Civil society stakeholder views on forensic DNA phenotyping: balancing risks and benefits

ABSTRACT
Forensic DNA phenotyping (FDP) is an umbrella term for practices seeking to infer likely phenotypic characteristics based on crime scene DNA. Specifically, it is intended to help criminal investigators find an unknown suspected perpetrator by providing information about what the suspected perpetrator may look like based on the analysis of DNA left at the crime scene. While many purport the usefulness of FDP in this regard, its probabilistic nature, as well as its ability to disclose information about an individual that may be considered private, raises a range of ethical and social concerns. This paper reports findings from interviews with thirty civil society stakeholders across nine European countries. Our findings reflect the wide variation of views in Europe regarding if, when and/or how the technology should be used in the criminal justice system, and we illustrate this by presenting the different ways in which our participants strike a balance between the potential usefulness of the technology, and the various ethical and social considerations.

KEYWORDS
Forensic DNA phenotyping, forensics, DNA, ethics, interviews, qualitative research, privacy, discrimination, molecular photofitting, ancestry testing, public engagement
INTRODUCTION

Forensic DNA phenotyping (FDP) is a technological practice which seeks to make probabilistic inferences regarding an individual’s phenotype based on the analysis of unknown origin DNA left at a crime scene. Exact definitions of FDP vary between contexts and stakeholders [1], but for the purposes of this paper we use this term to refer to a cluster of technologies used for the probabilistic inference of externally visible characteristics (EVCs) (appearance, such as eye, hair and skin colour), as well as for age and biogeographical ancestry (BGA). While many purport its usefulness as an investigative tool for criminal investigations [2], its probabilistic nature, and the possibility that information considered private may be inferred from it, raise a range of ethical and social concerns, predominantly relating to privacy and discrimination, but also to issues of resource allocation, utility and value, and to the interpretation of findings [3]. While such ethical and social concerns have been mapped out in both the scholarly and grey literature (see below), controversies remain about how to address these concerns at a governance level. To address this, scholars have proposed a proportionate approach to balance any potential security or justice benefits of FDP against possible intrusions of privacy, discrimination, or other potential harms [4]. This approach mirrors strategies for the governance of other forensic technologies [5-9]. It says little, however, about how such balancing of potential benefits and harms should take place in practice. In terms of substantive discussions about how and where boundaries between acceptable v. unacceptable practices should be drawn, many authors suggest that FDP should only be used for externally visible traits (i.e., those that are clearly apparent to people looking at a person, as opposed to ‘internal’ traits, such as health- and disease-related aspects), only for ‘serious crimes’, or only as a ‘last resort’ (for a review, see [3]). Such an approach of “regulation by exceptionality” [10] – meaning that a technology is introduced with the intention that it should only be used in exceptional circumstances – is already applied in decision-making processes regarding other forensic technologies in the criminal justice system, such as for familial searching.\(^2\) Granja and Machado argue that such an approach of regulation by exceptionality:

\[\text{separates what is serious enough [in terms of the crime committed] from what is not, what could be solved through other investigative leads from what cannot be, and from what is generally ethically acceptable and what is not. In other words, this regulatory framework}\]

\(^1\) We acknowledge, and indeed our previous research has identified, that professional stakeholders differ in their views regarding whether age and/or BGA should fit under the umbrella of FDP.

\(^2\) Familial searching is a technology that detects genetic relatedness. The term is generally used to refer to searches conducted in criminal DNA databases to identify criminal suspects through their connection with relatives.

defines the stipulated limits of privacy, confidentiality, equality, and (the presumption of)
innocence within the bounds of a particular criminal case [10].

In the Netherlands, one of the few countries worldwide that explicitly allows FDP in case work and
has specific laws to govern it, some of the above goals and limitations have been enshrined in law.
For example, DNA-based phenotypic testing for sex, biogeographical ancestry (“race”) and hair and
eye colour is permitted only for serious offences [11]. In the European Union (EU), there is only
one other country, Slovakia, that explicitly allows the use of FDP (for the ‘prediction of visible
phenotype demonstrations’ in connection with severe crimes); all other EU countries – alongside
most countries in the rest of the world – have no explicit frameworks for FDP (though the German
Land of Bavaria has explicitly permitted FDP use for BGA, age, and hair, eye and skin colour to
pre-empt immediate threats – that is, not for the investigation of crimes that have already taken
place). Whether FDP is allowed in these countries, and under what circumstances it can or cannot
be used, needs to be inferred from a careful interpretation of laws on genetic testing for criminal
justice, as well as other relevant laws [11].

Exploring the ‘ethical moment’
Ethical discussions regarding FDP use and regulation can been viewed as an ‘ethical moment’ [12]
in the technology’s development. Heeney describes an ethical moment as a period when what is
ethical in terms of any new technology comes into question, and conflicts emerge regarding how to
proceed with regulation and practice [12]. Ethical moments offer deliberative opportunities to
discuss different understandings about FDP and the potential ways of it ‘being’ in society, which
can help with governance efforts [4].

