Biometrics and Forensics Ethics Group

Notes of the 15th meeting held on 9 March 2021, via videoconference.

1 Welcome and introductions

1.1 Mark Watson-Gandy, Chair, welcomed all to the 15th meeting of the Biometrics and Forensics Ethics Group (BFEG) – see annex A for attendees and apologies.

2 Notes of the last meeting, action log and matters arising

2.1 The minutes of the December meeting had been published on the BFEG website.

2.2 A review of open actions from previous meetings can be found in annex B. All other actions were complete.

3 Chair's update

3.1 The Chair was pleased to announce that the following members of the BFEG had been reappointed for a further three-year term; Liz Campbell, Tom Sorell, Louise Amoore, Peter Waggett, Mark Jobling, Denise Syndercombe Court, and Simon Caney.

3.2 The Chair announced that following the conclusion of a period of co-option, Nina Hallowell's final term on the BFEG would conclude at this meeting. The Chair, all the members of the BFEG, the Science Secretariat and Home Office colleagues expressed thanks to Nina dedicated and valued work over ten-years on the BFEG.

3.3 The BFEG was informed that a recruitment competition for five new members of the Group was shortly to be commenced and the secretariat would circulate the details once the competition was live.

3.4 The Chair thanked the members for their work on two recent publications, the briefing note on the ethical issues arising from public-private collaboration in the use of LFR, and the update to the BFEG Ethical principles. The 2019/20 annual report was expected to be published later in March.

3.5 The Chair introduced the newly appointed Biometrics and Surveillance Camera Commissioner, Professor Sampson, who took up his post on the 1st of March.

3.6 Professor Sampson introduced himself and outlined his portfolio which would combine the posts of the Commissioner for the Retention and Use of Biometric Material and the Surveillance Camera Commissioner, although the roles would remain distinct with distinct statutory functions.

3.7 Before his appointment Professor Sampson had been on secondment to the Police, Fire and Crime Commissioner in North Yorkshire from his role as Chief Executive and solicitor to the Police and Crime Commissioner in West Yorkshire. The new

Commissioner would also continue his role as Honorary Professor and member of the Advisory Board at the Centre for Excellence in Terrorism, Resilience, Intelligence and Organised Crime at Sheffield Hallam University.

3.8 The new Commissioner took questions from the BFEG and suggested that the BFEG could draft a list of live issues that the Commissioner should be aware of.

3.9 The Chair thanked the new Commissioner and welcomed him to attend the quarterly BFEG meetings to keep the Group informed of the work in his office and utilise the knowledge and expertise on the BFEG to assist where appropriate.

4 FIND Strategy Board update,

4.1 The main points of the update from the Forensic Information Databases (FIND) Strategy Board were:

- The FINDS Fingerprint Data Assurance Strategy, which includes integrity and quality of data, was now complete and aligned to the DNA Data Assurance Strategy. The FINDS Fingerprint Data Assurance Strategy focused on monitoring sampling errors for the data loaded onto IDENT1. This would enable FINDS to provide feedback to police forces and drive improvement.
- The International DNA and Fingerprint data exchange policy had been updated and issued by FINDS. There were two key updates in the policy in relation to Prüm data sharing that had previously been shared with the BFEG which were; inclusion of sharing of suspects' (non-convicted subjects) DNA profiles, and Prüm Stage two processes once data was passed from the National Crime Agency (NCA) to police forces.
- The UK was connected and sharing live DNA data with 12 EU Member States. On average there were over 100 matches against UK crime scenes per month.
- The legislation passed for the European Union Future Relationship Act 2020 meant there were no immediate changes to the existing process in exchanging fingerprint and DNA data with EU member states.
- As a result of the EU exit the UK lost access to the Schengen Information System (SIS II), and the existing fingerprint collection held in IDENT1 for extradition fingerprints would also be deleted. The FIND Strategy Board agreed the recommendation to allow the UK International Criminality Bureau (UKICB) to adopt a manual process from January 2021 for extradition fingerprints to be uploaded to the unified policing collection in IDENT1 as an interim measure whilst an international special collection on IDENT1 could be created in order to upload and compare fingerprints.
- The replacement DNA Database, NDNAD2 went live on 23rd November 2020.

