



OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Commissioner for the Retention and Use
of Biometric Material Annual Report
April 2023 to March 2024

And

Surveillance Camera Commissioner
Annual Report April 2023 to March 2024

December 2024

Commissioner for the Retention and Use of Biometric Material Annual Report
April 2023 – March 2024

And

Surveillance Camera Commissioner Annual Report April 2023 – March 2024

Presented to Parliament pursuant to Section 21(4)(b) and Section 35(1)(b) of
the Protection of Freedoms Act 2012

December 2024



© Crown copyright 2024

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at enquiries@obscc.org.uk

ISBN 978-1-5286-5206-3

E03213131 12/24

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office



The Right Honourable Yvette Cooper MP
Secretary of State for the Home Department

Home Office
2 Marsham Street
London

10 October 2024

Dear Home Secretary

Biometrics and Surveillance Camera Commissioner Annual Report – 2023/2024

As Commissioner for the Retention and Use of Biometric Material, I am required under s21(1) of the Protection of Freedoms Act 2012 (PoFA) to make a report to you about the carrying out of the Commissioner's functions. Additionally, as the Surveillance Camera Commissioner, I am enjoined under s35(1) of PoFA to prepare a report about the exercise of my functions in that role.

I had not originally planned for this to be a formal report on the carrying out of my functions, but rather a valedictory note setting out what I had achieved in my time-limited tenure as Commissioner, together with a short reflection on the successes of my recent predecessor, Professor Fraser Sampson, who was the Commissioner for the majority of this reporting period. However, when the then Prime Minister called a General Election for 4 July, the Data Protection and Digital Information Bill fell. This meant that the abolition of my role, the closure of my office, and the transfer of biometrics casework functions to the Investigatory Powers Commissioner's Office was halted, as there was no longer a legislative vehicle to bring about those changes. This report is, therefore, much briefer than in previous years, given the extent to which the work of the office had been significantly scaled back ahead of


those anticipated changes, which were likely to have come into effect in summer 2024.

Notwithstanding that, it has been a privilege to have followed in the footsteps of my predecessors, and I am grateful for the opportunity to have contributed to the important work of my office.

Much of my focus during my time in post had been on ensuring a smooth transition of the biometrics functions to the Investigatory Powers Commissioner's Office, and in developing an exit and continuity strategy that would have enabled both the orderly closure of my office and the continuance of key functions on behalf of communities and stakeholders. I am particularly grateful for the work of Sir Brian Levison and his team, all of whom were committed to ensuring a seamless transition of statutory functions to IPCO. I would also like to recognise the professionalism of Home Office officials who were overseeing the changes that the DPDI Bill was intended to deliver.

As with previous reports, I do not believe that this annual report contains any material which might need to be excised in the public interest or for reasons of national security.

Yours sincerely

A handwritten signature in black ink, appearing to read 'A. Eastaugh', is written on a light yellow rectangular background.

Tony Eastaugh CBE

Commissioner for the Retention and Use of Biometric Material and Surveillance
Camera Commissioner (December 2023 to August 2024)

Contents

Executive Summary	5
Part 1 – Building on the past and working towards closing the office	9
A potted history.....	9
Activities to ensure closure of the office.....	11
Part 2 – Biometrics	14
Chapter 1 – Retention of biometrics for national security purposes: National Security Determinations (NSD).....	14
Utility	14
Legislative changes.....	15
NSD Decisions	16
Chapter 2 – Section 63Gs	18
Applications to retain DNA and fingerprints.....	18
Preliminary applications	22
UZ Marker reviews	23
Chapter 3 – International Exchange	24
Chapter 4 – Compliance, Retention, Use and Destruction	24
Custody images	24
Compliance visits	25
Voluntary attendance	25
CPIA Exception.....	25
Part 3 – Public Space Surveillance	27
Part 4 – Reflections and Conclusion	30
Reflections.....	30

Executive Summary

I have not reported on some of the statistics that have previously featured in the annual report, as they can be found elsewhere. Similarly, my office had negotiated the continued reporting of other data that the Biometrics Commissioner alone published, to ensure continued transparency when the requirement for the Commissioner to report annually ceased. As the future of the office and its function, at the time of writing, is still being considered by government, I have maintained this position.

Part 1 – Building on the past and working towards closing the office

The past

- Predecessors in the roles of both Biometrics and Surveillance Camera Commissioners have made significant contributions in both arenas.
- This includes contributing to the case of *Bridges v South Wales Police*, and issuing comprehensive guidance in the light of that case, *Facing the Camera*.
- Other developments included launching the Secure by Default certification scheme, the Surveillance Camera Commissioner's Buyer's Toolkit, and the Passport to Compliance.
- Most recently, the previous Commissioner was at the forefront of the endeavour to confront security and ethical issues in the use of surveillance camera technology, achieving positive outcomes through extensive engagement with Ministers, officials, law enforcement, civil society groups, academics, and the media. This culminated in the Cabinet Office Minister instructing departments to cease the deployment of surveillance systems manufactured by companies subject to the National Intelligence Law of the People's Republic of China.
- Regular surveys with police and local authorities on the use of surveillance camera technologies have provided further evidence of the need for precision in regulations to sustain the use of this technology by relevant authorities.

