who owns the data irrespective of the subsequent use of such data.

The Court in Gaughran enumerated the recent retention periods among member states and demanded that they have to be coupled with sufficient safeguards.160 Luxembourg, Finland and Estonia retain profiles after death161 while Netherlands has the highest retention period of twenty years after death for those convicted of serious offences.162 Other states limit it to a few years after death or until the person reaches a certain age, like 80 for both Austria and Denmark, or 100 years after inclusion for Lithuania and 100 years after the person’s date of birth in Slovakia.163 In Chipovski, the Court ruled that ‘[i]n the absence of anything to suggest that such retention may be linked to any fixed point in time, the Court considers that the respondent State permits indefinite retention period of DNA profiles’.164 In Martens, however, the Court found no violation even when there was no retention limit but the applicant had an option to review such retention.165

Member states retain profiles even after death presumably to increase the statistical value of matching reports and to use them in familial searching166 both of which are inapplicable in universal databases167 where data will only be useful during a person’s lifetime. The enabling universal database law shall then provide an option for family members to review whether the DNA profile data of their deceased relatives have been purged out of the system—a safeguard that is absent in current systems that retain data even after death.

158 Marper, ECtHR at paras 119–21.
159 Id.
160 Gaughran, ECtHR at para. 53 in relation to 94.
161 Id. at para. 15 in relation to 53.
162 Id. at para. 53.
163 Id. at para. 15 in relation to 53.
164 Chipovski, ECtHR at para. 52.
165 There were ‘no statutorily prescribed time-limits’ in Martens, but there was an option to review the retention of DNA profiles in the database; see Martens, ECtHR at para. 46.
166 Familial searching is used when the profile of a criminal perpetrator is not kept in the database but may be traced from the profiles of their relatives including those who are already dead.
167 The accuracy of DNA matching probability and the practice of familial searching will no longer be an issue in the presence of a comprehensive DNA database since crime scene samples will be expected to have a direct one-to-one correspondence with a profile (or profiles if there are more than one perpetrator).
4. Retention of Data of Minors

One key issue in Marper was the retention of DNA profile data of one of the accused who was a minor. Citing Article 40 of the United Nations Convention on the Rights of the Child, the Court noted the ‘special position’ of minors in the criminal justice system especially regarding the protection of their privacy during criminal trials. In universal databases, collection of samples may vary from state to state. Should a state decide to collect samples at the time of birth—due to logistical considerations or peculiarities of its legal system—the enabling law shall provide data anonymization or pseudonymization as a legal safeguard until they reach the state’s minimum age of criminal liability. This safeguard will ensure non-use of biometric data until the time that their owners can be made liable for a crime in accordance with the state’s penal law.

5. Provision for Review

ECtHR case law places a high premium on the existence of a review provision in evaluating the acceptability of a national DNA database law. One key reason for the finding of a violation in Marper is the lack of provision for independent review in relation to the retention of DNA profiles and there was no ‘defined criteria’ to make the review possible and measurable like the evaluation of the seriousness of the offence, history of arrests, the strength of suspicion and other special circumstances. In Gaughran, the Court qualified the review further: it should provide effective relief to the applicant and not something ‘so narrow as to be almost hypothetical’. And it is the availability of review in Martens that rendered the retention of the applicant’s DNA profile acceptable although retention limit was not provided for in the domestic law. The enabling law for universal databases shall then include an option for those enrolled to review the faithful compliance by the state on the legal safeguards enshrined therein.

Another review safeguard emphasized in Gaughran and Chipovski is the possibility of deleting one’s DNA profile in the database. The Court held in Gaughran that the domestic law should allow those enrolled in the database to petition for the deletion of their file ‘if conserving the data no longer appears necessary in view of the nature of the offence, the age of the person concerned, the length of time that has elapsed and the person’s current personality’. In Chipovski, the Court ruled that it is not...

