3 August 2020

LEDS Consultation Response to the College of Policing

Q1 Thinking about the proposed layout, structure and language used for the Code and guidance document, do you feel it is clear and understandable?

Answer: Disagree.

Whilst the Code and the Guidance Document are clear in terms of layout and language, the actual *information* provided about LEDS should be expanded.

Transparency is key. Brief reference to the Nolan Principles addresses neither the reality of policing in the 21st Century, nor the ongoing real-time use of massive databases in the modern age. Policing in the UK and around the world has turned into a sophisticated data operation.

Privacy International believes that the obligation of transparency imposed by the General Data Protection Regulation should extend to all organisations and relevant third parties who will have access to LEDS. As a result, concrete information is needed in the final Code around the safeguards that will be implemented, how role-based access controls will be allocated and reviewed in the future, who will oversee this process, the data that will be kept, and the extent to which it will be shared with other organisations and third parties.

The Scope of the Code (contained in Section 4) states that:

This Code and the Guidance Document should be considered by organisations ***other than police forces in England and Wales.*** *By contractual arrangements, it will be applicable to other agencies within the United Kingdom that can access LEDS and selected data sets. This includes* ***police forces that are not covered by the Police Act 1996****, s 1, as well as other agencies with access to LEDS that exchange information with the police service in England and Wales.*

This paragraph requires clarification as it causes significant confusion in its current form. Does it mean that the code is not applicable to police forces in England and Wales and only to "other agencies within the United Kingdom that can access LEDS and selected data sets"? Or does it meant that these police forces should not take part in the consultation? We recommend that these issues are addressed and clarified.

Q2. Do you feel that the Code and Guidance Document effectively support the implementation of the five aims that are outlined on page 6 of the Code (safeguarding people, promoting accountability, promoting understanding, enabling performance and promoting fairness)?

Answer: Strongly Disagree.

Both the Code and Guidance Document are ambiguous, talk in the abstract, and fail to explain in any real detail how these five aims will be achieved, implemented, or measured, the Code should be expanded to provide further clarity and instruction.

We believe the development of LEDS poses serious threats to privacy and other fundamental rights, and therefore must be not only subject to strong oversight, safeguards, and transparency measures, but also these measures must be clear and implementable, with direct lines of responsibility. Neither the Code nor Guidance Document provide this, and instead refer to broad principles rather than concrete measures.

It remains unclear how those individuals entered on the LEDS database will be safeguarded against deliberate misuse of their data, such as so-called "LOVEINT"[1]– the use of massive and intrusive databases to spy on partners – or from incorrect or invalid data. As a result, neither the Code nor its Guidance document explain in sufficient detail how they will be safeguarding people, promoting accountability and understanding.

The Public Guide document provides that 'as well as sharing data between police services, the data LEDS will process for law enforcement purposes will come from a wide variety of sources including:

- International law enforcement agencies and bodies,
- Emergency services, such as fire and rescue ambulance services
- Courts
- Security companies that transfer prisoners
- Partner agencies involved in crime and disorder strategies
- Private sector organisations working with the police in anti-crime strategies
- Voluntary sector organisations,
- Approved organisations and people working with the police,
- People arrested
- Victims
- Witnesses
- Relatives, guardians or other individuals associated with missing people
- Individuals passing information
- Local authority and private CCTV cameras
- Body-worn video operated by police officers
- Custody images[2]

[1] https://en.wikipedia.org/wiki/LOVEINT
[2] Public Guide para 15.6

We believe this list of sources risks providing data that goes beyond "law enforcement purposes". Under data protection law, fairness is intimately linked with an individual's reasonable expectations as to how their data may be used. Thus, the way data is increasingly used for law enforcement purposes and the sources where it may come from, may not be within individuals' reasonable expectations because they are either unaware of it or because they are aware of it but find it unacceptable, thus raising questions of fairness.