Closure of the office

- To ensure an orderly closure of the office in anticipation of the passing of the Data Protection and Digital Information Bill (DPDI Bill, or the Bill), the

Commissioner ended the Surveillance Camera Strategy. Similarly, both of the Commissioner's two certification schemes, which were linked to the Surveillance Camera Code, were effectively closed down with the Third Party scheme's closure linked to what would have been Royal Assent of the Bill.

- Proper arrangements were made to establish appropriate representation on the various boards on which the Commissioner sat.
- The office worked with both the Home Office and the Investigatory Powers Commissioner's Office (IPCO) to ensure transfer of all biometrics casework functions to the latter.

Part 2 – Biometrics

Chapter 1 – Retention of biometrics for national security purposes

- The ability of chief officers to make National Security Determinations (NSDs) to retain the biometrics of those assessed to present a risk to national security is a vital tool. However, as also noted by previous Commissioners, there remain significant issues with the IT used to record and keep NSDs under review.
- Further, it remains impossible to obtain certain information to allow the Commissioner to fully discharge his statutory obligations and to obtain and publish statistics for transparency.
- In whatever guise there continues to be a process of reviewing NSDs, there needs to be investment in the IT system that supports that process and assists in proper audit and accountability.
- As noted in last year's report, the legislation surrounding the making of NSDs does not require a Determination to be cancelled where retention under the NSD is no longer necessary. The risks around this need to be addressed by the Home Office.
- During the reporting period there were 266 NSDs made by chief officers, of which 227 were agreed by the Commissioner. The number of occasions on which chief officers declined an NSD was around 10%, which is about half of the figure for last year. Further, the Commissioner challenged or sought further information in approximately 20% of cases in the reporting period. This is about half of the number of challenges in the last report and,

notwithstanding some issues identified with the paucity of some chief officers' comments, it would tend to suggest that the quality of the applications is continuing to improve, and that there is more intelligence available on which the Commissioner can make a balanced decision.

- The number of cases in which biometric data was lost (administrative error or cases not progressed within the statutory time limit) has also reduced, albeit in a shorter reporting period.

Chapter 2 – Section 63G

- In May 2024 the office hosted an online workshop, with assistance from the Metropolitan Police Service (MPS) and Leicestershire Police, to encourage greater use of the s63G process and improve applications. Nearly 100 participants from 17 police forces attended.
- In the reporting period 149 applications were made, which was 9 more than the last period which was 3 months longer. Although the MPS continue to contribute over half of all applications, the increase in number and spread of those applications would indicate that the value of the process is gaining greater traction across forces.

Chapter 3 – International Exchange

- The anticipated closure of the office, together with resource limitations meant that no dip samples were undertaken during the reporting period.

Chapter 4 – Retention

- Again, in anticipated closure of the office, no police visits were undertaken in the reporting year.
- No progress has been made around the challenges of voluntary attendance and the opportunities to capture biometrics. This has been raised with the Home Office.

Part 3 – The future and public space surveillance

- The use of facial recognition technology remains contentious. There remain potential regulatory and policy deficiencies in its widespread roll out. There are also continued question marks about the accuracy of the technology.

Government and officials must continue to engage with stakeholders and civil liberties groups on the issues.

- Huge data sets are being generated, such as by Automatic Number Plate Recognition (ANPR), that are potentially being used in a way not originally envisaged.
- Growth and expansion in the range of new biometric data sets needs to be a focus for government policy; it must be allied to proper accountability.
- A lack of specific guidance can inhibit planning and investment in new and emerging technologies.
- The role of the Office of the Biometrics and Surveillance Camera Commissioner (OBSCC) in relation to the future regulation and oversight of biometrics and surveillance cameras must be clearly defined and agreed. Accountability and governance of this critical area of work should remain a government priority.
- To gain public trust and confidence there needs to be more transparency about how technology is deployed. Increased stakeholder and public engagement is critical.

Part 4 – Reflections and conclusion

- Despite the importance of the work of the office it has proved very difficult to win interest within Whitehall for that work.
- Should OBSCC continue in its current form then it needs to be fully staffed and appropriately funded to carry out its functions.
- Consideration should be given to how the office fits within the larger regulatory functions that overlap with Artificial Intelligence (AI).
- Greater certainty in the shape of regulation needs to be provided in those areas currently lacking it, including facial recognition, use of AI, new and emerging biometrics, and the retention of biometrics beyond fingerprints and DNA.

Part 1 – Building on the past and working towards closing the office

1. At the time of writing the long term future of my office is still being considered. Therefore, I would like to reflect and comment on some of the achievements of the two offices and of my most recent predecessors.

