Biometrics and Forensics Ethics Group

Notes of the 13th meeting held on 23 September 2020, via videoconference.

1 Welcome and introductions

1.1 Mark Watson-Gandy, Chair, welcomed all to the 13th 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 June meeting had been agreed and submitted for publication.

2.2 March 2020 Action 1: FRWG to draft a briefing note on collaborative use of LFR. The briefing note has been shared with the BFEG and will be discussed under item 8.

2.3 March 2020 Action 3: CDWG to produce general guidance on ethical issues in binary systems. The guidance is currently pending, and work will commence once the report for The Data Analytics Competency Centre (DACC) has been completed.

2.4 March 2020 Action 4: Complex Datasets Group to share their report on the 2 use cases. The report has been shared with the BFEG prior to the meeting and will be discussed under item 9.

2.5 March 2020 Action 5: Policy to share draft of custody leaflet with the secretariat. The policy representative explained to the group a draft of the custody leaflet had been produced, and the draft would be circulated shortly.

2.6 June 2020 Action 2: Create a guide for DNA profiling for BFEG members. Members had been provided with a link to a DNA guide co-produced by one of the BFEG members, this link had been circulated to members and a copy could be provided if required.

2.7 June 2020 Action 4: FINDS to share the draft policy for the familial DNA proposal with the BFEG. The draft was in progress and would be shared at the BFEG December meeting.

3 Chair's update and Biometric Commissioner's update

3.1 The Chair presented the written update on behalf of the Biometric Commissioner. The main points were:

- The Biometric Commissioner's term had been extended until 15th December 2020.
- A recruitment campaign had been launched for a new joint Biometrics/Surveillance Camera Commissioner.
- A request had been made to extend section 24 of the Coronavirus Act by six months. This would allow the police to retain biometrics of national security interest individuals which could not be kept, for any other lawful reason

without carrying out a full risk assessment or making a National Security Determination.

3.2 A BFEG member noted that in relation to section 24 of the Coronavirus Act 2020 biometrics should only be retained in exceptional cases, and longer retention periods should be avoided where possible.

4 FIND Strategy Board, update

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

- The new IT platform for the National DNA Database (NDNAD2) was due to go live on 21st September 2020, however this had now been delayed as a result of issues identified during testing. A new go-live date would be shared once these issues were resolved.
- The UK was sharing DNA data exchanges with 10 EU Member states. In August 2020 the EU Council approved the UK's connection to Prüm fingerprints exchange, and exchanges with Germany would commence in October 2020.
- An updated policy and consent form for the collection of samples for the Vulnerable Person DNA Database would be presented to the BFEG at the December 2020 for review.

4.2 The representative from FINDS was asked about the process to approve the decision to share suspect's data with other countries under the Prüm agreement. Under the Prüm framework EU members had agreed that data from suspects may also be shared along with data from convicted individuals. The FINDS representative was asked about the process of removing a suspect's data if they were no longer a suspect in a case. The FINDS representative would follow up on this query and provide an answer for the BFEG.

Action 1: FINDS representative to provide information on the decision-making process for sharing and deleting suspect's DNA and fingerprint data with Prüm member states.

5 Home Office policy update

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

- The Court of Appeal ruled on the case of Bridges v South Wales Police (SWP). The Home Office was working with SWP, to determine what needs to be done to ensure future deployments of Live Facial Recognition (LFR), were compliant with the judgements. The police guidance would be reviewed to ensure the police could demonstrate that they were acting in accordance with the law when deploying LFR. Updating the Surveillance Camera Code of Practice was another option being considered. It was noted that meeting the Public Sector Equality Duty (PSED) requirement to test the LFR software for algorithmic bias mentioned in the judgment would be a challenge because of

social distancing rules. Proposals were being developed with Cardiff University to carry out an evaluation of bias in the LFR algorithm used by SWP.

- The Home Office would be working with policing, government departments, parliamentarians, industry, oversight and civil liberty groups and the public to address wider issues with the biometrics legal framework and provide a greater consistency, and clarity in the regime for police use of biometrics.
- The process of recruiting a new combined Biometrics and Surveillance Camera Commissioner was in progress. The statutory duties of both roles would remain the same, with two part-time roles combined into one role.
- The Centre for Data Ethics and Innovation (CEDI) algorithmic bias review publication was delayed but publication was expected in the coming month.
- A new Digital Forensics Policy Team had been recruited and would be developing a clear policy for Digital forensics that would apply to extraction, storage, and deletion across a range of crime types. The changes would take into account ethical considerations, legal requirements, operation needs and the recommendations of the Information Commissioner's report on mobile phone extraction.

