Chapter 16
Ethics and Policy of Forensic Biometrics

Emilio Mordini

Abstract Ethical issues raised by forensic biometrics partly overlap with general ethical implications of biometrics. They include issues related to collecting, processing, and storing, personal data, privacy, medical information, and respect for body integrity, risks of misuse and subversive use, and respect for human dignity. There are, however, also ethical issues specifically raised by forensic biometrics. One of them is particularly intriguing. It concerns the nature of biometric evidence and to what extent biometric findings could be accepted as an evidence in court. At a first glance, this problem could seem purely legal, without major ethical implications. Yet, at a deeper analysis, it turns out to have significant ethical components. I will focus on them and on some recent policy developments in this field.

Ethical issues raised by forensic biometrics partly overlap with general ethical implications of biometrics [1]. They include issues related to collecting, processing, and storing, personal data [2], privacy [3], medical information and respect for body integrity [4], risks of misuse and subversive use [5], respect for human dignity [6]. There are, however, also ethical issues specifically raised by forensic biometrics. One of them is particularly intriguing. It concerns the nature of biometric evidence and to what extent biometric findings could be accepted as an evidence in court. At a first glance, this problem could seem purely legal, without major ethical implications. Yet, at a deeper analysis, it turns out having significant ethical components. I will focus on them and on some recent policy developments in this field.

E. Mordini (✉)
Responsible Technology SAS, 12 rue de Ia Chaussee d'Antin, 75009 Paris, France
e-mail: emilio.mordini@rtexpert.com

M. Tistarelli and C. Champod (eds.), *Handbook of Biometrics for Forensic Science*, Advances in Computer Vision and Pattern Recognition,
DOI 10.1007/978-3-319-50673-9_16

16.1 Biometric Evidence in Law Enforcement and Criminal Justice

The history of biometrics largely coincides with the history of its forensic applications, which include applications used for crime prevention, crime investigation, and administration of justice. Also prejudicial scientific discourses applied to criminology, such as physiognomy and phrenology, owed mostly to biometrics their temporary good scientific reputation (incidentally, this is likely to be one the reasons why biometrics have had later on such a bad press among human rights advocates and ethicists).

In early 1900s, law enforcement agencies started collecting fingerprints from convicted criminals and suspected individuals, and rather soon, they created vast fingerprint libraries. In parallel, the refinement of methods for latent fingerprints retrieval made biometric identification a fundamental tool for investigation at the crime scene. Finally, fingerprints (and later on, palm prints and impressions of bare soles) were accepted as admissible evidence into courts in most jurisdictions. Since then, biometrics (chiefly fingerprint) have been increasingly used for revealing or confirming the identity of people involved in the criminal investigation or in the judicial process (including victims); for establishing whether an accused person was at the scene of a crime or used an item that was used in perpetration of the crime; whether other person was at the scene of the crime or touched an item that was used in perpetration of the crime; whether an alleged victim was at some place that was consistent with the prosecution; whether a witness was at a place it is claimed he was. Biometrics have been also used to impeach the credibility or integrity of a suspect or a witness or a victim, based upon criminal records that show his prior history. Into courts, biometrics provided also a certain, additional, "scientific objectivity" to "traditional" (e.g., eyewitness) circumstantial evidence.

The way of assessing of biometric findings varies among jurisdictions, notably between common law and civil law systems. There are, however, also important similarities. As it happens with most scientific evidences,[1] usually biometric findings are not considered immediate evidence, but they have to be presented in court by one or more qualified experts who provide their testimony. Their opinions are assessed by the judge, who takes the final decision about whether biometric findings are admissible as an evidence in that specific case. In some jurisdictions (especially in the civil law area) the law establishes the minimum number of biometric details that should be analyzed in order to produce a positive identification; in other jurisdictions (especially in the common law area), the judge simply assesses experts' qualification and credibility. In both cases, the judge asks the expert to state whether a given biometric finding allows recognizing an individual, say, whether it matches with any recorded biometrics collected in the past, or with biometrics

[1]"Scientific evidence" in court is an evidence that is inferred from a known fact by using the scientific method.

gathered from any relevant individual involved in the judicial procedure. Experts are expected to answer yes or no.