A potted history

2. Prior to March 2021 when my immediate predecessor was appointed to both roles, the Biometrics Commissioner and Surveillance Camera Commissioner's roles were held by two separate Commissioners. Mr Tony Porter served as the Surveillance Camera Commissioner from 2014 until 2020, and was a key contributor in the case of Bridges v South Wales Police in which the High Court initially ruled against Mr Bridges' claim against the unlawful use of automated facial recognition, before the Court of Appeal ruled in favour of three of the five contested grounds. The Court recommended an update to the Surveillance Camera Code of Practice to provide greater rigour around who is on a watchlist and where this technology can be deployed and, whilst other guidance is in place, the updated Code still remains the only statutory guidance on facial recognition. This set clear parameters as to use, regulation and legal oversight. Following the case, he issued comprehensive guidance, Facing the Camera, which provided a roadmap to police forces through the complex terrain of how to legitimately use live facial recognition technology in accordance with the legal framework where its use is integral to a surveillance camera system being operated in live or near live time operational scenarios. In 2019, Mr Porter launched the Secure by Default certification scheme, which included guidance on self-certification for manufacturers of video surveillance camera systems, which ran until its official closure in 2023. His contributions included the development of the Surveillance Camera Commissioner's Buyer's toolkit, the Passport to Compliance, a self-assessment tool for organisations and a data protection impact assessment for surveillance cameras.
3. Professor Paul Wiles was appointed as Biometrics Commissioner in June 2016 and held the position until 2021. Throughout his tenure he brought about

necessary awareness to technological advances that involved the retention of biometrics and how they are used in the public sector and private sector, and raised concerns a number of times around police use of new biometrics that are not covered by the governance arrangements created by PoFA. A number of these issues remain unaddressed, particularly those linked to the potential uses of artificial intelligence in law enforcement.

4. The two Commissioner roles (Biometrics, and separately, Surveillance Cameras) were brought together under Professor Fraser Sampson in March 2021. Professor Sampson was a vocal advocate for the responsible use of facial matching and other emerging biometrics by the police. He focused on evolving technology throughout his tenure as the Biometrics and Surveillance Camera Commissioner. Professor Sampson spearheaded the endeavour to confront security and ethical issues in the use of surveillance camera technology, accumulating significant positive developments through active engagement with Ministers, chief police officers, police and crime commissioners, local authorities, civil society groups, academics, and the international news media. His actions highlighting the links between the use of surveillance camera technology to human rights abuses and fundamental concerns about the security of the technology culminated in the Cabinet Office Minister instructing departments to cease deployment of surveillance systems manufactured by companies subject to the National Intelligence Law of the People's Republic of China¹. His influence paved the way for the National Police Chiefs' Council to adopt an ethical procurement position when considering the trading history of surveillance partners.
5. During his tenure Professor Sampson carried out three major surveys: two with the police and local authorities on the use of surveillance camera technologies, and one on drones. They aimed to capture the extent of technology deployment, and compliance with statutory obligations under the Protection of Freedoms Act and Surveillance Camera Code of Practice. These findings revealed a general lack of awareness within those organisations of what technology is held and its capabilities, provided further evidence of the need for precision in regulations to sustain the use of this technology by

¹ <https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386>

relevant authorities, and highlighted the need for due diligence in the procurement process.

Activities to ensure closure of the office

6. Notwithstanding the fall of the DPDI Bill, I wanted to comment on the work and activities that were undertaken to ensure the orderly closure of my office and transition of my statutory functions during the reporting period up to 31st March 2024. I have set these out because they were an important part of my tenure.
7. My immediate predecessor advised the strand leads of the previously established Surveillance Camera Strategy that the strategy would effectively end at the closure of my office. Options and mitigations were discussed with strategy leads who, I want to add, have acted diligently and professionally in their roles despite being volunteers. At the time of writing, and given that the future role of OBSCC remains to be defined, those discussions remain paused.
8. My office had run two certification schemes: a Secure by Default scheme (effectively self-certification) and a third-party scheme involving independent accreditors. Both of these schemes were linked to the Surveillance Camera Code that would have been effectively ended by the DPDI Bill. Consequently, both schemes have been closed. However, there remained the prospect of other third-party providers stepping in to provide similar certification using the *principles* of the Surveillance Camera Code but not the Code itself. Given these were schemes the Surveillance Camera Commissioner established, no other government department or agency would have adopted oversight against a Code that would no longer exist. Going forward, consideration could be given to the resurrection of such schemes, although this should be linked to the future strategy relating to the role of OBSCC.
9. The potential risks arising from the loss of the Surveillance Camera Code have been articulated elsewhere by my predecessor and within the independent Gap Analysis² that he commissioned. However, I had reached

² <https://www.gov.uk/government/publications/changes-to-the-functions-of-the-bscc-independent-report>