In this paper we were interested in gaining an understanding of this ethical moment from the
perspective of people and organisations who have a stake in the issue of FDP use and regulation
because they represent minority groups, victims of crime, or because they are dedicated to data and
civil rights protection. Our research question was: What are the views, opinions and experiences of
European civil society members who have a stake in the issue of FDP regarding the use and
regulation of this technology? The importance of listening to the views of civil society stakeholders
on technology development and use – and feeding these views into policy processes - is well-
established [6, 13-15]. More broadly, public engagement is widely seen as a necessary condition for
good research practice, and this is part of a broader shift in science governance that includes
engagement and deliberation strategies within understandings of responsible research and innovation (for example, see [13, 16, 17]). Indeed, evidence is emerging on the beneficial impact of public engagement strategies [18], which are seen to empower members of the public to play a role in shaping current or future research or governance practices [19]. Given this, calls for engagement with stakeholders and the wider public specifically in the area of genomic technologies more broadly [1, 20-22] and particularly in the forensics arena [23-26], have been particularly prominent, while other authors have called for caution about engagement strategies and practices that may turn out to be tokenistic or merely symbolic. Engagement strategies that serve the primary purpose of granting legitimacy to decisions that experts and other elites have taken would be highly problematic, not only in that they reduce trust in public engagement [27], but also in that they are disrespectful of the stakeholders and publics that participated in such engagement.

Granja and Machado have argued that understanding stakeholder views in forensic technologies allows us “to interrogate the different elements that compose the social construction of notions such as social risks, public good, and the accountability of the state” from the perspective of civil society [10](p. 4eprint). This is vital, state Williams and Johnson, because ‘what seems operationally ingenious to investigators [in terms of DNA profiling technologies] may seem dangerously intrusive to external observers’ [28](p. 17). Indeed, work in the “sociology in bioethics” literature [29, 30] argues that understanding the plurality of stakeholder ‘ethical vantage points’ in terms of how they each construct relevant ethical issues and have different ethical obligation sets allows a valuable lens for understanding the ethics of FDP use, and to question the traditional centre of gravity of ethical analysis and eventual governance.

While the need to understand civil society stakeholder views about FDP is clear, very little research so far has done this in connection with FDP [31]). The objective of this paper is to start filling this gap by exploring and reporting the views of members of civil society with a stake in the issue of FDP about this technology, specifically for the European context.

We conducted 30 interviews across nine EU countries with people in civil society stakeholder organisations to explore the considerations that weight into their decision of whether to use FDP in any specific context. Our findings show how and where these stakeholders strike the balance between such considerations. Before presenting our findings, we contextualise them by reviewing some key ethical and social issues associated with using FDP in the criminal justice system.

*Forensic DNA phenotyping: relevant ethical and social challenges of implementation*
Our structured literature search of the scholarly and grey literature has identified a number of ethical and social challenges related to the use of FDP within the criminal justice system [3]. The most prominent concerns are related to privacy, discrimination and interpretation of findings. We discuss these here, pointing to key issues of contention, though note that other concerns have also been raised relating to notions of resource allocation, utility, value and mis-use.

First, many scholars, particularly social scientists and ethicists, have raised concerns about the nature of the information that FDP can provide, and the possibility of such information being overinterpreted, or considered more reliable than they are (for example, see [32]). These scholars highlight that FDP results are, by nature, always probabilistic and thus contain a level of uncertainty. Because probabilistic information – especially, but not only, in the context of genetics – is known to be difficult for human beings to grasp, there is the concern that the complexity involved in understanding this probabilistic nature of FDP may lead to police and justice officers’ over-interpretation of the findings [33-37]. Such concerns, these critics say, are compounded by the fact that studies suggest people have greater trust in the scientific accuracy of forensic DNA technologies than other types of information and evidence in forensics and criminal investigation – a phenomenon that has been termed ‘CSI’ effect (e.g. [38-43]). These scholars argue that, if too much emphasis is placed on these probabilistic findings, they could spur criminal investigators to potentially follow false leads, wasting valuable resources [44-46]. This risk is particularly high in the absence of established standards to translate the raw data emerging from an FDP test into predictions of physical appearance - meaning that there is a greater likelihood that police officers and others could mis-interpret the findings [47-49]. Finally, a number of scholars (mostly from the social sciences, ethics, and law) also emphasise that even if we assumed that FDP findings could accurately predict externally visible traits, characteristics such as eye or hair colour can easily be changed [46, 50-55]. Others, particularly forensic scientists, recognise concerns related to the interpretation of FDP findings as important, but they note that this technology is just one tool at the disposal of the police officer; proportionate weight should be placed on FDP findings; and the purpose of FDP is to act as one part of many pieces of evidence (for a review see [3]). Instead, these and other scholars call to train, educate and provide information to stakeholders in the field (e.g. police and justice officers), to establish common standards of FDP use, and to implement them at the local level [34, 44, 47, 56, 57].

Second, many social science and ethics scholars worry that FDP use could lead to, or exacerbate, undue discrimination, in particular of minority groups. They see this as resulting, for example, from database and algorithmic bias causing some populations to be over- or under- represented in terms
of prediction values [49, 58]. It could also materialise at the operative investigative level, where scholars are particularly concerned that probabilistic BGA inference could lead to racial profiling if law enforcement make decisions based on predisposed expectations about the link between BGA and racial/social identity [35, 59-61]. Social scientists Williams and Wienroth (2017) also note a potential for stigmatisation of particular ethnic groups who become the focus of investigative attention based on a BGA prediction [6]. These authors argue that even though these persons may become persons of interest on the basis of other types of police intelligence, this does not mitigate the risk of undue discrimination because ‘the positive and negative meanings accorded to genetic science mean that more investigative weight, as well as more social freight, accompany its deployment’ [6](p.161). Finally, some social science scholars speak of an intrinsic discriminatory nature of FDP given that its primary function is to implicate or rule out minority populations during a criminal investigation; and also because its use may lead to reification of the belief in the biological basis of race, which might, in turn, deepen the social divide between different groups or individuals [56, 62-66]. As we highlighted in our structured review of the literature [3], others reject these concerns, arguing that if evidence points to an individual from a specific continental region being involved in a crime, this is not to be considered racial profiling [52, 60, 67]. Rather, as lawyer Charles MacLean posits, FDP might do the opposite, such as by proving that a perpetrator does not have ancestry from a specific continental or sub-continental region, which might lead even racially biased investigators to overcome their prejudices [51, 67, 68]. Moreover, forensic scientist Manfred Kayser and others hold that if an unknown perpetrator’s predicted phenotype does not match a minority group this may help avoid discrimination [53, 69, 70].