In conclusion, the main events occurring under the heading of forensic biometrics include (1) the preventive activity of police and other law enforcement agencies, which collect biometrics from convicted criminals and suspected individuals in order to monitor them and prevent crime; (2) if a crime occurs, biometrics could be collected on the crime scene and in other relevant contexts, in order to ascertain the identify of supposed victims, suspected criminals, and alleged witnesses; (3) finally biometric findings are usually brought into court where the judge (after hearing experts and parties) decides whether, and to what extent, these findings could be considered an evidence and will contribute to form the judicial decision.

16.2 Digital Biometrics

This scenario is changing with the arrival of new digital biometrics. New digital biometrics (automated biometrics) entered into the market in the late 1970s, chiefly thanks to the development of new sensors, capable of capturing a vast array of different inputs. Sensors are devices that turn various inputs—generated by the interaction between them and physical object—into electrical outputs, whose electrical magnitude is proportional to the magnitude of the initial signal. Through the repetitive measurement of the electric output at certain intervals of time, the magnitude of the voltage is turned into a proportional number, which is further encoded into a binary number, or a gray code, or still in other ways. This allows representing bodily attributes (including those that were traditionally considered qualitative, such a skin color, or walking style) as measurable physical properties.[2] Two or more individuals could be subsequently compared in quantitative terms to ascertain whether they share the same properties as far as specific bodily attributes are concerned. From such a comparison, one could deduce whether two (apparent) individuals are actually the same individual, whose attributes were captured in different fractions of time, say, one could identify the individual (in the literally sense of assessing whether there is only one individual, considered under different accounts, instead of two or more distinct individuals). The main conceptual differences between pre-digital and digital biometrics is that digitalization allows performing the comparison (1) always in quantitative terms, avoiding qualitative assessment; (2) automatically, by exploiting ad hoc computer algorithms; (3) on a huge number of bodily attributes, unthinkable in the pre-digital era.

[2]Physical properties are discrete elements that can be put in bi-univocal correspondence with a set of numbers. There are seven base physical properties, Length, Mass, Time, Electric Current, Temperature, Amount of Substance, and Luminous Intensity. Biometric sensors measure one or more of these properties.

Absolute identity is logically and practically impossible. It does not take a Heraclitus, to realize that all bodily attributes, even the most stable and persistent, change (maybe slightly) over time, and conditions of data collection change, as well as sensor sensitivity. In other words, biometric features vary, sometime degrade by themselves; moreover, they also vary in the way in which they are presented to sensors. Finally, sensor precision is limited and may vary at different sites and according to different conditions of usage. This implies that it is impossible that two or more data sets captured by a sensor and turned into digits might exactly match, digit by digit. In other words, digital biometric recognition is always by approximation, and it inevitably implies some errors. This could be mitigated by creating, storing and comparing normalized biometric samples, called "templates". Yet errors cannot be eliminated because of their systematic nature. Accordingly, one of the main features to be considered in any given biometric system is always its error rate. One speaks of "false rejection", or "false negative", when the system fails to recognize someone; and "false acceptation", or "false positive", when the system recognizes someone erroneously. The ratio between false negatives and the total examined population is called "specificity"; the ratio between false positives and the total examined population is called "sensitivity". Specificity indicates the system ability to discriminate between different individuals; sensitivity indicates the system ability to detect all searched individuals. In principle, sensitivity and specificity are independent, in practice; there is a tradeoff, such that they are almost inversely proportional to one another. Also pre-digital biometrics could not avoid systematic errors, but their degree of uncertainty have been never studied in rigorous probabilistic terms, as it is today with new digital biometrics.

If only biometric features perfectly matching, point by point, led to recognition, the system would never recognize anyone because such a perfect identity can never be obtained. Consequently, the system tolerance level must be tuned, that is to say, the system must be "told" within what confidence interval it should consider two different biometric sets as though they were identical. In practice, this means that engineers have to decide when the gap between two biometric series can be considered negligible. Rather intuitively, the narrower the confidence interval is, the higher are the probabilities that the recognition is accurate, say, there will be less false positive. Yet, with a too narrow confidence interval, the system would increase the risk of failing to recognize the same individual presented twice, because the gap between his biometric features, taken in different moments and circumstances, could fall outside the confidence interval. Larger confidence intervals would mitigate this risk, but they would increase false acceptation (someone confused with someone else). It is important to emphasize that there is not a "right" confidence interval, but it depends on the specific context and application. Ultimately, the decision on the confidence interval depends on the policy adopted by system administrators.