- out to other agencies, to see whether ownership of the principles of the Code could be adopted by another party to ensure consistency of operations within, for example, law enforcement. This remains without conclusion and therefore a potential risk in relation to promulgating best practice.
10. Arguably, the Code is one of the few documents that addresses the use of facial recognition technology. I believe that clearer regulation of how facial recognition is used to protect the public will become more critical as that use expands and grows. While some elements of the Code do cross over with data protection matters (or arguably duplicate them), my discussions with other regulators suggests that there could be a narrower approach to this subject that may exclusively focus on data protection issues. This may present a risk that will need addressing by policy and regulator colleagues.
 11. One of the unique advantages of my office is that it acts as a central interface with the public and interested parties for both biometrics and surveillance cameras. My engagement with the public, stakeholders, suppliers, other regulators, and government officials confirms that this role is highly valued by all who engage with my team. When deciding on the future role and function of OBSCC, consideration should be given as to how these key interface and conduit roles will be maintained and upheld.
 12. My office carries out two key biennial surveys: examination of open space surveillance, including the use of drones, by police forces and by local authorities. These are valuable exercises in assessing how both sets of agencies/bodies use some surveillance tools, the extent to which they carry out due diligence in acquiring such tools, and inform assurance about oversight of use. The future of these biennial surveys is unclear.
 13. I am satisfied that I have made proper arrangements for there to be representation on the numerous boards on which I sit including the National Security Biometrics Board. Additionally, I have ensured that officials have been fully apprised of all my stakeholder arrangements and I reflect further on that below.
 14. I had put in place, with the invaluable assistance of IPCO and Home Office, all the mechanisms needed to ensure that the biometrics casework functions as set out in the legislation would have been transferred in a timely and efficient manner at the closure of my office. These included transfer of all relevant

staff, casework, and IT needed for the purposes of National Security Determinations. Similarly, training of Judicial Commissioners within IPCO was in hand. It remains undecided as to what visits IPCO could have undertaken to police forces as an adjunct to their own inspection programme, as this activity was not catered for within the legislation. However, in advance of IPCO adopting the biometric casework my office had undertaken further training of police forces, which was also attended by IPCO. This transfer of casework had also been underpinned by the drafting of transitional regulations that would have ensured that there would be a clear delineation between casework completed by my office and that started under the responsibility of IPCO.

15. There would have no longer been a mechanism by which oversight of biometrics and surveillance cameras, as carried out by me, could have reported to Parliament. However, in this report I have set out data for biometrics designed to fit within the annual reporting (calendar year) cycle of IPCO, in the event that they would report such in future.

Part 2 – Biometrics

16. I do not intend to comment on the legislative backdrop to the police's retention and use of biometrics, or the decision-making powers of the Biometrics Commissioner. Nor will I draw attention to the other independent oversight of police use of biometrics that exists at the time of writing. Instead, I would direct the reader to my predecessors' annual reports to find that detail.

Chapter 1 – Retention of biometrics for national security purposes: National Security Determinations (NSD)

Utility

17. In the short period during which I have been considering chief officers' rationales in making National Security Determinations in order to retain the biometrics of individuals assessed to present a real risk to national security, it is clear what a vital tool this is.
18. As previously reported by my predecessors, however, there remain significant issues with the IT used to record and keep under review NSDs, and on which I record my agreement (or otherwise) to the retention of the relevant biometrics. And it is frustrating that I echo all the sentiments previously expressed around software failings resulting in inaccurate records, such as the period for which biometrics are to be retained, and the legislation under which it is retained.
19. It continues to be impossible to obtain certain information which would allow me to fully discharge my statutory obligation of keeping under review the use to which material retained under an NSD is being put, and of obtaining statistics to ensure transparency: for certain NSD data (see table 1 below), it is not possible for statistics to be extracted for a set period on any date other than the final day of the period. Therefore, it has not been possible to include statistics to what would ordinarily have been the end of the reporting period (31 March 2024), as I did not pivot to a full report until after the general election was called on 24 May.
20. Like my predecessors, I have raised this with CT Command, and it is fair to say that all of us who use the application as part of our role acknowledge its

shortcomings. I have heard no further updates on the much-anticipated software upgrade that has previously been reported, but can only echo what has gone before on its necessity to ensure accurate recording of legally binding decisions taken covertly.

21. I have also discussed with CT Command their intention to establish a cadre of chief officers to professionalise the consideration of National Security Determinations. I am in full support of this proposal: during my time reviewing chief officers' decisions, I have witnessed a regression in the content and quality of some of their comments. Some of this stems from a high turnover of chief officers. However, the variation in standards, attention to detail and overall thoughtfulness between 'the best' and 'the rest' has become starker. I understand there are some challenges around agreeing just who will form that cadre and, while the OBSCC team will continue to provide any support necessary to make the cadre happen, its future existence is entirely within the gift of CT policing as a collective. There is a need to agree a way to resolve those challenges.

Legislative changes

22. Provisions in the DPDI Bill that would have made the changes previously reported (paragraph 19 of 2021/22 report) also fell. I am hopeful that these are taken forward by government to bring retention for national security purposes in line with existing legislation, to ensure the retention of biometrics of those seeking to do harm to the UK.

23. In carrying out my NSD functions, I have noted that the relevant legislation surrounding the making of NSDs does not require a Determination to be cancelled where retention under the NSD is no longer necessary. And while the national guidance requires that chief officers keep NSDs under review to ensure retention remains both necessary and proportionate, the software does not allow for cancellation. For example, where the subject has been convicted of a recordable offence. Operational colleagues have raised this with my office as a risk of legal challenge, and will be taking this forward with Home Office policy officials to understand whether greater certainty can be achieved through a policy decision, or whether amendments to legislation are required.