4.2 A member asked if the automatic deletion function under the Protection of Freedoms Act (PoFA) was available on the new NDNAD2 system. The FINDS representative explained deletions under PoFA were partially automated and would continue to do be so on the new NDNAD2 system, however the process was faster on the new system.

4.3 A member requested engagement with the BFEG in the development of new EU-UK DNA and fingerprint data sharing agreements with regard to Prüm and international biometrics data exchange. The BFEG could provide a wider ethical view on the proposed arrangements. The FINDS representative agreed this would be very helpful and would look into when a detailed impact analysis would be available to share with the BFEG for their views.

Action 1: FINDS to share draft UK-EU DNA and fingerprint data sharing agreement to allow BFEG to consider ethical issues in international data exchange of biometrics.

Update on Vulnerable Persons' DNA Database (VPDD) process

4.4 Following a request by the BFEG at the June 2020 meeting to update the VPDD consent form to reflect the change in process, FINDS had provided the updated consent form and VPDD policy to members for comment.

4.5 The BFEG observed that section A of the VPDD consent form was very dense and hard to read, with complex terms such as 'result derived from my sample'. The BFEG would recommend rewording the form into plain English and increasing the font size.

4.6 A proposed update to section A of the VPDD consent form had now been drafted and shared with the BFEG for comments.

4.7 Clarity was sought over inclusion of DNA profiles from vulnerable persons on the National DNA Database (NDNAD) and whether these profiles would be deleted if consent was withdrawn for inclusion on the VPDD. The FINDS representative explained the vulnerable person profile is only added to the NDNAD if the police force believes the individual may have come to harm. If the individual withdrew their consent, the police force would arrange for their profile to be removed from the NDNAD. The BFEG noted that the consent form should make it clear that if an individual withdraws their consent their profile is removed from the VPDD and the NDNAD. The FINDS representative agreed this should be added.

4.8 The FINDS representative was asked why VPDD samples were retained and reviewed every two years whilst forensic DNA samples were destroyed after six months. The FINDS representative explained that under PoFA samples taken for criminal purposes had to be destroyed after six months and this Act did not cover samples taken that were not related to offences. The FINDS representative agreed to check the reason for the two-year retention period for Vulnerable Person DNA Database samples and provide the answer for the BFEG.

Action 2: FINDS to update the BFEG on the reasons for defining a two-year retention period for Vulnerable Person DNA Database samples.

4.9 Additional comments on the consent form were provided:

- The style of language could be further improved for readability, a review of the form by an expert in readability was recommended.
- Provision of the form in other languages.
- The tone of the language and the emphasise on the donor should be reviewed, for example *then you are required to provide your consent by signing this section of the form below* should be *we are required to obtain your consent*. Vulnerable persons may be alienated by the tone used.
- More clarification of terms such as - *if deemed appropriate*, *for safeguarding measures*, *elimination purposes*, *crime stains*, *forensic investigation*, and *contamination events* was needed.
- Specific examples should be included after the statement - *the person taking my sample may be required to give evidence and/or provide a written statement to the Police in relation to the sample taken* as this may cause undue worry.
- Contact details needed to be included so that an individual could withdraw consent if they chose to. This could be the Data Protection Officer of the specific police authority.

4.10 The FINDS representative noted these suggestions and agreed inclusion of contact details was a good idea, however the precise process would depend on the police force. Guidance could be developed for police forces on what should be provided.

4.11 The BFEG highlighted that the person signing the consent form must receive a copy, not providing a copy would be unacceptable.

4.12 It was agreed any further comments on the updated consent form should be sent to the secretariat.

Action 3: Members to send secretariat comments on the updated VPDD consent form and secretariat to share comments and the DNA leaflet with FINDS

5 Home Office policy update and Custody Leaflet

5.1 The main points of the update from the policy sponsor were:

5.2 The HO were working with the College of Policing (CoP) to develop national guidance on use of live facial recognition (LFR) which would address the issues raised in the Bridges ruling. Consultation on the draft guidance would be sought in the near future and the BFEG would be consulted as part of this process.