16.3 Probabilistic Biometrics in Court

Past debates on forensic biometrics chiefly focused on conditions of admissibility of biometric evidence and qualifications of expert witnesses [7]. Today, legal experts, jurists, and scholars find increasingly problematic the probabilistic nature of biometric identification. I will only hint at the main terms of this debate, which is richer and full of nuances, because it is not the focus of my article, although it is a necessary premise to my argument.

Current debate on probabilistic biometrics in court is driven by two main facts. The first is a 1993 decision of the US Supreme Court,[3] which introduced new standards for scientific evidence. Although this decision was directly relevant only to the US legal system, its philosophy is considered a benchmark and has deeply influenced many other legal systems, including those belonging to the civil law area. In this sentence the Supreme Court ruled that a scientific evidence could be admitted into court only if it respects the following five criteria: (1) the evidence "can be (and has been) tested" using a scientific method; (2) such a method has "been subjected to peer review and publication"; (3) it is known the "potential rate of error" of the method in question; (4) the "existence and maintenance of standards controlling the technique's operation"; (5) the "general acceptance" of the technique within the relevant scientific community. Would biometric evidence survive *Daubert* criteria? This has been the core discussion, developed first within the US forensic community and then among scholars and legal experts belonging to other jurisdictions and legal schools. In particular, some scholars [8, 9] have argued that the scientific soundness and reliability of expert-testimony-based biometrics is definitely suboptimal. This was emphasized also by a few clamorous cases of error, for instance the one that occurred in the wake of Madrid terrorist attack [10].

The second driver of the current debate is a technological driver. With the rapid development of new digital biometrics (and a vast array of new biometric applications, exploiting modalities whose existence were not even imaginable in the pre-digital era) the issue of probabilistic identification has become paramount. Scholars [11, 12] have advocated a more mindful, and scientifically refined, approach to forensic biometric by adopting a probabilistic mindset. For instance, Champod et al. [13] have suggested that, instead of posing the naïf question whether a biometric feature is ***identical*** to another, a biometric examiner should ask to himself "*Given the detail that has been revealed and the comparison that has been made, what inference might be drawn in relation to the propositions that I have set out to consider?*" (p. 25).

The two discussions are clearly intertwined, as *Daubert* criteria should be applied to new digital biometrics, and digital biometrics should come to terms to more stringent legal criteria for admissibility of scientific evidence [14]. The interplay between the notion of forensic evidence and the probabilistic nature of

[3]Daubert v. Merrell Dow Pharm. Inc., 727 F. Supp. 570, 575 (S.D. Cal. 1989).

biometrics is the core of the next chapters, in which I will present my central argument.

16.4 Law Enforcement and Administration of Justice: Two Different Missions

In the first chapter of this paper, I listed the main activities included under the heading of forensic biometrics, say, anticipation of crime, criminal investigation, and administration of justice. Although practically and theoretically distinct, these three main activities belong to a unique cycle, whose languages must be interoperable if the cycle works. Two of these activities (anticipation of crime and criminal investigation) are carried out by law enforcement agencies; the third (administration of justice) is up to the judicial system. Law enforcement and judicial systems are thus distinct but interoperable. Their missions are different, yet in democratic and liberal societies, they have been developed rather harmonically in order to compensate each other.

Law enforcement's overarching mission is to prevent, and, in case, repress crime. To be sure, crime prevention includes many other activities, which are not up to law enforcement agencies, such as education, social policies, urban management, and so. Yet, there is an important aspect of crime prevention that is up to law enforcement authorities, that is to say, pre-crime (anticipative) investigation. Anticipative investigation [15] aims to prevent crime by identifying potential criminals and future criminal events, and by taking action accordingly. Ultimately, anticipative investigation is based on the assessment and management of risks, its goal is to prevent risks or, at least, to mitigate them. While anticipative investigation is proactive, criminal investigation is reactive, it follows crime and it aims to ascertain facts, identify, and prove the guilt of one or more suspects. Ultimately, its goal is to repress crime by bringing the suspects into the judicial system. Overall, anticipative and criminal investigations do not aim to discover truth, to pursue justice, or to achieve fairness—at least as their primary goal—rather they simply aim to reduce the rate of crimes in society. Unpleasant though it may sound, law enforcement must be ruled by the "principle of suspicion" (of course opportunely mitigated), that is to say, anybody could be in principle suspected.