NSD Decisions

Table 1: NSD decisions

Source: SO15

		2020	2021/2022*	2022/2023**	2023***
NSDs made by Chief Officer	New	197	443	371	221
	Renewals	209	392	76	45
	Total	406	835	447	266
NSDs declined by Chief Officer	New	6	35	73	18
	Renewals	5	22	14	10
	Total	11	57	87	28
NSDs supported by the Commissioner		155	927	438	227
NSDs challenged or further information sought		85	226	201	58
Destruction ordered by Commissioner		0	3	Not available	0

NB: some NSDs considered in a year may have been submitted the previous year

*01 January 2021 to 31 March 2022

** 01 April 2022 to 31 March 2023

***01 April to 31 December 2023

Table 2: Matches with NSD retained material

Source: SOFS

Type of biometric match	Number of matches			
	2020	01 Jan 2021 to 31 March 2022	01 April 2022 to 31 March 2023	Reporting period*
Fingerprint crime stain to tenprints	4	2	2	1
Tenprints (arrestee/Sch 7, etc) to tenprints	48	112	142	123
DNA crime scene stain to DNA reference profile	0	2	Not available	0
DNA reference profile to DNA reference profile	11	87	Not available	80
DNA arrestee to DNA reference profile	6	24	Not available	22

*01 April 2023 to 31 December 2023 for fingerprints, 01 April 2023 to 29 February 2024 for DNA

Table 3: Losses of biometric material of potential CT interest

Source: SO15

Reason for loss of biometric data	Number of losses of biometric data			
	2020	01 Jan 2021 to 31 Mar 2022	01 Apr 2022 to 31 Mar 2023	01 April to 31 December 2023
Administrative error by SO15/SOFS	1	1	11	1
Case not reviewed by Chief Officer within statutory time limit	0	0	1	0
Case not progressed within statutory time limit	0	0	5	3

24. During this reporting period, SO15 report that biometrics have been automatically deleted in 41 cases as a consequence of the POFA system being unable to recognise that the retention period initially given by the chief

officer has been reduced following a challenge by the BSCC. The failings of the software used to make NSDs has repeatedly been raised by my predecessors in their annual reports. I make the same point in this report. I understand that SO15 have raised this matter with relevant colleagues, and is thus further evidence to support the necessity of an urgent upgrade to the system.

Table 4: Holdings of biometric material on the CT databases

Source: SOFS

		2020	2021/22*	2022/2023	Reporting period**
DNA	DNA	9747	10301	11206	11605
	Of which unconvicted	2143 (22%)	2220 (21.6%)	2566 (22.9%)	2792 (24.1%)
Fingerprints	Fingerprints	11833	12839	13268	14224
	Of which unconvicted	1939 (16%)	2309 (17.9%)	2388 (18%)	3094 (21.7%)
Totals	Total holdings of material	21580	23140	24474	25829
	Of which unconvicted	4082 (19%)	4524 (19.6%)	4697 (19.2%)	5886 (22.8%)
	Individuals on databases	12676	13537	13968	15094
	Of which unconvicted	2099 (17%)	2442 (18%)	2521 (18%)	3304 (21.9%)

*Fingerprint data covers period 01 January 2021 to 31 March 2022, and DNA 01 January 2021 to 01 August 2022

**01 April 2023 to 31 December 2023 for fingerprints, 01 April 2023 to 29 February 2024 for DNA

Chapter 2 – Section 63G

Applications to retain fingerprints and DNA profiles

25. More forces are now using this legislation to better protect communities and vulnerable people. My office continues to have very good working relationships with forces, with a consistent focus on ensuring that the content and quality of applications are to the required standard. Forces receive a quarterly update from my office which shares best practice and highlights

how applications can be improved. Officers are also encouraged to contact my office should they require support with the application process, and where necessary, they can be directed to another force for support. My team and I are grateful to the Metropolitan Police Service, as they have been particularly collegiate and helpful in providing assistance to other forces with the s63G application process through sharing best practice and sample documentation.

26. In May 2024, my office hosted an online workshop, primarily covering the s63G application process. This was aimed at supporting users of the process, and encouraging new forces to consider use of the legislation as part of their service to victims. The workshop was co-hosted with support from the MPS and Leicestershire Police, who were able to give their perspectives on the process and provide advice to other forces on all aspects of utilising this power. It was positive to see nearly 100 participants joining from 17 forces across England and Wales, as well as colleagues from the Home Office and IPCO. The team remains committed to organising smaller, more bespoke sessions in the future on specific aspects of the process, based on the positive feedback they received from attendees.
27. In the past few months, I have noticed an increase in the number of s63G applications made to me where the subject has had multiple previous contacts with the police (in some cases, in excess of 30), none of which have resulted in convictions. Many of these cases involve domestic violence or gang-related activity, and my office is working with Home Office policy officials to provide evidence to support their work on violence against women and girls, and on other key manifesto commitments.
28. In this reporting period (April to December 2023), 149 applications were made under s63G. As in previous years, the MPS is the biggest user of the s63G provisions, and I am encouraged to see applications from forces who had previously made none or very few. Table 5 below shows the number of applications made by forces this year and compares that figure with the number made since the provisions came into force in October 2013.