Finally, FDP use is seen to raise a range of privacy concerns. Concerns about privacy have long been at the centre of ethical and legal interrogations of forensic genetics [6] and although the concept of privacy lacks consensus, most societies recognise that people have a legitimate ethical and legal expectation that certain kinds of information about them be kept private [71]. Some scholars, mainly including forensic scientists and lawyers, purport that FDP does not violate any aspect of a suspect’s privacy because the phenotypic traits being tested are not only known to the person already, but to everybody who has ever seen the person, and as such cannot be considered private data [2, 52, 70, 72, 73]. Others, among whom are many ethicists, disagree, pointing to the possible infringement on privacy in situations where the face an individual presents to the world

---


6 We note here that most of these scholars refer to age and ancestry – the situation is more complicated for BGA, as BGA inference may not always reflect what a person looks like.
does not reflect her genetic endowments [62]. Others again claim that because FDP analyses
does not reflect her genetic endowments [62]. Others again claim that because FDP analyses
personal genetic data it will inevitably infringe privacy rights. Moreover, argue social scientists
personal genetic data it will inevitably infringe privacy rights. Moreover, argue social scientists
Williams and Wienroth (2017), we must also address threats to the privacy of those who might be
Williams and Wienroth (2017), we must also address threats to the privacy of those who might be
approached to be sampled because they are members of a ‘suspect’ population. These authors argue
approached to be sampled because they are members of a ‘suspect’ population. These authors argue
that whilst consent is sought for this process, there are ‘*informational privacy rights that reside in
that whilst consent is sought for this process, there are ‘*informational privacy rights that reside in
the person’s sample [and whilst] principles of retributive justice and solidarity may be used to
the person’s sample [and whilst] principles of retributive justice and solidarity may be used to
justify the request...the persistence of opposing values means that some assessment of the
justify the request...the persistence of opposing values means that some assessment of the
proportionality of the privacy breach will need to be made on a case-by-case basis’ (p.158).
proportionality of the privacy breach will need to be made on a case-by-case basis’ (p.158).

Data protection issues have also been heavily discussed in the literature. Scholarly discussion has
Data protection issues have also been heavily discussed in the literature. Scholarly discussion has
addressed whether FDP tests should remain within the laboratory and the police should only receive
addressed whether FDP tests should remain within the laboratory and the police should only receive
the narrative descriptions of the findings, when narrative FDP information should be deleted, how
the narrative descriptions of the findings, when narrative FDP information should be deleted, how
long the FDP information should be kept if the case is not closed, whether current measures of data
long the FDP information should be kept if the case is not closed, whether current measures of data
protection are sufficient, and whether current practices within laboratories exist for deleting and
protection are sufficient, and whether current practices within laboratories exist for deleting and
encrypting FDP data (for a review see [3]). It is vital that such questions be addressed when
encrypting FDP data (for a review see [3]). It is vital that such questions be addressed when
considering the use of FDP in the criminal justice system, though such questions are not considered
considering the use of FDP in the criminal justice system, though such questions are not considered
in the remainder of this paper, and will be addressed in future publications.
in the remainder of this paper, and will be addressed in future publications.

**METHODS**

**Purpose**

Against the backdrop of the concerns discussed in the published literature, our research sought to
Against the backdrop of the concerns discussed in the published literature, our research sought to
enrich the debate by bringing in the voices of civil society stakeholders. It was carried out within
enrich the debate by bringing in the voices of civil society stakeholders. It was carried out within
the DEIDENTIFIED study. Our interviews were focused on the eight EU member states
the DEIDENTIFIED study. Our interviews were focused on the eight EU member states
represented in the DEIDENTIFIED project, bar one interview conducted with a Belgium
represented in the DEIDENTIFIED project, bar one interview conducted with a Belgium
stakeholder.
stakeholder.

**Recruitment and data collection**

Interviews were conducted with members of civil society groups whose work is relevant to FDP
Interviews were conducted with members of civil society groups whose work is relevant to FDP
because it focuses on human rights, privacy, data protection, ethics, minority-groups, victims of
because it focuses on human rights, privacy, data protection, ethics, minority-groups, victims of
crime, or missing persons. A preliminary list of relevant civil society groups to be contacted was
crime, or missing persons. A preliminary list of relevant civil society groups to be contacted was
sourced from two main publications: *European Privacy and Human Rights 2010* by Privacy
sourced from two main publications: *European Privacy and Human Rights 2010* by Privacy
International, the Electronic Privacy Information Center, and the Center for Media and
International, the Electronic Privacy Information Center, and the Center for Media and
Communications Studies; and *Victims of crime in the EU: the extent and nature of support for
Communications Studies; and *Victims of crime in the EU: the extent and nature of support for
victims. 2014* by the European Union Agency for Fundamental Rights. These publications
victims. 2014* by the European Union Agency for Fundamental Rights. These publications
contained details of privacy-/victim support- related civil society groups in European Union
contained details of privacy-/victim support- related civil society groups in European Union
countries. Alongside this, all DEIDENTIFIED members were asked to supply a list of relevant
groups to contact within their own countries; and a snowballing methodology was used to identify
further organisations. All civil society groups were contacted three times by email, after which, if
they had not replied, they were considered non-responders. The tables below give a summary of the
number of civil society groups interviewed in each country. To maintain the confidentiality of our
participants we have not supplied details of how many different types of civil groups were
contacted in each country, though we have supplied the number of each category of civil society
group interviewed overall. These categories have been divided into (a) groups representing those
who have - or know someone who has - been a victim of crime, or has gone missing; those who are
interested in human rights and data protection issues; those who represent national ethics bodies;
and those who represent minority-groups and therefore have a particular interest in issues of
discrimination (Table 1).