---

168 The Court found it ‘especially harmful’ due to minors’ ‘special situation and the importance of their development and integration in society’; see Marper, ECtHR at para. 124.
169 See Convention on the Rights of the Child, Article 40 (UN General Assembly, 1989).
170 Marper, ECtHR at para. 124.
171 Id.
172 One logistical consideration is to collect samples during mandatory newborn screening tests as discussed in Section 2.
173 The technical differences among anonymization, de-identification and pseudonymization are not discussed given the focus of this article. The main argument here is that DNA profiles may only be used to identify their source when they match a crime scene sample and only at the age of criminal responsibility which may vary according to the type of crime from state to state given the legitimate purpose behind their retention.
174 Marper, ECtHR at para. 119.
175 Gaughran, ECtHR at para. 94.
176 Martens, ECtHR at para. 46.
177 Or their parents and guardians in the case of minors.
178 Gaughran, ECtHR at para. 94.
enough for the police to be vested with power to delete personal data.\textsuperscript{179} The law should also specify the 'conditions under which it can be done and procedure to be followed.'\textsuperscript{180} Moreover, the law should provide for a 'specific review of the necessity of data retention.'\textsuperscript{181} The applicability of these review conditions to universal databases is doubtful as they go against the very essence of a universal database.\textsuperscript{182} If the Court would insist on their application to universal databases, it would be impossible for them to be established in Europe. What would be appropriate in a universal database system is the creation of a separate and independent review team composed of various stakeholders—representatives from government, scientists, NGOs and civic society groups—whose task is to conduct periodic reviews on the system’s adherence to the legal safeguards enshrined in the law \textit{in concreto} and \textit{in tempore}, with a corresponding power to propose sanctions in case of breach. The selection procedure on the composition of the review team may vary from state to state. In any case, its members shall be of proven integrity and are capable of working independently. Each member state can decide on the procedure for these review mechanisms given the peculiarities of their legal system subject to the Court’s final review when called for.

6. Data Security and Strict Penalties for Breach

ECtHR case law involving DNA profiles surprisingly did not indicate legal safeguards regarding data security in spite its classification of personal data protection under the right to respect for private life. Once translated into numerical data, DNA profiles can easily be copied from one computer to another or through cloud-based file sharing. The current practice of states covered by the Prüm Decision is to share their data electronically.\textsuperscript{183} They appear to ignore a possible hacking of their automated electronic sharing system. In universal databases, legislators themselves will be completely solicitous of DNA file data security because their own data are stored in the system.\textsuperscript{184} And the entire population will be keeping an eye over the way the system is administered. It is this egalitarian approach to universal databases that appears to provide more security to personal data and privacy.

\begin{itemize}
\item \textsuperscript{179} Chipovski, ECtHR at para. 53.
\item \textsuperscript{180} Id.
\item \textsuperscript{181} Id.
\item \textsuperscript{182} If people can opt out, it is no longer a universal database. The Portuguese government’s attempt to create a universal database is based on a volunteer-based system, although its manner of obtaining informed consent has been criticized to increase ‘mandatory volunteerism’; see H. Machado & S. Silva, \textit{Informed consent in forensic DNA databases: Volunteering, constructions of risk and identity categorization}, 4 BioSocieties 335, 345–6 in relation to 341 (2009).
\item \textsuperscript{183} See F. Santos & H. Machado, \textit{Patterns of exchange of forensic DNA data in the European Union through the Prüm system}, 57 Sci. Justice 307 (2017). See also S. Kierkegaard, \textit{The Prüm decision—An uncontrolled fishing expedition in ‘Big Brother’ Europe}, 24 Comput. Law Secur. 243 (2008). And also H.S. Muñoz & A. Fiodorova, \textit{DNA and law enforcement in the European Union: Tools and human rights protection}, 10 Utrecht Law Rev. 149, 151–4 (2014).
\item \textsuperscript{184} This was referred to by Kaye as a ‘simple precept’ or the Golden Rule where legislators and those who administer these databases ‘should do unto others as they would to themselves’. This can be viewed as a greater motivation for whoever will be responsible for creating a universal database law in their country to include sufficient safeguards for the protection of everyone’s right to privacy given that their own privacy rights are at stake. Additionally, it will also provide a greater motivation for those who will be tasked to administer these databases to be strict in following those safeguards because they themselves are included in these databases; see Kaye, \textit{supra} note 87, at 48.
\end{itemize}
Manual storage of DNA profiles appears to be the most secure way of maintaining universal databases. Computers shall be specifically dedicated for their use within a specified facility and a back-up facility created for that purpose. These computers shall not be connected to the internet and they are to be used solely for limited identification purposes.\(^{185}\) Manual storage of DNA data shall be supervised by an ‘independent database officer’ in order to protect it from political manipulation.\(^{186}\) Such exclusive facility is ideally an independent department (first department) not connected with the police and prosecution and shall only contain DNA profiles with codes assigned for each person as an identifier.\(^{187}\) A separate and independent department (second department) shall be keeping a copy of the names that correspond to those codes but without the DNA profile data.\(^{188}\) Disclosure of data will be regulated: only when there is a DNA profile match in the first department would the second department be tapped to determine the name of the person behind the DNA profile.