Table 5: Number of s63G applications to the Commissioner by force

Force	App's received April 2023 to Dec 2023	Total app's since 31 October 2013	Force	App's received April 2023 to Dec 2023	Total app's since 31 October 2013
Avon & Somerset	0	10	Leicestershire	4	6
Bedfordshire	2	11	Lincolnshire	0	1
Cambridgeshire	1	17	MPS	105	663
Cleveland	4	16	Norfolk	0	1
Cumbria	0	2	North Wales	0	4
Derbyshire	0	1	North Yorkshire	4	9
Devon & Cornwall	3	40	Northamptonshire	3	5
Dorset	0	9	Northumbria	0	24
Durham	0	5	Nottinghamshire	0	2
Essex	2	51	South Wales	1	34
Gloucestershire	0	5	South Yorkshire	8	27
Greater Manchester	0	3	Suffolk*	2	2
Gwent	0	5	Thames Valley	3	37
Hampshire	0	10	Warwickshire	0	7
Hertfordshire	3	16	West Mercia	0	6
Humberside	3	28	West Yorkshire	1	95
Kent	0	31	Wiltshire	0	3
			Total	149	1186

*Suffolk Police submitted their first s63G applications during this reporting period.

Table 6: Statutory basis for s63G applications to the Commissioner (31 October 2013 to 31 December 2023)

Victim criteria	Applications received	Approved	Refused
under 18	465	320	134
vulnerable	73	57	12
associated with subject of the application	222	152	66
Prevention/detention of crime	447	328	98

(The figures above include applications that may have been withdrawn or were invalid. Also, applications were previously counted more than once when more than one category applied.)

Table 7: S63G applications to the Commissioner since provisions came into force

Year	Number of s63G applications submitted	Approved	Refused	Withdrawn
2013	1	0	0	1
2014	126	91	18	17
2015	123	78	29	16
2016	136	77	48	11
2017	108	71	23	14
2018	76	53	18	5
2019	65	52	10	3
2020	113	78	29	6
2021	117	95	18	4
2022	127	112	6	9
2023	195	180	9	6

Table 8: Outcome of applications to the Commissioner to retain biometrics for qualifying offences under s63G (31 October 2013 to 31 December 2023)

Offence Group	Total applications	Approved	Refused	Withdrawn
Murder, Attempts and Threats to Kill	32	23	9	1
Sexual Crimes	592	391	146	47
Assaults	270	225	23	19
Robbery	166	138	15	11
Burglary	97	78	14	5
Other	29	23	1	5
Total	1186	878	208	88

(NB: In previous years, some applications were double counted, where the application was reliant on more than one offence.)

Subject challenges to police applications

29. The subject of s63G applications (or their appropriate adult if applicable) can submit representations to challenge the s63G application that has been

made. They are informed about this process at the time when the police submit the application to my office, and have 28 days to make a representation. For this reporting period only nine representations were made.

30. The process of submitting representations against retention is voluntary, but it continues to be of concern that very few are submitted compared to applications made (6%).

Table 9: Representations by subjects and outcomes

	01 Jan 2018 to 31 Dec 2018	01 Jan 2019 to 31 Dec 2019	01 Jan 2020 to 31 Dec 2020	01 Jan 2021 to 31 Mar 2022	01 Apr 2022 to 31 March 2023	01 Apr 2023 to 31 Dec 2023
Total applications received	76	65	113	150	140	149
Representations from subjects	8 (10.5%)	4 (6%)	9 (8%)	8 (5%)	6 (4%)	9 (6%)

Preliminary applications

31. A preliminary application can be made if a chief officer has concerns about disclosing certain information to the subject of the application, for example intelligence about live criminal activity or sensitive witness statements. The force can discuss with my office whether the information can be withheld from the subject before they formally submit the application.

32. From 1 April 2023 to 31 December 2023, 10 preliminary applications were submitted to the office, of which the withholding of certain information from the subject was approved by myself or my predecessor in eight instances. In the two instances where they were not approved, the information the forces wanted to withhold from the subject related to previous allegations those subjects were not aware of, therefore unfairly prejudicing the subjects' ability to make meaningful representations against retention, as envisaged by PoFA. Such circumstances would arguably be challengeable by Judicial Review, particularly given the Strasbourg jurisprudence on police record keeping. The forces went ahead with the applications, submitting an amended s63G application with the previous allegations omitted.

UZ Marker reviews

33. Police forces are able to place a 'marker' (UZ marker) on the Police National Computer (PNC) profile of an arrestee if they intend to make a section 63G application to the OBSCC for the retention of their biometrics. If no UZ marker is added to the PNC, the DNA profile and fingerprints are automatically deleted 14 days after the No Further Action (NFA) date, so the UZ marker ensures against that deletion until the Commissioner has made a decision on the s63G application.
34. The UZ marker remains live on PNC until a decision has been reached: if the application is approved, the marker remains in place for three years from the date the biometrics were taken. If the application is refused, the marker must be removed immediately, triggering an immediate deletion of that biometric data.
35. I monitor the number of UZ markers in use and check the data provided against my own records of applications made to me, and ACRO provide monthly reports on the number of markers in place.
36. Analysis for this reporting period shows that forces have mostly been applying the UZ marker correctly and have been removing the marker promptly when the 3-year retention period expires or when an application for retention is refused. The most common issue encountered by my office is where forces place UZ markers against 'potential applications' but do not subsequently submit those applications, and neglect to remove the marker, or erroneously place a marker on biometrics to indicate a successful s63G application has been made, meaning biometrics are retained with no lawful basis. This tends to happen in forces that submit fewer s63G applications, and are perhaps not as familiar with all the processes.
37. Following review, my team contacts forces and request that corrections are made to the UZ markers, and I am grateful for the prompt resolution from most forces when this is required. I would encourage all forces to deal with these requests from my office in a timely manner to ensure the lawful retention of individuals' biometrics.