A total of 30 individuals responded. Most of these individuals were interviewed on the phone or via
videolink (n=17); the rest were interviewed in person (n=1) or provided responses in writing where
language was a barrier to an audio interview (n=11). If necessary, interview schedules were
translated into relevant languages. Interviews were primarily conducted by the first author (GS; the
second author, BP, assisted when the interview was conducted in German). Most interviews were
conducted in English, and digitally recorded for transcription. Some interviewees replied to our
request for interview by supplying some of their written works which directly addressed the
interview questions (n=2).

<table>
<thead>
<tr>
<th>Country of representative individual or organisation</th>
<th>No. of organisations /individuals taking part in study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>3</td>
</tr>
<tr>
<td>Belgium</td>
<td>1</td>
</tr>
<tr>
<td>France</td>
<td>1</td>
</tr>
<tr>
<td>Germany</td>
<td>8</td>
</tr>
<tr>
<td>Poland</td>
<td>2</td>
</tr>
<tr>
<td>Spain</td>
<td>3</td>
</tr>
<tr>
<td>Sweden</td>
<td>1</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>3</td>
</tr>
<tr>
<td>UK</td>
<td>6</td>
</tr>
</tbody>
</table>
Table 1: The number of organisations which (a) were invited to take part and (b) took part in our interview study, categorised by their country of representation.

<table>
<thead>
<tr>
<th>Type of civil organisation or interest</th>
<th>No. of organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim/missing persons organisations</td>
<td>12</td>
</tr>
<tr>
<td>Human rights/data protection/digital rights/privacy</td>
<td>10</td>
</tr>
<tr>
<td>Ethics-related group</td>
<td>3</td>
</tr>
<tr>
<td>Minority-group related</td>
<td>2</td>
</tr>
<tr>
<td>Other non-profit or advisory groups</td>
<td>3</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>30</strong></td>
</tr>
</tbody>
</table>

Table 2: The number of organisations which (a) were invited to take part and (b) took part in our interview study, categorised by their interest/advocacy area.

Interviews and data analysis

The interview schedule included questions relating to the civil society organisations which the interviewees’ were associated with; interviewees’ views on age, appearance and BGA testing; any past experiences with FDP; whether their organisation would support the technology, and if so, under what circumstances; and their views on how FDP findings should be communicated, and how data should be protected. A thematic analysis of interview data was carried out using an inductive methodology. Transcripts were read and broad categories were developed from the data. These broad categories were discussed between the first and second author. The first author, GS, then conducted detailed coding of the interviews line-by-line using NVivo software to develop more intricate themes.

All interviewees were given pseudonyms so as to anonymise the transcripts. To protect confidentiality we have not provided information about our individual interviewees’ country of residence, nor their civil society group affiliation. However, where necessary to understand and contextualise our findings, we have noted relevant aggregate information about themes discussed and their relationship to different types of civil society organisations.

FINDINGS
When considering questions relating to the use of FDP during criminal investigations nearly all interviewees portrayed FDP as a technology that posed a number of risks, and that any potential usefulness of the technology in aiding criminal investigators needed to be balanced against considerations related to these risks. Five interviewees spoke about this explicitly. Interviewee 1, for example, highlighted the complexity of trying to balance this wide range of considerations when thinking about using FDP for different types of crimes:

That balance might not be the same for all crimes. ...there are quite a few questions of what are the conditions for the use of DNA forensics in property crimes...And then if you say “OK, robberies are fine, we need to catch these criminals” then you can go one step down... there must be a limit somewhere, and so this trade-up - they are not single trade-ups - I think they're also on the scale of what crime you are trying to solve. Which complexifies the problem even more (interviewee 1).

When balancing these considerations, interviewees tended to have different thresholds for finding the use of FDP acceptable. We have conceptualised these different thresholds on a balance scale, on which the various FDP-associated benefits and risks articulated by interviewees act as ‘weights’ on each of two balancers. A threshold is reached when the “expected benefits” and “risks” are balanced. Any point after this threshold, where the benefit balancer outweighs the risks, would permit the use of the technology, and vice versa. Importantly, interviewees articulated different threshold points depending on the reasons they gave to support their perspective on FDP use. These reasons were related to their underlying beliefs about the technology as well as their underlying value set and professional and personal life experiences. Some interviewees also referred to the specificities of their own national, political, and legal contexts. As interviewee 1, for example, explained, ‘reasonable balance, of course, varies from jurisdiction to jurisdiction’. Differences were also related to interviewees’ institutional and professional perspectives. For example, civil society organisations advocating data protection and privacy rights – those who had little explicit personal or close experience with serious crime, or were representatives of a minority group organisation - tended to have higher thresholds for finding the use of FDP acceptable compared to groups representing victims of crime or those who had interacted closely with law enforcement, for example in the case of missing persons; though this was not always binary, and views were more along a continuum of scale.