5.2 The judgement by the Court of Appeal in the Bridges v SWP case was deemed helpful by the BFEG, however the judgement did not address the issues around proportionate use of LFR. It was suggested that if the Surveillance Camera Code of Practice and other policies were updated, they should consider the other arguments made in the judgment. It was suggested policy provide an update at the next BFEG meeting on the work being done in response to the judgement. This included the police revised guidance, and the PSED proposal with Cardiff University.

Action 2: Policy to provide an update at the next BFEG meeting, on the revised police guidance and PSED proposal with Cardiff University, in response to the Bridges v SWP Judgement.

5.3 Members raised concerns that combining the roles of the Biometrics and Surveillance Camera Commissioners would present challenges as the remits of the two roles were large. A policy representative responded both the Biometrics Commissioner and Surveillance Camera Commissioner had shared stakeholders, and often their work would overlap. It was confirmed the new Biometrics and Surveillance Camera Commissioner would be a full-time post and would retain the same statutory powers of the previous separate roles.

6 Data Ethics Advisory Group update

6.1 The Data Ethics Advisory Group (DEAG) and the policy lead had met virtually to discuss the approach to submission of cases to review. The DEAG had agreed a

template for submission of use-cases. The template document was described as a work in progress and would evolve with feedback from the submitting groups.

6.2 The first use-case would be from the Police Data Laboratory who were expected to submit their completed form in the coming weeks. This would be followed by a virtual meeting between the project team and the DEAG to discuss the proposal.

6.3 There was a discussion around the accountability of the advice from the DEAG and what link there would be between the DEAG and the BFEG. The Chair of the DEAG suggested that the BFEG could be kept informed of the DEAG's discussions by sharing the minutes from the group's discussions with project teams. It was noted that for the DEAG to give timely advice, comment from the BFEG would need to be provided via correspondence and within a short time frame rather than at the plenary meetings. Members noted that comment from the wider BFEG would be beneficial in terms of provision of views from different stand points and different areas of expertise. The Chair of the DEAG proposed that once the first use-case was received the submission form could be circulated to the BFEG for comment.

Action 3: Secretariat to circulate the DEAG submission from the Police Data Laboratory once received.

7 Digital Forensics Presentation

7.1 Representatives from digital forensics policy, South Wales University, and Transforming Forensics (TF) gave presentation on approaches to the collection, use, retention and deletion of extracted digital forensic material. This was to provide context for the 2020/2021 commission.

7.2 The main points from the presentation were:

- Digital Forensics was described as the process by which information was extracted from any digital system or data storage media, rendered into a usable form, processed and interpreted for use in investigations or as evidence in criminal proceedings.
- Most reported crimes had a digital element requiring police to extract data for digital devices, the rapid and sustained growth of digital evidence presents challenges to policing.
- The most common devices examined were: computers, such as for investigations of sharing indecent images; and mobile phones, such as investigations into gang activity and sexual offences.
- The police would often extract data from digital devices to carry out effective investigations. Due to the limitations of the extraction software tools used, it would extract all data from the digital device, rather than specific data, for example a video. This provided the police with access to vast amounts of highly sensitive data.
- The police must act in a way that both protects privacy of the victims and witnesses and secures justice. The data collected must be proportionate,

lawful, specific, and stored for no longer than necessary. This would give confidence in the criminal justice system.

- The Home Office would be undertaking a review of the way the police collect, use, retain, and delete digital data and during this review advice would be sought from the BFEG on the ethical considerations.
- The Digital Forensics Strategy from TF was feeding into Home Office policy development in this area.

7.3 The BFEG identified the following ethical issues that should be addressed when extracting digital data:

- Clarity over when a complainant would be asked to share a device.
    - The representative from TF stated that to seize a device there must be a firm belief that there would be evidence on a complainant's device that would assist the investigation. Digital processing notices, which were provided to complainants to seek their consent to examine their device, should not be used as a blanket approach to seizing devices.
- Clarity over what data would be recovered from a device and how that data would be related to the investigation.
    - The BFEG were informed that there were challenges with itemising the relevant data that may be present on a device, and that current methods did not allow recovery of data from a specific time frame, particularly when recovering deleted data. Consideration of how to capture data before there was knowledge of what data was there, and in what format, would be needed and it was important that this process was transparent.
- The risk of malicious upload of data and therefore the risk of injustice.
    - It was noted that there was a need for underpinning science to support identification of spoof images. It was also mentioned that when data was acquired from tables of data, if the defence raised issues or disputed the data, the tables of data would need to be looked at again.
- The need for processes to prevent bias as a result examination of irrelevant data and view forming about individuals.
    - The representative from TF noted that avoidance of bias was linked to quality standards, validation and accreditation and that transparency needed to be at the fore to support public confidence.
- Whether the current legislation was sufficient to deal with digital data.
    - The representative from TF noted that consideration of issues identified in the judgement of *R v Bater-James and Mohammed* [EWCA Crim 790, 2020] was needed.