Chapter 3 – International Exchange

38. As with previous years, uncertainty around the future of the office and consequent resource limitations have meant my predecessor and I have not undertaken any dip samples. Whether this activity is taken forward in the future and by whom will be dependent on decisions made by ministers on the future shape of biometrics oversight.
39. Similarly, my predecessor had notified the Prüm Delivery Board of the need to ensure the continued reporting of Prüm exchange statistics once the office closed. As such, I took the decision not to include those statistics in this closing report and, for reasons set out elsewhere in this report, I did not reverse that decision when the DPDI Bill fell.
40. There is an existing requirement in the Home Office's International DNA and Fingerprint Exchange policy document for the UK³ to notify my office of any concurrent international exchanges of DNA profile and demographic data. Whilst no such notifications were made between 1 April 2023 and 31 March 2024, one instance was reported to me in June this year.

Chapter 4 – Compliance, Retention, Use and Destruction

Custody images

41. As previously reported in the 2021/2022 annual report, the retention and use of the photographs taken of every person arrested and taken into custody (custody images) remains of significant interest to me. Whilst not strictly a biometric for which I am required to provide oversight, it is nonetheless a concern that forces continue to retain and use images of people who, while having been arrested, have never subsequently been charged or summonsed. The use of these custody images of unconvicted individuals may include for facial recognition purposes.
42. However, I am grateful that work is underway within policing looking at ways to manage the retention of custody images to ensure these are lawful, proportionate and consistently applied, and my office is fully engaged with this work and will continue to support it.

³ Para 2.1.2

Compliance visits

43. Managing the closure of the office and reducing staff headcount necessitated a continued scaling back of efforts to match the resource to demand. As a consequence no police visits have been conducted in this reporting period.

Voluntary attendance

44. Voluntary attendance issues around lost opportunities to capture biometrics persist, having been discussed at some length in previous annual reports. I have raised the issue with senior officials in the Home Office and continue to press for a decision on their next steps.

CPIA Exception

45. In some exceptional cases, retention of DNA samples is required until a criminal investigation and allied disclosure arrangements are concluded, and a force may retain it under PACE s63E (CPIA exception⁴). Previously the Forensic Information Database Service (FINDS) collated returns from forces and passed the figures to the OSBCC to monitor and report in the Commissioner's annual report. However as part of preparations for the closure of the office, I confirmed that my office would cease to monitor and report use of the CPIA exception by police forces to retain DNA samples, and wrote to both the Chair of FINDS and the Head of FINDS in January 2024 to formally hand over its monitoring and reporting.

46. I report in the table below statistics for the period 1 April to 31 December 2023, which are broken down into two categories: those held by forces, and those held on behalf of forces by Forensic Service Providers (FSP). Figures for the previous reporting period are included for comparison purposes and show an overall increase in arrestee/PACE samples and an overall decrease in elimination samples retained under the CPIA exception: the total number of arrestee/PACE samples has increased by 9798 to 22024, and elimination samples have decreased by 1177 to 6032. It should be noted that this is not a complete return from all England and Wales forces, as returns from Avon and

⁴ Paragraph 78 to 80 in the last annual report provide further background to this exception

Somerset, City of London, Hampshire, Humberside, West Midlands, and Wiltshire were not received.

Table 10: Forces' use of the CPIA exception to retain biometrics

	Total		Held in Force		Held by FSPs	
Arrestee/ PACE samples	12226	22024	557	1404	11669	20620
Elimination samples	7209	6032	5841	4116	1368	1916

Part 3 – Public Space Surveillance

47. I set out in Part 1 of this report how I built upon the work of my predecessor in ensuring that an orderly closure of my office would be achieved. The majority of effort to ensure closure and transition of OBSCC functions related to activity in the surveillance camera space. Consequently, no further work of significance in this arena was initiated. This contrasts with the ongoing engagement and casework in the areas of biometrics for which I also have responsibility. I therefore use this part of the report to reflect on issues that are related to technology and the future. Some of those reflections encompass biometrics, where the two increasingly overlap.
48. No area, aside from the use of foreign manufactured surveillance camera equipment that poses a risk to national security and potentially human rights, has been more contentious than the use of live facial recognition technology in public spaces. Falling across both surveillance cameras and biometrics, its widespread roll-out illustrates the potential regulatory and policy deficiencies that exist in dealing with biometrics that are neither fingerprints nor DNA. The way forward in the absence of additional regulation remains unclear. Notwithstanding the independent testing that has taken place, my concern beyond the approach in use relates to the accuracy of such technology, and I believe it incumbent upon government to engage more fully with civil liberties groups on risks and benefits of facial recognition technology, including structures and frameworks for the accountability of its use in public spaces.
49. Allied to that is the rapid development of AI. The new dimension here is the potential exploitation of huge sets of data that are now being generated. Similarly, even in what might be termed conventional surveillance camera spaces, such as ANPR, there is now the prospect of using such tools in ways that were not originally envisaged to support public safety. This is a matter that my predecessor wrote to the Secretary of State for Transport about.
50. Biometric technology remains an area of huge growth and innovation. In many respects one might argue that the greater the number of appropriately used biometric data sets, the better. Provided all the appropriate checks and balances are in place, then more biometric data ought to secure greater accuracy in identification. However, this growth in the range of biometrics, or