Below we describe and explain interviewees’ differing thresholds of FDP use in detail, and the different trades and balances they needed to make to reach the threshold which they believed, after
which, FDP use should be permitted in the criminal justice system. We do so by classifying these thresholds into three groups, ranging from high threshold (where the “risk” balancer is heavy so that a lot of “benefit” weight is needed to reach threshold), low threshold (the “risk” balancer is light, thus less “benefit” is needed to reach threshold) and middle threshold.

High threshold
For about half of the interviewees, especially representatives of civil society organisations advocating data protection, privacy and/or minority rights, FDP had many risks and potential harms because it was viewed as ‘intrusive’ or ‘invasive’. For these specific individuals, many of whom worked to protect the civil liberties of members of the public from over-surveillance by the state, concerns revolved around the potential impact on these rights when using FDP in the criminal justice system. Some of these individuals were also concerned that permitting the use of FDP for age, appearance and BGA would lead to a ‘slippery slope’ (interviewee 14) of using the technology for other more intrusive predictions, such as those related to medical conditions, which would further infringe on individual rights. Interviewee 14 explained:

*I am pretty sure that within a very few years we will have this situation where the findings of DNA phenotyping will be used in regular searches in police databases [and] that it will not be limited to appearance and age and biographical regions but also to other features [such as diabetes or some other medical problems]*

This meant that the threshold for the technology’s use in a criminal case could never, or was unlikely to ever, be reached. It was not that these individuals believed that civil rights should never be infringed upon - they also valued the need to find a perpetrator - but the potential ‘added value’ this technology could add to a criminal investigation was not enough to permit its use. Interviewee 14 continued:

*it’s a very invasive technology. And if you look at the potential added value, I mean if you weigh this in terms of a proportionality assessment, is it really necessary? I don’t see how it outweighs all the risks and problems that you have on the other side, because you need to have very good reasons to justify such an invasive measure.*

Whilst this may, on the surface, look like a balancing of privacy risk versus utility/benefit, each interviewee explained their high threshold for seeing FDP as an acceptable technology by using different justifications (or ‘balance weights’). Some interviewees reached the threshold by
balancing multiple weights: First, the financial cost of the technology factored into many interviewees’ discussions, especially given the often-limited resources of police officers. For these interviewees, the cost of FDP would prohibit its use in many criminal investigations: ‘we think it’s the matter of finance, it’s not possible for investigators, police, to use this technology in every single case, it would be too expensive’ (interviewee 12); and FDP use should only be considered after ‘weighting’ the financial cost against the perceived benefit. One interviewee spoke about the need to conduct a cost benefit analysis when considering whether to use the technology:

If we were to look at the costs of doing an additional test and the cost for the laboratory fees, and I don’t know how much additional cost it is beyond a DNA sample, but I would imagine there is some additional cost attached to that. And then the analysis costs. So there is a kind of cost benefit analysis from a criminal justice side of things in terms of whether you would want to use that type of technology (interviewee 5).

Second, many interviewees were worried about the probabilistic nature of FDP findings (‘it sounds kind of useful but...it’s not certain, so I see there are some dangers…’ (interviewee 13)). Here, interviewees raised a range of concerns related to the technology. One pertained to its practical use, given that it was seen as relatively easy to change one’s appearance (what’s the use of...[FDP]... in the investigation work....the skin colour could probably change... you can dye your hair, you can stop somehow wearing colourful contact lenses... ’ (interviewee 17)). Other respondents wondered whether the technology had been properly validated (‘I tried to find some evidence somewhere about the predictive validity of it [FDP] and the value in terms of turning a hopeless case into a successful one. And at the moment if the information is there it’s not readily available. And actually, you don’t know how valuable it’s going to be until you have actually done it’ (interviewee 5)). Some voiced concerns about the potential for over-interpretation of FDP findings (‘I think it’s dangerous, if you have a high likelihood ratio, the layman [sic] - and I consider legal professionals laymen - might have the tendency of thinking the likelihood ratio is high, chances he did it are high. Which is not the same’ (interviewee 15)), especially given ‘most people, criminal investigators too, have a very high trust in natural scientific procedures - because it’s science, it’s so reliable, and it’s always crystal clear and 100 percent’ (interviewee 10).

Concerns about the probabilistic nature of FDP findings also related to the possibility of creating ‘suspect populations’ (interviewee 5). Here, seven interviewees worried that probabilistic FDP findings, which aim to narrow down the suspect population, could open the possibility for false leads, which, in turn, could create ‘an unjustifiable number of innocent people as suspects’: the
“certain likelihood” would need to be of a high degree of certainty to avoid the risk of generating false leads and landing an unjustifiable number of innocent people as suspects (interviewee 29).

For these interviewees, the risk of infringing these innocent people’s rights also needed to be taken into account on the balance scale. At the same time, they thought, this makes the balancing process really difficult, because one can never be sure how many people’s privacy rights will be infringed: where do you find the balance because you are also throwing the…privacy rights of people who have not committed the crime and might be affected by the investigation (interviewee 1).

Interviewee 16 (Spain) believed that the probabilistic nature of FDP findings could affect the technology’s credibility if it turns out that the FDP findings actually ‘got it wrong’. This was particularly a concern for BGA testing, as so many interviewees stressed, given the social sensitivity of BGA, the risk of harm in terms of discrimination and/or stigmatisation in society (see below) would be so great, that the FDP technology should only ever be used in situations in which it was highly predictive. As interviewee 16 explains:

The racial element is so important to the respect of the dignity of persons...So this could be used from a social and political viewpoint so badly that even if the technology is properly conceived, and there is a logical sense in trying to get the resources to only focus on those that make the more likelihood, if we are wrong we will be very wrong. It is not only that we did it wrong, we are going to lose also the credibility of the technology and therefore it is bad overall. So I think that we need to be careful.