The personnel of the two departments shall be independent from each other.\(^{189}\) This system prevents leakage in the process of data sharing between computers in different facilities—including among member states under the Prüm Decision\(^{190}\) — making it secure from external hackers. Whatever possible breaches in unwarranted data exposure can be traced back to the personnel within the system.

Admittedly, manual storage is cumbersome but it will minimize the automatic processing of personal data thereby providing another layer of protection to the right to privacy. Member states shall be encouraged to incorporate severe and deterrent penalties in the universal database law for breach of this safeguard and less severe penalties for the breach of other safeguards. Legislators are expected to be more than willing to exact severe censures and penalties because their own personal data are included therein. Penalties may vary from member state to another depending on their

\(^{185}\) They shall only be used for authentication- and association-identification searches, and never for trait-identification as discussed in Section 4.

\(^{186}\) This idea is derived from Europol’s ‘independent data protection officer’; see Regulation (EU) 2016/794: On the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135/53 Article 41 (European Parliament and the EU Council, 2016). See also K. AMBOS, EUROPEAN CRIMINAL LAW 567–8 (2018).

\(^{187}\) One author suggested that a master list of the identities of persons with their code numbers be maintained by a separate agency and that police officers have to apply for a court order to access such identities. See Monteleoni, supra note 94, at 258.

\(^{188}\) Limited access with severe penalties for misuse has been regarded as a strong safeguard for to universal DNA databases. See N.A. Bennett, A privacy review of DNA databases, 41 I/S: J.L. & POL’Y FOR INFO. SOC’y 821, 837 (2008).

\(^{189}\) On the need for independence of the officers involved in data processing, see J. Kokott & C. Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR, 3 INT. DATA PRIV. LAW 222, 227–8 (2013). See also Nuffield Bioethics Council, supra note 56, at para. 4.74.

\(^{190}\) This suggestion is controversial as it may appear to go against the automatic processing of data under the Prüm Directives. It could be a propitious subject for a more extensive and separate research. See also V. Toom, Cross-border exchange and comparison of forensic DNA data in the context of the Prüm decision, POLICY DEPARTMENT FOR CITIZENS’ RIGHTS AND CONSTITUTIONAL AFFAIRS (EUROPEAN PARLIAMENT), www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604971 (accessed Apr. 28, 2021).
criminal justice system and tradition of imposing penalties. In any case, penalties should be serious enough to deter any breach of DNA profile data. 191

VI. CONCLUSION: IS IT RIPE FOR UNIVERSAL DATABASES TO BE ESTABLISHED IN EUROPE?

Using ECtHR’s extant ratio decidendi on DNA-related case law, it would be extremely difficult, if not impossible, for universal forensic DNA databases to be accepted as proportionate interferences to the right to respect for private life under Article 8 of the Convention. At the same time, there is a glimmer of hope at the horizon in the presence of sufficient legal safeguards as expounded on each of the four-fold tests employed.