- Whether a statutory code of practice (as suggested in the Information Commissioner's Office report on mobile phone extraction) would be appropriate.
    - The policy representative commented that the Home Office were considering all the options and were also assessing whether the current legal framework was fit for purpose. A broad input would be required and input from the BFEG would be sought as the review developed.

7.4 A working group of the BFEG had been established to provide a point of contact for this review. Technical advice was also offered from a member of the BFEG with relevant expertise. Further advice could also be sought from the representative from the University of South Wales. The next step would be for policy colleagues to meet with the working group and take forward the first elements of the review.

Action 4: Secretariat to arrange a meeting between the Digital Forensics Review Working Group and Home Office policy representatives.

8 Facial Recognition WG update and briefing note

8.1 The Facial Recognition working group (FR WG) held an evidence gathering event on the 29th of June on the collaborative use of live facial recognition technology between the police and the private sector. The group heard from representatives from: NHS digital, Counter Terrorism Policing, Southern Co-operative stores, and Liberty.

8.2 The group had subsequently met virtually to discuss their report and a draft had been circulated for comment from the BFEG. Some members had provided feedback ahead of the meeting for which the Chair of the FR WG noted her thanks.

8.3 Specific areas of the draft report were identified by the Chair of the FR WG where comment from the BFEG would be beneficial. These areas were discussed, and members were asked to send comments to the secretariat.

Action 5: Members to send comments on the draft FR WG report to the secretariat by the 7th of October.

9 Complex Datasets Working Group update

9.1 The Complex Datasets working group (CD WG) had received the final data protection impact assessments (DPIA) for the two use cases they had been reviewing. The group had met virtually to discuss the DPIAs and finalise their report.

9.2 The BFEG had been invited to read the draft report and send comments and any suggested amendments to the secretariat. Some members had provided feedback ahead of the meeting for which the Chair of the CD WG noted his thanks and suggested that further discussion of their feedback would be beneficial.

Action 6: Members to send comments on the draft CD WG report to the secretariat by the 7th of October.

Action 7: Secretariat to arrange a meeting between the Chair of the CD WG and members providing comments.

10 Proposal to update BFEG principles

10.1 A proposal for a self-commission for the BFEG had been submitted: “To consider the ethical impact of biometric technologies specifically on people with protected characteristics”. The proposal had wide support from the members of the BFEG.

10.2 In response to this proposal it had been suggested that the BFEG Ethical Principles be updated to incorporate the proposed self-commission into all of the BFEG’s work, rather than being associated with one working group or use case.

10.3 The members of the BFEG were asked to review the proposed changes to the principles and consider if further changes were needed.

10.4 One member had provided feedback ahead of the meeting for which the secretariat was very grateful, and a meeting between the member drafting the proposal and the member giving feedback was agreed to draft a final update of the principles which would then be circulated to the BFEG for comment.

Action 8: Secretariat to arrange a meeting to finalise a draft update to the BFEG principles.

11 AOB

11.1 The HOB EWG would be meeting on 9th October 2020, and an update would be provided to the BFEG at the December 2020 BFEG meeting.

11.2 The BFEG was asked for suggestions on virtual away day activities, and to send suggestions to the secretariat.

Action 9: Members to send suggestions on virtual away day activities to the secretariat.

Annex A – List of attendees and apologies

Present – all via videoconference

- Mark Watson-Gandy - Chair
- Louise Amoore - BFEG Member
- Simon Caney - BFEG Member
- Richard Guest – BFEG Member
- Nina Hallowell - BFEG Member
- Julian Huppert – BFEG Member
- Mark Jobling - BFEG Member
- Nóra Ni Loideain – BFEG Member
- Isabel Nisbet - BFEG Member
- Thomas Sorell - BFEG Member
- Denise Syndercombe Court - BFEG Member
- Jennifer Temkin - BFEG Member
- Charles Raab – BFEG Member
- Peter Waggett - BFEG Member
- Andrew Thomson – FINDS Unit, HO
- Juliette Verdejo - FINDS Unit, HO
- Rebecca Madgwick – Biometrics Commissioner's Office
- Alex MacDonald – Data and Identity Unit, HO
- Carl Jennings - Data and Identity Unit, HO
- Caitlyn Seymour - Data and Identity Unit, HO
- Cheryl Sinclair - Data and Identity Unit, HO
- Geoff Keogh - Data and Identity Unit, HO
- Dominik Steinmeir - Data and Identity Unit, HO
- Nadine Roache - BFEG Secretariat, HO
- Jennifer Guest - BFEG Secretary, HO

Apologies

- Adil Akram - BFEG Member
- Liz Campbell - BFEG Member
- Victoria Longworth - Data and Identity Unit, HO