Another person, interviewee 14, pointed to EU legislation to purport this, which allows the collection and use of sensitive information, in the words of this interviewee, only “if absolutely necessary”:7 ‘and I think this is the use of DNA phenotyping for tracing biogeographic ancestry’. So, this interviewee concluded, ‘this is the last resort argument. And so then it needs to show some type of results at least with the very high probability that it will really help to solve the case’.

Finally, many interviewees stressed that whilst FDP may have the potential to narrow the pool of suspects, ‘such a method could lead to... discrimination against certain groups of people’ (interviewee 29). For example, that unconscious bias would lead police officers to interpret the FDP findings in a discriminatory way (‘I personally am generally sceptical about …the ability of law

---

7 The legislation this interviewee was referring to was Principle 2 of the Council of Europe, Committee of Ministers Recommendation R(87)15. Regulating the use of personal data in the police sector https://polis.osce.org/node/4656
enforcement agencies to use such technologies in a non-discriminatory and even-handed way’
(interviewee 29). This was perceived to be particularly problematic for BGA testing, the very value
of which was seen to rest in its ability to be able to discriminate between different societal groups:

In my view, this technology is very dangerous whose only effect is to discriminate against
minorities. As such a technology is only operational if the result of the analysis [the FDP
findings] is deviating [sic] from the appearance of the majority society, which automatically
leads to general suspicion towards minorities. Nobody benefits from this technology. I think
that in particular in our current situation of right-wing populism it is a problem and creates
more racism (interviewee 17).

Interviewees were worried that such discrimination could potentially ‘evoke certain prejudices’
given the social sensitivity of issues related to ethnicity. This was viewed as especially problematic
for those countries that had problems with racial, ethnic, and other forms of discrimination.
Interviewee 13 discusses this with relation to the situation in Austria:

if it comes to ancestry...in Austria this is very, very sensitive issue...So it could also evoke
certain prejudices against certain groups of people. So, I see there are some dangers here.

This, in turn, could ‘lead to stigmatisation and racial stereotyping’ (interviewee 30): ‘the problem
with this tool is that it points out the group of people when you belong to this ethnic minority that
you feel discriminated’ (interviewee 12). For some interviewees, this concern weighed so heavily
on the balance scale that a threshold for such phenotypic testing could never be reached.

Low thresholds of FDP use: benefits often outweigh the risks

For a small number of interviewees, especially those affiliated with victim support groups or
support groups for relatives of missing persons, protecting individuals in society from serious harm
or death was of paramount importance. For those affiliated with such support groups, they had first-
hand experience of victims of crime, as well as the personal understanding of what emotional
trauma such experiences entailed. These experiences meant that they placed the value of finding a
perpetrator higher than concerns around privacy. In fact, when discussing privacy and surveillance
concerns raised by the use of FDP in the criminal justice system, interviewee 9 remarked: ‘I just
think there are so many do-gooders out there that want to actually complain about anything that’s
about personal, technology used in a personal way’. For these interviewees, the possibility that
FDP findings could assist in a serious criminal investigation far outweighed any potential
infringement of rights:
If you ask…[our organisation] then it’s just a matter of whatever it takes to find the murderer - no restrictions should be put on the police because we are very, very worried that it’s going to happen again to somebody else (interviewee 4).

I think that anything that can help solve investigations is a good thing…we [the interviewee’s organisation] support anything [including FDP] that can help investigators resolve an investigation [so that] justice is returned to them [the victims or their families] (interviewee 21).

For these interviewees, the good of preventing crime weighed so heavily on their balance scale that it outweighed anything else. This meant that a low threshold (in terms of potential benefit of FDP findings) was required for these interviewees to support the use of FDP. In fact, for one interviewee, FDP use, similar to the use of other technologies such as CCTV surveillance, should not be understood as a ‘human rights issue’, leaving the ‘potential harm’ side of their balance scale completely un-weighted:

And we have the same argument about CCTV, Big Brother is watching you hobble down the street. Now I would have loved the French to have had CCTV to see what had actually happened [when her relative was a victim of a crime]. So yes, advances in medicine, CCTV, whatever is happening, and I just see it as a step forward not a human rights issue (interviewee 9).

Another interviewee explained that using FDP, at least to determine EVCs of a suspected perpetrator, was ‘not particularly sensitive’, and thus not ethnically problematic:

I don't see, I suppose, a problem with it ethically....it’s not particularly sensitive information of that person, it’s obvious [to the naked eye] if they are freckly or going bald. It’s just whether that would be particularly useful to the police (interviewee 2).

Some interviewees explained their ‘low threshold’ balance scale by addressing and rejecting critics’ arguments against FDP use. For example, one interviewee explained away the concern, raised by many interviewees, that using FDP findings would lead to innocent people being turned into a ‘suspected population’ (and the subsequent harms related to this). For this interviewee, because the findings from a DNA-based forensic test would never be enough to convict an individual of a
crime, or even implicate them as a suspect, the likelihood that using FDP findings could ‘implicate the innocent’ was too ‘few and far between’ to be of particular concern:

Trace DNA can be left at the crime scene and you can sneeze or something and leave your DNA there. Ultimately because of sensitivities your DNA gets picked up at a scene where you have only walked - passed - two weeks earlier and you weren't there at the time of the crime and therefore you become implicated. But there needs to be corroboration over and above the DNA profile itself for a prosecution to be safe. So I can see why some people may have a perspective that they are too intrusive and therefore too sensitive and therefore might implicate the innocent. But I think that would be few and far between (interviewee 3).