The judicial system aims instead to administer the justice. What is "justice"? Lay citizens often think that making justice means to discover factual truth about a crime or a civil case. Yet legal scholars know that in court factual truth is hardly at stake. Actually, the business of a court of justice is not to discover the truth, as Oxford professor and distinguished English legal scholar, Sir Frederick Pollock (1845–1937) put it,

> Its real business is to pronounce upon the justice of particular claims, and incidentally to test the truth of assertions of fact made in support of the claim in law, provided that those assertions are relevant in law to the establishment of the desired conclusions [16]

In other words, the goal of the judicial procedure is not to ascertain the "truth" in trivial sense, rather to identify the "legal truth". The "legal truth" is the truth as it emerges from the judicial hearing [17]. It may or may not corresponds to the totality of facts. Even when it does not correspond to facts, the "legal truth" is still practically effective, say, it produces effects, as it is showed, for instance, by the principle that a defendant cannot be tried twice on the same charge following a legitimate court decision. The notion of "legal truth" is better understood by considering it in parallel with another notion, which is foundational for the whole Western legal system, the principle of presumption of innocence. Presumption of innocence is a legal principle adopted in criminal cases. In criminal cases, the gap between "factual" and "legal" truths could produce inacceptable outcomes; presumption of innocence mitigates this risk. Its original formulation dates back to Roman law and reads "*Ei incumbit probatio qui dicit, non qui negat*" (the burden of proof is on he who declares, not on he who denies), also "*in dubio pro reo*" (when in doubt, for the accused).[4]

In modern terms, presumption of innocence is usually expressed by saying that a defendant is innocent until proven guilty,

> In a criminal case the truth of facts against the accused must be established "beyond a reasonable doubt," and in certain civil cases, e.g., where punitive damages may be awarded for fraud, the truth of facts against the defendant must usually be shown by "a clear and convincing preponderance of the evidence". The more that is at stake, e.g., criminal blame, or punitive damages, the higher the standard of proof. In an ordinary civil case involving an ordinary claim for damages, the facts against the defendant need only be shown by a "balance of probabilities", a significantly lower standard of truth. Thus, depending on the relevant standard of truth, the very same evidence would warrant a finding of truth in one type of case but not in another. Thus, truth varies with standards of proof, and standards of proof vary with what is at stake. Yet, as indicated, there are good reasons for these variations in standards of truth. In criminal cases for example, we accept a higher risk of erroneous acquittals in order to minimize the risk of erroneous convictions. Moreover, this may have the effect of increasing the total number of erroneous verdicts. Our tolerance for the risk of divergence, here, goes up the more that is at stake [17]

Presumption of innocence, which was initially a legal procedural rule, has become one of the main principles of Western legal systems, a constitutional principle in many democracies,[5] and a fundamental human right. The Universal Declaration of Human Rights, Article 11, reads

> Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defense

Similarly Article 6.2 of the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe reads

[4]"*Digesta seu Pandectae* 22.3.2" (http://webu2.upmf-grenoble.fr/Haiti/Cours/Ak/Corpus/d-22.htm).

[5]Presumption of innocence is mentioned for instance by Italian, French, German, Brazilian, Canadian, Russian constitutions. It is not explicitly mentioned by the US Constitution, yet there is a consensus that it follows from the 5th, 6th, and 14th amendments.

> Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law

Finally, the same principle is iterated by Article 48 of the Charter of Fundamental Rights of the European Union, which reads

> Everyone who has been charged shall be presumed innocent until proved guilty according to law

In conclusion, law enforcement and administration of justice have different (although congruent) missions and follow two distinct logics; the former is ruled by the *principle of suspicion*, while the latter is governed by the *presumption of innocence*. In democracies, these two different perspectives are mutually consistent, because systematic errors made by the former are compensated by systematic errors made by the latter. In other words, the law enforcement system shows a natural tendency to minimize false negative (no criminal should get off scot-free), although this could rise false positive (an innocent could be unjustly accused); the judicial system shows the opposite behavior, say, it aims to keep false positive as lower as possible (no innocent should be wrongly condemned), although it could increase false negative (it could happen that a guilty individual is acquitted). If the two systems work properly, and each one of them respects its mission, the overall cycle functions rather well because opposite errors mutually compensate. The law enforcement tight mesh net may capture also innocents, but they will be eventually released by the judicial wider mesh net (of course, it is always possible that a criminal escapes and an innocent is condemned, I am just arguing that the two systems are theoretically complementary).