5.3 The Home Office had also drafted changes to the Surveillance Camera Code, which would sit above the guidance from the CoP. These changes would be discussed with the new Biometrics and Surveillance Camera Commissioner (BSCC), prior to discussions with ministers.

- Together with the changes to the SCC and the guidance from the CoP Policy recognised the need for a reform of the legislation and oversight of biometrics and technology which was complex and confusing for the police and public, inconsistent across biometric types, and inflexible in responding to developing technology.

5.4 Over the coming months the Home Office would be working with policing, the Information Commissioner's Office, the Biometrics and Surveillance Camera Commissioner and the Department for Culture, Media and Sport, who lead on data protection, to consider the analysis of issues and ways to address them. The Home Office would consider public attitudes and ethical considerations and the publication of the BFEG report on LFR was seen as an important consideration of the issues to be addressed.

5.5 Policy were engaging with colleagues in the Home Office biometrics programme to progress automated deletion of custody images. An agreed approach was to be discussed with the National Police Chief's Council by May and an update would be provided to the Information Commissioner.

5.6 Pending a technical solution, a leaflet would be provided giving advice on removal of custody images. The BFEG had reviewed an earlier draft of this leaflet and comments were reflected in the new draft. Additional comments raised by BFEG members had been shared with policy colleagues.

5.7 The Policy representative was asked about technical options for automated deletion of custody images and whether this mirror the DNA process. The BFEG were informed that mirroring the requirements for DNA samples set out in the PoFA was one option being considered and the aim was consistency, however there were also technical issues to consider with retro-fitting a deletion schedule to an older database.

5.8 The BFEG were of the view that custody image retention schedules should be mapped to PoFA guidelines and not determined by technological capabilities, although these were of relevance.

5.9 The BFEG were informed that the Police, Crime, Sentencing and Courts Bill (PCSC Bill) had been introduced to Parliament on 4 March and would allow a person to be recalled for DNA, fingerprints and photographs to be taken, if not done on initial arrest.

5.10 The PCSC Bill also included clauses to create a specific, non-coercive power with appropriate safe-guards for victims and witnesses to give permission to police to extract data from their devices as part of an investigation. The Home Office worked closely with the Victims' Commissioner and Information Commissioner on these clauses. The Home Office would also produce a Code of Practise to provide guidance on the use of this power by the police and other authorities.

5.11 The BFEG were advised that the government continued to support the provision of statutory powers for the Forensic Science Regulator and that an interim regulator was in post pending confirmation of the appointment of a new regulator.

5.12 On data ethics the Home Secretary had commissioned work looking at the Home Offices' approach to data ethics and detailed work would be instigated in a number of areas over the coming weeks and months.

5.13 The BFEG were informed that Policy colleagues were meeting with the Centre for Data Ethics (CDEI) for an update on their work with Police Scotland to test the CDEI framework being developed for data analytics in policing following discussions between CDEI and senior officials at Police Scotland. Any resulting updates to the framework would be shared with the HO and the BFEG.

5.14 The Deputy Director for Data Policy in the Home Office would be meeting with the director of the CDEI to discuss their future work programme and areas of potential collaborative working, particularly around governance. Policy colleagues were also meeting with representatives from the Government Digital Strategy (GDS) for an update on their work with the GDS data ethics framework.

5.15 A Round Table discussion on the proposed West Midlands National Data Ethics Institute had been attended by a Home Office representative. The BFEG were informed that the Home Office was supportive of policing taking forward work to consider the how to address data ethics issues. A read out from the meeting was expected and there would many issues to consider, including the position of the institute. Policy would update at the next BFEG meeting.

5.16 The BFEG were advised that the College of Policing (CoP) was exploring development of data management principles and ethical implications in policing and the Home Office was engaging with the CoP on this.