Already this year, the ICO was very critical of the Police and CPS's use of digital data extraction from mobile phones and recommended that the police implements stronger safeguards to protect data gathered from victims' and witnesses' phones.[3]

The ICO report highlighted numerous risks and failures by the police in terms of data protection and privacy rights. The report also confirms PI's concerns that the data extracted and processed from the mobile phones was often too excessive.[4] The police and the CPS were not giving enough consideration to "necessity, proportionality and collateral intrusion" given the intrusive nature of the mobile phone extraction technology. This is just one example of many, and when combined with further subjective, potentially excessive sources, or fully lawful behaviours – such as car ownership or immigration status – we believe LEDS will not meet the principles of accountability, fairness or understanding, and as we have seen in the case of mobile phone extraction may contribute to behaviours the opposite of safeguarding.

Further, considering that LEDS will not be open for public access[5], individuals whose information is contained in the system may not have any knowledge that such an entry exists, let alone be able to correct any mistakes – accidental or otherwise. The Guidance document expressly provides that there are restrictions and exemptions that can be applied to prevent individuals from exercising their rights under the data protection legislation (such as right of access and right of erasure) if these are considered to fall under the law enforcement purposes.[6] Sections 31 and 45(4) of the Data Protection Act 2018 provide for broad exemptions for subject access rights with regard to information relevant to the 'law enforcement purposes' and prevention, detection, investigation or prosecution of criminal offences. As a result, there is a strong chance that the individual requiring access to their information will not be provided with it, particularly in relation to intelligence material stored on the database.

Considering LEDS, by design, combines the public record with intelligence material, this is problematic. The nature of intelligence material is such that it is very unlikely to ever be subject to scrutiny or challenge. To the extent that the intelligence material is

[3] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[4] https://privacyinternational.org/press-release/3941/press-release-critical-ico-report-says-police-must-stop-taking-data-victims
[5] Public Guide para 16, p 26.
[6] Guidance Document p. 58

inaccurate, those inaccuracies may go un-corrected for a considerable period of time – if ever.

We highly recommend the implementation of a robust system of redress to allow individuals to challenge their inclusion in LEDS if they fear it to be unlawful, as well as sufficient transparency to allow individuals to understand if they are included.

There are currently about 12 million images enrolled into the PND gallery – equivalent to 1/5th of UK's population – a number of which are held unlawfully. Whilst the Guidance Document states there is no intention to bring facial recognition or AI technology into LEDS, it will gain the facial matching capabilities currently in the PND. This facial search facility enables users to upload a probe image from an external source – such as from CCTV, mobile phones, cameras, and photocopied documents such as passports[7] – and then compares this probe image across all images attached to personal or custody records to see if there are any suggested matches.

The prospect of integrating these capabilities with other data sources such as immigration or DVLA provides a further, rich source of potential "watchlist" images, as we have seen with the Met's controversial "Gangs Matrix". Once operational, the Home Office will not be able to control police or others' use of LEDS. They would not, for instance, be able to prevent the downloading of images for other purposes.

Absent further legal controls, all information on LEDS will be liable for integration with locally held databases used for other purposes, including potentially automated facial recognition technology (AFR), as has been trialled by The Met and South Wales, rendering moot the lack of AFR in LEDS itself. It is also possible that constabularies build their own parallel databases (such as the Metropolitan Police's Gangs Matrix)[8] and/or augment their existing local databases with data from LEDS. This compounds existing concerns around AFR as it is currently implemented in the UK.[9]

Considering neither the Code itself nor the Guidance Document outline how these issues are expected to be dealt with other than an assertion that they won't happen, they do not go far enough to effectively support the implementation of the five aims mentioned on page 6 of the Code.

As a result, PI recommends implementation of robust controls to ensure that the images and data contained in LEDS cannot be used for any other purposes such as AFR technology, building parallel databases or watchlists. PI is aware that access to DVLA data through LEDS will occur via an API interface[10] that will allow access to DVLA

---

7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721542/NLEDP_Privacy_Impact_Assessment_Report.pdf

8 https://www.stop-watch.org/uploads/documents/Being_Matrixed.pdf

9 R (Bridges) v CC South Wales [2020] EWCA Civ 1058

10 https://www.college.police.uk/What-we-do/Standards/Codes_of_practice/Documents/Why_might_my_details_be_on_LEDS.pdf

but no copying would be allowed.[11] This would preserve the integrity of the information, reduce the risks of data loss and prevent copies and distributions. We strongly recommend adopting the same mechanism for all data contained in LEDS, to reduce risks of misuse and to preserve data quality.