16.5 Probabilistic Biometrics and Presumption of Innocence

I have illustrated the probabilistic nature of biometric recognition and the way in which biometric applications deal with it, by tuning the tolerance of the system according to different user requirements. I would like now to pose a question: could law enforcement and judicial systems adopt the same degree of tolerance? Say, are user requirements the same in the two systems, which jointly form the forensic cycle? This question could seem purely technical; on the contrary, I argue that it is the main ethical question raised by forensic biometrics.

Suppose that positive identification is the critical element to determine who committed a crime (e.g., detecting and identifying terrorists who attacked a metro station). Suppose that positive identification should rely on biometrics (e.g., face recognition carried out on a videotape recorded on the crime scene) and suppose that the biometric matching system is based on a similarity score[6], which range from 0.0

[6]Beyond similarity scores, there are also other mathematical tools used for comparing two biometrics, but this would not change the sense of my example.

(no match at all) to 1.0 (exact match digit by digit). As I have previously explained, a perfect match is theoretically and practically impossible, consequently the similarity score should be set by administrators at any value lower than 1.0. For instance, if one sets the system at a similarity score of 0.95, it means that only biometrics which have a score beyond this threshold will match. Now, suppose that we know (from previous performance tests) that a 0.95 score implies a very low—suppose 0.1%—risk of false recognition (that is to say, almost all recognitions are right). Yet from the same tests, we also know that the score 0.95 implies 20% failed recognition (20% guilty individuals who escape from our biometric fishnet). If we lower the score to 0.75, the failed recognition rate will decrease dramatically to 1% (only 1% guilty individuals would escape recognition). Unfortunately, such a lower score would also provoke a hike of false recognitions, which would increase to 10%, say, our fishnet will wrongly fish also 10% innocent people. What should system administrators do? In the investigation phase, they would be plenty legitimate to set the system at the lowest similarity score compatible with its correct use. This would respect the logic behind criminal investigation, which aims to avoid that a criminal gets off scot-free. This might imply that some 10% innocent people are unjustly accused of being terrorists. In an ideal world, these people would be discharged by the judicial system. What happens if probabilistic digital biometrics is admitted as an evidence in court? It happens that the 10 % innocent people of our example are burdened by a "positive identification", notwithstanding the doubt that they could be "false positive". The principle of presumption of innocence is de facto bypassed, because its foundation, *in dubio pro reo*, could not put up with an evidence obtained through a system whose initial aim was to detect the highest number of suspects.

I argue that if a biometric system is tuned in order to meet law enforcement requirements, its results should not be transferred, as they stand, into the judicial system, which has different, even opposite, user requirements. Also pre-digital biometrics were somehow probabilistic, at least in very rough terms, but today one can set the degree of confidence of the system. In other words, differently from the past, probabilities of recognition can be tuned. If biometrics in law enforcement were tuned to minimize the risk of false recognition, I would not see any ethical problem in being their results transferred in court as well. Yet, would law enforcement agencies ever accept to purchase (and use) a system burdened by a higher failed recognition rate when that system could be tuned in order to minimize it?[7] I doubt.

If a system fulfills law enforcement requirements, it cannot also fulfill judicial requirements, and vice versa. Both requirements are fully legitimate, but they should work in parallel. If one of them "takes the leadership" (notably, law enforcement requirements) this becomes a serious ethical and democratic problem.

[7]The biometric performance at different thresholds is expressed through the "Detection Error Tradeoff" (DET) curve.

16.6 Solutions and Trends

The ideal technical solution to this ethical challenge would be to develop more robust, accurate, and sensitive, biometric applications, with negligible false rejection and false acceptance rates. If false rejection and false acceptance rates were truly negligible, the contradiction between law enforcement and judicial system requirements would be eliminated and one could transfer results from one system to the other, without major ethical issues. This is the illusion that has ruled forensic biometrics till almost today. This illusion is no longer tenable and there are not current applications which are contemporarily—in real life (not in labs)—as specific and sensitive as to consider negligible both their false rejection and false acceptance rates. In principle, a strategy exists that could increase contemporarily both specificity and sensitivity. This strategy is based on tighten requirements on the quality of biometric input data. Unfortunately, this would imply that a larger number of people could not be enrolled in the system, because of their poor biometric features, due to various causes, including the way in which in real life conditions biometric features are presented to sensors. Notably, this solution would not be applicable to biometrics extracted from materials, which were not originally designed for collecting biometrics. This is the case of latent fingerprints, but also of other "biometric traces" (e.g., recorded images, voices, pictures, etc.) that we are increasingly able to detect and collect for forensic reasons.