5.17 Other updates were provided in a written update and included:

- Home Office Science had re-engaged in work with UK Research and Innovation (UKRI) to consider how science and technology could provide the most effective tools for police officers to prevent and detect crime.
- Potential legislation was being developed to establish a statutory framework for the extraction of data from digital devices of complainants, witnesses and others in the course of a criminal investigation or for purposes of safeguarding or supporting the investigation of death that may be investigated by a coroner. The legislation would be supported by the introduction of a code of practice.
- A series of ten studies that would "prove the principle" of work to measure the impact of forensic science on the Criminal Justice System were underway across policing and with support from academia. The studies were beginning to deliver data sets for statistical analysis.

Action 4: Members to send any comments on the Policy update or updated custody images leaflet to the secretariat.

6 Forensic Capability Network – Ethics Framework

6.1 At the March 2020 BFEG meeting the BFEG heard from the Forensics Capability Network (FCN) about the FCN Ethical Framework that, once drafted, the FCN

would like to seek feedback on from the BFEG. Following on from this the FCN Forensic Science Code of Ethics had been drafted and shared with the BFEG. The framework was presented to the group by Carolyn Lovell of the FCN.

6.2 In drafting the Code of Ethics, the FCN had carried out consultations and reviewed other, international ethical frameworks.

6.3 The FCN Code of Ethics was intended to complement the existing College of Policing Code of Ethics and had been created specifically to consider research and forensic activity.

6.4 The BFEG was advised that the FCN was also running a number of projects on data ethics and accepted that there may be some elements of cross over with the Code of Ethics, however the focus for the Code was on the professional status of the practitioners in research and forensic environments.

6.5 The BFEG identified some areas of the 'respect' section of the Code of Ethics for review:

- There was reference to researchers being able to proceed without informed consent. The BFEG advised that informed consent should always be obtained, and examples would be needed to demonstrate the circumstances under which the levels of harm resulting from not carrying out research might be considered acceptable for a researcher to proceed without consent.
- Respect for fragments of deceased people should be explicitly mentioned. The need for respect in the way material from deceased individuals was handled and treated during the activities of the forensic and research staff should be included.
- Acknowledgement of specific considerations for people with protected characteristics should be included.

6.6 The BFEG had also provided other specific comments on wording and definitions.

6.7 The representative from FINDS highlighted that the bibliography of the FCN Code of Ethics should include the FINDS policy for the use of DNA, fingerprints and biometrics in research and the FCN should ensure that the Code of Ethics was aligned with the FINDS policy.

Action 5: Members to send any additional comments on the framework to the secretariat to share with the FCN.

7 Biometrics and Digital Forensics Working Group update

7.1 The Biometrics and Digital Forensics Working Group had met to consider the ethical issues arising when a complainant, having reported a sexual offence to police, was asked to provide consent to examine a digital device, such as their phone.

7.2 The chair of the Biometrics and Digital Forensics Working Group provided the BFEG with an update on the discussions. The main points were:

- The Working Group had noted the process on obtaining consent to examine a device may differ between the 43 police forces.
- The Group also noted that if consent was obtained, then the entire contents of a device may be downloaded. This was seen by the Working Group as a deterrent for victims in reporting sexual offences crimes.
- Issues with extraction of data from digital devices had previously been raised in the report on Mobile Phone Data Extraction by the Information Commissioner and in the Appeal Court ruling of *R v Bater-James*.
- The College of Policing had produced guidance for police and a proforma for the complainant as well as a consent form.
- The Working Group had expressed concerns over whether informed consent could be provided by a complainant following a traumatic experience and wished to strengthen the process of providing consent.

7.3 The Working Group Chair outlined the initial recommendations that the group were considering.

- The complainant's device could be taken and held for a short 'cooling off' period while the complainant decided whether to give consent. The complainant would be provided with information explaining the process of examining the device to review over this period.
- Information about the examination of a digital device could be provided in a video to explain the process in simple terms.
- The complainant could also receive guidance from a support worker on the process of digital analysis and consent to examine a device.
- Special considerations should be in place for under-age children or vulnerable adults with mental health issues, where they may not fully understand what it would mean to provide their consent.
- The College of Policing guidance for the police should be expanded and include the types of scenarios where the police should not ask for consent to examine the device, for example a historic case. This would ensure the minimum level of intrusiveness.
- The consent form should clearly state when the complainant would get their device back.