Another interviewee from the Netherlands, where FDP is explicitly permitted, concluded that societal concerns about the potential of FDP to be used for racial profiling varied according to how the issue was presented to them:

It just depends how you put it...If you start with saying “this is going to be discriminating certain people” you think “well, no, we can't do that”. But if you just see everybody has got certain markers and this it’s going to help solve a crime then everybody is happy to do it. I think discrimination is a sensitive subject but that’s what we make of it isn’t it (interviewee 4)

Finally, three of our interviewees who argued that there should be a low threshold for seeing FDP as an acceptable technology for use in case work believed that those who committed crimes had ‘fewer’ human rights than others (i.e., there was less weight on the ‘do not use’ balance): ‘once you commit a crime like that you shouldn’t be to....- you forfeit your rights to me’ (interviewee 4, the Netherlands). For other interviewees, it was also strengthened by the belief that using this technique ‘correctly’ could decrease biased behaviour by the police and gain public trust in the fact that all was being done to solve a crime (i.e., there was more weight on the ‘use FDP balance’):

All examples are serious crimes [murder, rape, armed robbery, non-armed robbery] where education to preserve citizens’ trust in enforcement of the law and to prevent repeat offenses takes precedence over data protection considerations (interviewee 20).

If it was a high statistical probability then you could actually reduce the allegations of police bias rather than increasing them. Which obviously would be a great use of the
technology….\[\ldots\] I think if used well then it would probably help the police in terms of reputation and trust in how they are conducting searches or investigations (interviewee 8).

**Middle threshold**

Most interviewees, whilst leaning towards a low threshold for the acceptability of FDP use, were also concerned about the risks attached to the technology and the potential for harm (as described in the previous section ‘High Threshold’). As such, for many of these interviewees their threshold for FDP use changed depending on the type of crime for which the technology would be used. For serious crimes, such as rape, murder, or ‘terrorism’, there was wide agreement amongst these interviewees that the ‘weight’ of potential benefit offered by FDP use in terms of helping law enforcement apprehend a suspected perpetrator who could potentially kill or rape again, was greater than any possible risk of harm instigated by the technology. Interviewee 15 emphasised this, pointing towards each country’s criminal code as a useful guidance to categorise the various types of serious and less serious crimes:

*It [FDP] is quite intrusive …I think we should reserve this for something that there is a very strong [and] legitimate interest in doing this. …it’s probably better if we focus on crimes that are more important from taking into account how the criminal codes are drafted in each of the countries. So I would think that terrorism or rapes…these kind of things...* (interviewee 16).

For less serious crimes, the possibility of future serious harm was perceived to be lower (i.e., it was not related to death or rape). Because of this, the ‘weight’ was lighter on the balance scale for ‘FDP’ use, and it was more easily outweighed by the risks related to the technology; *'I think like murder or rape, any kind of crime where there are persons as victims. So I think it would be too much to do for like a robbery or a burglary’*(interviewee 13). In some instances, however, interviewees explained that the decision to use or not use FDP in a criminal case for a less serious crime should be influenced by *'the seriousness in which its [the crime is] held by the public at large’*(interviewee 3). This added another ‘weight’ to the balance scale – the publics’ perception and beliefs. As this above interviewee described, when deciding whether to use FDP during an investigation, it is not just the seriousness of the crime which needs to be balanced against the intrusiveness of the technology, but also *public perception* of the seriousness of the crime, because even those crimes which may be deemed less serious, may still have a serious ‘community impact’: 
Murder, rape, these are givens you would say you would always use phenotyping in those categories. But there are crimes below that in terms of community impact and you might say this fits the bill because it’s the seriousness in which its held by the public at large...You can never be...black and white about it...you wouldn't want to...rule out the use of...phenotyping in a case whereby strict rules and regulations doesn’t fit [sic], but actually in terms of community impact and wider seriousness actually in that instance it would be proportionate...(interviewee 3).

CONCLUSION

In this paper we were interested in gaining an understanding of civil society stakeholder perspectives on FDP use and regulation. Our research question was: What are the views, opinions and experiences of European civil society members who have a stake in the issue of FDP regarding the use and regulation of this technology? Our findings reflected a wide variation of views regarding if, when and/or how the technology should be used in the criminal justice system which were dependent on interviewees professional and personal perspective and value sets (Table 3). To help us map this range of views, we conceptualised a balance scale, upon which the various FDP-associated benefits and risks articulated by interviewees acted as ‘weights’ on each of two balancers. When the scales were balanced a “threshold” was reached, after which FDP use was viewed as permissible.