the potential use of new biometrics, must become a focus for policy, and possibly legislative, solutions. Whilst fingerprints and DNA have the primary interest, the advances in voice patterns, odour, and gait are becoming ever more sophisticated. Law enforcement colleagues, particularly those in the National Crime Agency who are at the cutting edge of the use of new biometrics, would be keen to achieve greater certainty in the access and use of such, whilst also understanding how they remain publicly and legally accountable for such use.

51. There can be no question that the use of these tools can be invaluable in bringing about increased public safety, but what is clearly needed is a balance between intrusion and the legitimate protection of society, and privacy. It is not the first time that technology has outpaced policy and regulation, however the speed of this innovation means that we must all work harder and smarter to keep alive to the risks and threats that these advances present to governance and accountability structures.
52. To reiterate, these rapid technological changes in the arena of public space surveillance, biometrics and all the interconnected technologies, necessitates the need to have clearer processes and assurances that relate to the development and deployment of such technology, including clear, published, and accessible policies that stakeholders, users and innovators can refer to. There is a need to ensure this sector has strong legal, ethical and societal frameworks in place that are robust and properly understood. Conversely, the lack of specific guidance could have an inhibiting impact on public safety, through reducing planning and investment in new and emerging technologies. Significant opportunities to support investigations and prosecutions are becoming increasingly available with new technology. It is imperative, therefore, that consideration is given to how this can practically be addressed. There is a desire from stakeholders on all sides of the debate to have greater clarity on these issues.
53. Further, with greater transparency comes greater trust and public confidence, especially when new technology is being developed, or being deployed. It is vital that people have confidence in the relevant technology doing what it is supposed to. And this means the whole ecosystem of surveillance cameras and biometrics, not simply novel offshoots of it. Confidence is required by all

of society: those who the technology is being deployed against and those deploying it, wider civil society, democratically elected representatives, and developers. Any use of technology in the public space must remain proportionate, legal, accountable and necessary.

54. As I have stated previously in this report, I believe increased stakeholder engagement is a vital part of gaining trust and confidence at all levels, and across all communities. There is a need to have a clear stakeholder engagement plan that can help form and contribute to the development and use of technology that has clear operational benefits for protecting the UK and keeping its citizens safe.

Part 4 – Reflections and Conclusion

Reflections

55. There is much to be proud of in relation to the work of OBSCC; it is evident that all the Commissioners have undertaken this role diligently and professionally. It is also clear to me that law enforcement take their responsibilities in relation to upholding public safety very seriously. In addition, I have found the arguments and positions taken by many civil liberty groups to be equally compelling, thoughtful and genuinely held. And the ‘thought leadership’ given by key academics has been impressive. There is now a unique opportunity to rethink, redesign and reshape how the governance, scrutiny and accountability of biometrics and surveillance cameras is conducted in England and Wales. Through tapping into the diversity of thinking and approach held by all the key stakeholders, there is the possibility for ministers to obtain the best, most robust and properly tested advice that is currently available. However, notwithstanding the process of how any such advice is collated, the end outcome must be greater clarity and guidance on how biometrics and surveillance camera issues are to be delivered and overseen for the public. There are many options that could work, and I look forward to seeing what those structures will look like in the near future.
56. Finally, I am grateful for the opportunity to have been the Biometrics and Surveillance Camera Commission, albeit for a time-limited period. I have confidence that future structures of the office are being considered thoughtfully and with foresight. And I remain entirely optimistic that any such solution will continue to engage with the full diversity of stakeholders.

Annex - Acronyms

ACRO	ACRO Criminal Records Office
AI	Artificial Intelligence
ANPR	Automatic Number Plate Recognition
CCTV	Closed Circuit Television
CPIA	Criminal Procedure and Investigations Act 1996
DPDI Bill	Data Protection and Digital Information Bill
FINDS	Forensic Information Databases Service
FSP(s)	Forensic Service Provider(s)
IPCO	Investigatory Powers Commissioner's Office
ICO	Information Commissioner's Office
IDENT1	The national police fingerprint database
MPS	Metropolitan Police Service
NCA	National Crime Agency
NDES	National Digital Exploitation Service
NDNAD	National DNA Database
NFA	No Further Action
NPCC	National Police Chiefs' Council
NSD	National Security Determination
OBSCC	Office of the Biometrics and Surveillance Camera Commissioner
PACE	Police and Criminal Evidence Act 1984
PNC	Police National Computer
PoFA	Protection of Freedoms Act 2012
SOFS	MPS Secure Operations – Forensic Services
VA	Voluntary Attendance

E03213131

978-1-5286-5206-3