Under the preliminary interference test, the all-inclusive coverage of universal databases constitutes a serious interference into a person’s private life as can be predicated from DNA-related case laws starting with Van der Velden. In order to limit the amount of data to be retained in these databases and thereby limit the sensitivity of the information retained, destruction of cellular samples after the generation of DNA profiles would be an appropriate safeguard.

As to whether the interference would amount to a violation of the right to respect for private life, the three tests of legality, legitimate purpose and proportionality show discordant results. Universal databases pass the legality test in so far as the availability of legal instruments within the Council of Europe that do not negate the possibility of their existence. However, under the element of foreseeability of the law, universal databases will fail if the Court will continue to confound the three meanings of identification—authentication-, association- and trait-identification. The prohibition of trait-identification is a legal safeguard that appears to lend more privacy protection compared to current police investigation practices such as DNA dragnets, shed DNA sampling, and familial and ethnic searching, the latter being described as a ‘highly sensitive’ procedure in Marper.

Universal databases pass the legitimate purpose test as long as they are used strictly for the purpose of crime prevention, and consequently, respecting the rights and freedoms of others, both under Article 8 § 2 of the Convention. Their use in criminal investigations appears to be more scientifically accurate given their person-specific matches—instead of current protocols using probability estimates—thereby making them less confounding for the trier of fact. The benefit of inclusion in a database has been indirectly recognized by the Court when it asserted that one may be ‘rapidly eliminated’ from the list of suspects in case of a non-match. It provides a sense of security for the innocent and a deterrent for the guilty to know that DNA matches may no longer be questioned for their statistical value. They may still be questioned for other matters like contamination of the crime scene sample but not for the DNA profile match itself. However, a DNA profile match is not the end-all and be-all of conviction. The speed and accuracy they lend to investigations should be balanced by a legal safeguard: DNA profile match data should not be used as a sole evidence for conviction. While a universal database will definitely assist the police and prosecutors in limiting the scope of their investigations, they should gather other supporting evidence if they want to

191 In the US, some states have elevated the misuse of DNA databases from a misdemeanor to a felony. See Peterson, supra note 45, at 1226.
secure a conviction. A court of law should dismiss a case that presents DNA profile matching as its sole evidence in a crime.

It is in the proportionality test where the biggest obstacle was encountered as case law revolves around measuring data retention safeguards with the presence of conviction, although the Court continues to provide protection to convicted individuals as shown in Gaughran and Chipovsky. Unless the Court uses a different set of lens in its assessment, it would be next to impossible for universal databases to pass judicial reckoning at the ECtHR. Be that as it may, legal safeguards were identified as necessary inclusions in a theoretical enabling legislation for universal databases to tilt the balance towards their acceptance: anonymization/pseudonymization of minors’ data until they reach the minimum age of criminal liability, retention limit up to the time of death, manual and independent data storage, severe penalties in case of data breach, and a provision for independent review on the state’s compliance to these legal safeguards.

The current principles used by the Court in adjudicating a possible violation of the right to respect for private life involving retention of DNA profiles cannot be squarely applied to universal databases. Judicial reasoning may focus more on equality of treatment, where inclusion in the database no longer amounts to the stigma of having been convicted or at least suspected of a crime, knowing that only the guilty will be prosecuted and the great majority of the innocent exonerated in a more expeditious manner in a universal database system. At the same time, it should be made clear that failure to strictly comply with the identified legal standards will further tilt the balance towards a finding of violation of the right to respect for private life under Article 8 ECHR.

CONFLICT OF INTEREST
The author has no financial, personal, academic, or other conflict of interest in the subject matter discussed in this manuscript.

ACKNOWLEDGMENT
The author is deeply grateful to Dr. Mr. Christina Peristeridou for her constructive insights on some parts of the paper.