The balance scale gives us a more “grounded”, “everyday” [74] conceptualisation of interviewees’ decision-making when considering the use of FDP in the criminal justice system. This is because, when discussing the implications of a technology we can sometimes fall into the trap of singling out only particular issues which need addressing. For example, when implementing a technology in the criminal justice system, much discussion (though not all) in the forensic science literature has focused on the need to minimise infringements on privacy [71, 75-78]. Such a model can potentially miss the consideration of other key ethical, and particularly social impacts of the technology. Our balance scale allows us to view these “other” issues through the voices of our interviewees, and also allows us to view how these issues feed into interviewees’ underlying reasons for their final perspectives about FDP use. Moreover, it also permits us to better understand how these issues interrelate as they are weighed in practice and allows us to more clearly draw out the similarities and differences across the interviewees narratives as we seek to build a fine-grained picture of how civil society stakeholders articulate the ‘ethical moment’ of FDP.
Our findings show that interviewees considered a wide range of concerns when making judgments about FDP use, and interviewees ‘weigh’ their ‘FDP balance scale’ differently, with interviewees having different thresholds for FDP use. None of our respondents held the view that FDP should be in the routine toolbox for any type of crime regardless of the severity and the nature of the investigation. Views varied between considering FDP as unacceptable altogether on one end of the scale, and considering FDP a legitimate tool for criminal investigation in the case of serious crimes when other investigative measures had not resulted in any leads at the other.

In order to obtain a better understanding of the underlying reference points of our respondents’ answers, we grouped their views into three different categories according to whether they believe that there should be a low threshold for using FDP, a medium threshold, or a high threshold (the latter including whether it should be not permissible at all). What all respondents had in common was that they balanced different benefits and risks of the technology against each other.

While our interviewees’ views and values differed in what benefits and risks they considered to weigh more heavily than others – exemplifying the plurality of perspectives often articulated for any new technology [29, 30] - none of our respondents saw this balancing act as a zero-sum game where risks to some goods and rights detract from others [79]. Instead, each risk and benefit needed to be carefully balanced against another. Such findings support Pavone and colleagues’ work, which argues that we should not think of the social impacts of security technologies in terms of trade-offs between different benefits and risks – typically between increased national security and decreased privacy rights. This is because national security must not be the only security measure considered during decision-making about a surveillance technology’s implementation and use [79]. Other security assets related to individuals and social society also need considering. For FDP, we could perceive this as a need to consider the types of issues highlighted by our interviews, in particular, people’s civil rights and liberties as well as their culture and community in terms of the possibility of undue stigma or discrimination, and individual security in terms of undue over-surveillance. As the authors state:

The introduction of security measures [for example, FDP] is to be evaluated not against the security level of the specific subset of assets it aims at protecting, but against the overall security levels of the global system of interrelated subsets of security assets. The latter includes the security of individual communications, their social interactions, and their intimacy as well as the security of intermediate actors between the state and the citizens, such as families, associations, movements, and organizations [79](p. 242)
Any ethical and socially responsible implementation of FDP into the criminal justice system in the European context needs to consider these “other assets”. And while some civil society stakeholders have higher “thresholds” for FDP use, and while the perspectives of our interviewees situated along a continuum rather than in discrete categories, we need to be attentive to all concerns.

Unfortunately, some public engagement strategies seem to serve largely for the benefit of science and scientists who need to build trust to gain public support for their research [80]. At the same time, this does not detract from the need to bring in the perspectives and values of civil society stakeholders to inform regulatory debates. Ultimately, if stakeholders purporting the benefits of FDP - including law enforcement officers and forensic scientists [3] - wish for the technology to be used within European criminal justice systems (under stipulated regulation), public trust in the technology is vital [81][p. 140], and trust can only be garnered and maintained by recognising, respecting, and addressing the concerns of civil society stakeholders. By analysing European civil society stakeholder perspectives on FDP, this paper seeks to contribute towards the inclusion of concerns and hopes of civil society stakeholders in the development of policies in this field.

Table 3. The different considerations interviewees balanced to determine the threshold for FDP use

<table>
<thead>
<tr>
<th>Reasons why interviewees thought FDP should not be used</th>
<th>Reasons why interviewees thought FDP should be used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential for discrimination</td>
<td>Ethical issues are too few and far in between to worry about</td>
</tr>
<tr>
<td>Cost of technology</td>
<td>Perpetrators have fewer human rights, so there is less need to worry about privacy/discrimination issues</td>
</tr>
<tr>
<td>Infringement on privacy rights</td>
<td>It is important that the police are seen to be using everything at their disposal to try and solve a crime</td>
</tr>
<tr>
<td>Uncertainty of findings</td>
<td>No problems issues have emerged in countries in which FDP is used</td>
</tr>
<tr>
<td>No evidence of usefulness</td>
<td></td>
</tr>
<tr>
<td>Possibility of over-interpretation of findings</td>
<td></td>
</tr>
<tr>
<td>Loss of trust in technology if predictions are wrong</td>
<td></td>
</tr>
<tr>
<td>Suspect population’s rights need to be considered</td>
<td></td>
</tr>
<tr>
<td>Potential for stigma</td>
<td></td>
</tr>
</tbody>
</table>

ACKNOWLEDGEMENTS
We thank all members of the VISAGE Consortium for their continuing support with this work; their invaluable knowledge and expertise regarding forensic DNA phenotyping; and for also helping us access research participants. We are incredibly grateful to our research participants, and thank them for the time they gave to this research project.

REFERENCES


3. Samuel, G. and B. Prainsack, *Report on challenges to the implementation of FDP in an ethical and societally responsible manner, with special emphasis on privacy and data protection*. 2019, VISAGE.


37. Toom, V., et al., Approaching ethical, legal and social issues of emerging forensic DNA phenotyping (FDP) technologies comprehensively: Reply to ‘Forensic DNA phenotyping:


Stanley, J., Forensic DNA Phenotyping American Civil Liberties Union, 2018.


Lab, L.s., Facing the Facts on DNA Phenotyping. 2015.


Augenstien, S., DNA phenotyping recreates the face of an alleged serial killer, in Forensic Magazine. 2016.