This leads to the problem posed by biometrics extracted from outside the forensic context, and brought into the legal cycle only at a later stage. Recorded faces, images, and voices, found online, in the Internet, are the largest (accidental) biometric library ever created (it is enough to think of the number of freely available pictures of Facebook users). Searching these huge, dispersed, online, databases is becoming one of the main activities, not only in criminal investigations, but also in crime prevention and judicial decisions.[8]

Online face and voice recognition—often coupled with soft biometrics[9] and geolocalization—are increasingly used for searching and recognizing people. This is destined to become still more pervasive with the arrival of new and emerging biometrics. New behavioral biometrics (also including electrophysiological biometrics) and cognitive biometrics will be able not only to extract biometric features from recorded online materials, but also to elicit meaningful biometric information from online behaviors and human-machine interaction patterns. New biometrics are extremely promising for law enforcement purposes. Will these biometrics be ever

[8]To give an idea of the magnitude and pervasiveness of this phenomenon, it is enough to mention that the Internet is today the main source of evidence on marriage validity or nullity in Catholic ecclesiastic courts.

[9]Sex, ethnicity, age, body shape, skin color, and so.

admissible in court? I doubt if presumption of innocence still rules criminal proceedings. Yet, trends seems to go toward an opposite direction.[10]

In November 2013, the European Commission presented a package of proposals to strengthen procedural safeguards for citizens in criminal proceedings. *Inter alia*, these proposals included a proposal of "*Directive on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings*",[11] aiming at harmonizing this principle (considered chiefly in its dimension of procedural right instead of human right) in different EU jurisdictions. When legislators feel the need to rule on great principles, it is often because they aim to mitigate them. Indeed, after a long preamble and four initial, generic, articles, Art.5 of the proposal directive focuses on *Burden of proof and standard of proof required.* Par.1 reaffirms the principle that

> Member States shall ensure that the burden of proof in establishing the guilt of suspects or accused persons is on the prosecution. This is without prejudice to any ex officio fact finding powers of the trial court

But Par.2 seriously mitigates it, by allowing Member States to shift the burden of proof on the defendant for any "*sufficient important*" (!) reason

> Member States shall ensure that any presumption, which shifts the burden of proof to the suspects or accused persons, is of sufficient importance to justify overriding that principle and is rebuttable.
> In order to rebut such a presumption it suffices that the defense adduces enough evidence as to raise a reasonable doubt regarding the suspect or accused person's guilt.

The Commission explained the rationale behind Art.5 Par.2 in an accompanying Communication on Making progress on the European Union Agenda on Procedural Safeguards for Suspects or Accused Persons—Strengthening the Foundation of the European Area of Criminal Justice,[12] which reads,

> In criminal proceedings, the burden of proof should be on the prosecution and any doubt should benefit the suspect or accused person, without prejudice to the independence of the judiciary when assessing the suspect or accused's guilt. A judgment must be based on the evidence put before it and not on allegations or assumptions. However, the ECtHR[13] has accepted that in specific and limited cases, the burden of proof may be shifted to the defense, and the Directive will reflect this standard, striking a balance between the public interest in effective prosecution and the rights of the defense.

[10]In his 2003 paper on Evaluation of Forensic Science [18], Arizona State University Professor of Law, Michael J. Saks, raised the issue of reversal of the burden of proof related to biometric evidence. His argument is different from mine, because he focuses on the fact that some courts are asking the defendant to demonstrate that biometric evidence ***does not*** fulfill *Daubert* criteria, instead of assessing by themselves whether it does. However, it is interesting to note that trends move in the same direction.

[11]COM(2013) 821 final, Brussels, 27.11.2013.

[12]COM(2013) 820 final, Brussels, 27.11.2013.

[13]European Court of Human Rights.