7.4 In response to the initial recommendations the BFEG raised concerns over holding a complainant's phone for a cooling off period as this was likely to be their main (or only) means of contact and support. However, the BFEG was in agreement that the complainant should be provided with relevant information and given the time to make an informed decision. A follow up call by the police officer investigating the case was also recommended. The Chair of the working group responded that holding the device was proposed to avoid loss of data and would be for a short time period, however the Group would discuss this further.

7.5 It was highlighted that in older/historical cases, where it was noted that it may not be appropriate to examine the device, issues around intrusiveness may still arise as the complainant may still be living with the offender. The Working Group Chair agreed with this and commented that additional guidance was needed in this area.

7.6 It was suggested a home visit could be carried out at an agreed time by police together with a victim support officer. The digital device could then be downloaded in the complainant's presence onto a secure external drive to take back to the police station. However, it was highlighted that the home may not be a suitable or safe place to conduct the visit for all complainants.

7.7 A member noted that it was technically possible for the police to capture and encrypt data from the complainant's device onto a secure device at the time of reporting the complaint, and then return the device to the complainant. This would allow for a cooling off period without risking the loss of data. The downloaded data could be stored in encrypted state generated using a key generated by the complainant. The complainant would hold the encryption code and consent would need to be sought before the police could access the device.

7.8 It was highlighted that encryption of data did not address the issue of proportionality if it resulted in all data being downloaded. Download and encryption of data from specific apps could be considered as an alternative. The Chair of the Working Group responded that the use of specific search terms and screen shots, which had been mentioned in the *R v Bater-James* ruling, could be a way to limit the amount of information the police downloaded from the device.

7.9 The Policy lead noted that the issues raised regarding how data could be captured were being considered and an update on the discussions would be provided at the next meeting.

7.10 The BFEG also noted that the full process of the data analysis including how it would be collected, shared, analysed and used should be explained to the complainant before consent was obtained as information could be inferred from processes such as data filtering.

7.11 The Chair of the Working Group thanked the BFEG for their comments and suggestions and would discuss these with members of the Working Group.

Action 6: BDF working group to discuss issues highlighted by the BFEG around how best to allow time for a complainant to consider giving consent to allow police to download data from a digital device.

8 Data Ethics Advisory Group update

8.1 The DEAG continued to work with a team from the Law Enforcement Portfolio (LEP) on the ethical review of a proposed proof of concept study.

8.2 Following the initial meeting with the DEAG and the comments made the LEP team had updated their DEAG submission form and shared the DPIA with the group for the DEAG to review.

8.3 The proof of concept study was in its final stages of data analysis and a further meeting with the LEP team was planned for around the end of March to provide the DEAG with their findings from the trial.

9 Face Algorithm Bias Playbook update

9.1 The Chair of the Home Office Biometrics Ethics Working Group (HOB EWG) updated the BFEG on a meeting that was held to discuss the Face Algorithm Playbook.

9.2 At the BFEG December meeting, a representative from the HOB programme provided the BFEG with an overview of the Face Algorithm Bias Project. A playbook was proposed to provide practical responses to support business areas in the use of face algorithms. Volunteers were sought from the BFEG to provide comments on the first draft of the playbook and attend a meeting with the HOB representative to discuss the comments.

9.3 A meeting of the HOB sub-group was held on the 5th of March with the HOB programme Lead to discuss the group's initial comments on the draft playbook. The playbook would guide the business areas when considering using facial algorithms, from assessing requirements, through procurement, testing, implementation and performance review.

9.4 The group highlight that clarity was needed on who would use the playbook and when. The group also highlighted the possible risk of harm that could arise from false negative results generated by face algorithms in the processes they were applied to and their outcomes.

9.5 The HOB programme representative had thanked the group for their useful comments and would be working through their comments and recommendations.

9.6 A further draft of the playbook was expected to be completed in April 2021 and the HOB representative would be seeking further comments from the group. A follow up meeting with the group would be arranged once the updated draft was complete.

10 AOB

10.1 The next meeting would be held on 9th June 2021.

Annex A – List of attendees and apologies

Present – all via videoconference

- Mark Watson-Gandy - Chair
- Adil Akram - BFEG Member
- Louise Amoore - BFEG Member
- Simon Caney - BFEG Member
- Nina Hallowell - BFEG Co-optee
- Mark Jobling - BFEG Member
- Isabel Nisbet - BFEG Member
- Jennifer Temkin - BFEG Member
- Thomas Sorell - BFEG Member
- Denise Syndercombe Court - BFEG Member
- Richard Guest – BFEG Member
- Charles Raab – BFEG Member
- Julian Huppert – BFEG Member
- Nóra Ni Loideain – BFEG Member
- Peter Waggett - BFEG Member
- Andrew Thomson – FINDS Unit, HO
- Juliette Verdejo - FINDS Unit, HO
- Fraser Sampson – Biometrics and Surveillance Camera Commissioner
- Alex MacDonald – Data and Identity Unit, HO
- Carl Jennings - Data and Identity Unit, HO
- Geoff Keogh - Data and Identity Unit, HO
- Cheryl Sinclair - Data and Identity Unit, HO
- Caitlin Seymour, Data and Identity Unit, HO
- Jo Wallace, HO Science
- Nadine Roache - BFEG Secretariat, HO
- Jennifer Guest - BFEG Secretary, HO

Apologies

- Liz Campbell - BFEG Member

Annex B – review of open actions from previous meeting

March 2020

Action 3: (Complex Datasets working group to produce general guidance on ethical issues in binary classification systems). The CD WG report was shared with the Data Scientists, who confirmed they would be producing a report in response and this report would be helpful for the general guidance. Action ongoing.

Action 7: (Secretariat to make amendments to recommendations for 2019/20 annual report and share with BFEG). The Annual report was expected to be published in March 2021. Action closed.

Sept 2020

Action 2: (Update on the revised police guidance and Public Sector Equality Duty proposal with Cardiff University) – the work had been delayed by Covid-19 restrictions. Action ongoing.

Action 9: (Suggestions on virtual away day activities). Action ongoing.

December 2020

Action 2: (BFEG member to raise with relevant groups the lack of oversight of familial DNA search algorithms used by Forensic Service Providers). A report would be prepared for the Chair. Action ongoing.

Action 3: (FINDS to provide an update on efficacy and false positive matches following the introduction of the new familial DNA policy). FINDS had carried out some review work on the requirements that Forensic Service Providers (FSPs) need to meet to conduct National DNA Database (NDNAD) familial searches and would begin to consider how to assess the impact of the new policy. Action ongoing.

Action 4: (FINDS to identify the correct forum for a review the wording of section A of the DNA sample consent forms (including Vulnerable Persons' DNA Database (VPDD) consent form) and secretariat to follow up on a review of this form). The VPDD form had been updated by FINDS and provided for BFEG review (see section 4). The FCN were carrying out a review of the DNA consent forms and the secretariat had made a request for the BFEG to feed into this review. Action ongoing.

Action 6: (Comments on the draft custody images leaflet to be sent to the BFEG for collation and feedback to Policy). The leaflet was reviewed by Policy and an updated leaflet, taking on BFEG comments had been provided to policing partners for review. Additional comments from the BFEG on the update had been submitted to policy. Action complete.

Action 7: (Secretariat to publish the updated BFEG principles). The updated Ethical Principles were published on the 22nd of December. Action complete.

Action 8: (Members who would like to be involved in the Face Algorithm Playbook to contact the secretariat). A draft of the face algorithm playbook had been shared with those who had volunteered, and a meeting to discuss their comments had been held (see section 10). Action complete.

Action 9: (Secretariat to publish the FRWG briefing note on the ethical issues arising from public-private collaboration in the use of live facial recognition technology). The FRWG briefing note had been published on 21 January 2021. Action complete.