The initial formulation of COM (2013) 821 has raised many perplexities in the LIBE[14] (main) and in the JURI[15] (opinion) Committees of the European Parliament. More recently, the Council[16] has proposed to modify Art.5 Par.2 by eliminating the expression "*sufficient importance*" in its place listing cases in which it would be possible to shift the burden of proof on the defendant, say,

> (…) in two situations:
>
> (a) in case of certain minor offences, notably traffic offences (see recital 15a);
> (b) in case of certain other types of offences, when two conditions have been complied with:
>
> (i) the shifting of the burden of proof must be strictly necessary in the interest of the criminal proceedings; and
> (ii) the shifting of the burden of proof must be justified to override the principle that the burden of proof is on the prosecution (see also recital 15b);

It is definitely out of scope of this article to discuss this important debate, and its potential consequences on the European legal system. I think that the reader has probably understood that the issue at stake is something more important than "minor traffic offences".[17] This is also suggested by the web page of the *Justice Directorate of the European Commission*, which is not, of course, a Commission official statement or a policy document, but it is expected to represent the Commission's point of view,

> When designing and implementing measures in this field, it is important for the EU to get the balance right between measures that protect such rights and those that *facilitate*[18] the investigation and prosecution of crime [19]

This is why the current debate is likely to be so relevant also to ethics of forensic biometrics, because it finally concerns the delicate balance between pursue of the common good, and respect for individual liberty.

References

1. Mordini E, Tzovaras D (2012) Second generation biometrics: the ethical and social context. Springer, Berlin
2. Mordini E, Massari S (2008) Body, biometrics, and identity. Bioethics 22(9):488–498
3. Mordini E (2008) Nothing to hide. biometric privacy and private sphere. In: Tistarelli M, Juul N, Drygajlo A, Schouten B (eds) BIOID 2008 Biometrics and identity management, Springer, Berlin, Heidelberg, pp 247–57

[14]European Parliament Committee on Civil Liberties, Justice and Home Affairs.

[15]European Parliament Committee on Legal Affairs.

[16]Council of the European Union, 12196/14, Brussels, 29 July 2014.

[17]It is worth recalling that the issue of presumption of innocence has been one of the main issues at stake in the US legal, political, and ethical debate on war on terrorism and terrorists' detention.

[18]My italics.

4. Mordini E, Rebera AP (2013). The biometric fetish. In: About I, Brown J, Lonergan G (eds) People, papers, and practices: identification and registration in: transnational perspective, 1500−2010 London, Palgrave, pp 98−111
5. Mordini E (2009) Ethics and policy of biometrics. In: Tistarelli M, Stan ZL, Chellappa R (eds) Handbook of remote biometrics for surveillance and security. Springer, Berlin Heidelberg, pp 293–309
6. Mordini E, Rebera AP (2011) No identification without representation: constraints on the use of biometric identification systems. Rev Policy Res 29(1):5–20
7. Moenssens AA (1963) Admissibility of fingerprint evidence and constitutional objections to fingerprinting raised in criminal and civil cases. Chicago-Kent Law Rev 40(2):85–124
8. Kaye DH (2003) Questioning a courtroom proof of the uniqueness of fingerprints. Int Stat Rev 71:521–533
9. Haber L, Haber RN (2004) Error rates for human latent print examiners. In: Bolle R, Natalini R (eds) Advances in automatic fingerprint recognition. Springer, New York, pp 339–360
10. Stacey R (2004) Report on the erroneous fingerprint individualization in the madrid train bombing case. J Forensic Ident. 6(54):706–718
11. Champod, C. (2000). Standards of proof. In: Siegel J(ed) Encyclopaedia of forensic sciences, Academic Press p 890
12. Egli NM, Champod C, Margot P (2007) Evidence evaluation in fingerprint comparison and automated fingerprint identification system—Modelling within finger variability. Forensic Sci Int 167:189–195
13. Champod C, Lennard C, Margot P, Stoilovic M (2004) Fingerprints and other ridge skin impressions. CRC Press—Taylor & Francis, London
14. Cole S (2008) Comment on 'scientific validation of fingerprint evidence' under Daubert'. Law Probab Risk 7:120–132
15. Hirsch Ballin MF (2012) Anticipative criminal investigation. Springer, Berlin
16. Pollock F (1922) Essays in the law. Oxford University Press, Oxford
17. Summers RS (1999) Formal legal truth and substantive truth in judicial fact-finding—their justified divergence in some particular cases. Cornell Law Faculty Publications, Paper 1186
18. Saks MJ (2003) The legal and scientific evaluation of forensic science (especially fingerprint expert testimony). Seton Hall Law Rev 1167–87
19. European Commission (2014) Rights of suspects and accused. http://ec.europa.eu/justice/criminal/criminal-rights/index_en.htm. Accessed 2 June 2015