Q3 Do the Code and Guidance Document set out and explain the ethical principles that individuals and organisations using LEDS should follow?

Answer: Strongly Disagree.

Whilst the Code and Guidance Document state that LEDS information and data should be used ethically and in accordance with human rights, we believe that the current safeguards are insufficient to ensure this is the case. While the principles are useful, they are insufficient as safeguards for users and organisations to ensure their compliance with the ethical standards, human rights and equality principles.

As mentioned previously, the inclusion of intelligence material within the scope of LEDS, and therefore providing it by default to the numerous users and organisations expected to access LEDS rapidly increases the risks of misuse or other exploitation of such data.

The Code and the Guidance Document emphasises that individuals and organisations using LEDS should not:

- Share information with colleagues for a purpose which is not a specific law enforcement, other policing or safeguarding task.
- Share information with colleagues which is not proportionate or relevant to the identified law enforcement, other policing or safeguarding task.
- Share information externally on individuals who may be in the public eye, whether for personal gain or for other reasons.
- Share information externally on individuals, vehicles or other matters to assist third-party enquiries (colleagues, family members, friends or others) which are not linked to a legitimate law enforcement, other policing or safeguarding purpose.
- Share information externally to others with a view to perverting the course of justice or interfering with a law enforcement purpose.[12]

However, the documents fail to provide concrete safeguards to ensure these practices do not take place, nor outline details of the redress or disciplinary procedures as a result of misuse. It is also not clear whether, as we have seen in various disciplinary proceedings before Professional Standards in the Met, disciplinary

[11] https://www.openrightsgroup.org/blog/police-data-practices-need-to-change-leds-is-the-start-of-that-change/
[12] LEDS Guidance Document p. 49

proceedings may be bypassed altogether by officers under investigation leaving their roles.[13]

The LEDS single interface to numerous diverse databases provides much more information than would traditionally be expected for policing – including immigration status, driving licences, and material gathered from intelligence. As a result, it is crucial not just that all users adhere to the ethical principles, but that relevant, clear and effective safeguards exist, are enforceable, and are enforced.

The LEDS Public Guide refers to the audit departments for the Police National Computer and the Police National Database, who pick random transactions to check whether they were appropriate. However, the auditors currently only pick about 5% of transactions meaning that 95% of transactions will go unchecked. [14] This is unsatisfactory, considering that the Information Commissioner's Office (ICO) has previously found that the Police contravened data protection principles in its investigation into the Gangs Matrix,[15] and Mobile Phone Extraction.[16]

In particular, the ICO had significant concerns regarding the data entered into the Gangs Matrix database. Statistics from July 2016 show that 87% of the people recorded in the Gangs Matrix were from Black, Asian or Minority Ethnic (BAME) backgrounds. Further, 78% were Black, despite the fact that only 13% of London's total population are Black. Additionally, 99% of people recorded on the Gangs Matrix were male.[17]

Given the risks of misuse and exploitation of data, we believe:

- There should be clearer rules that will provide greater clarity and foreseeability about when, why and how the police and other third parties are able to use and access LEDS.
- Robust policies and procedures must be put in place to ensure the appropriate handling and deletion of data.
- More transparency surrounding the way role-based access controls will be assigned, controlled, monitored, and publicly notified
- To meet the standards required for fair processing, there should be further guidance on how police forces should engage with individuals whose data has been stored on LEDS to inform them and what their rights are.
- Details of the redress or disciplinary procedures as a result of misuse of LEDS should be made clear.

[13] https://www.telegraph.co.uk/news/uknews/law-and-order/9839944/200-officers-a-year-retire-or-resign-to-avoid-disciplinary-proceedings.html
[14] LEDS Public Guide para 9.3 p 16
[15] https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf
[16] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[17] https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf.

- LEDS users should publicly disclose what access they have, how individuals can exercise their data rights, and how to seek redress.

Q4 Do the Code and guidance document make clear the range of organisations involved in LEDS, the roles of those organisations and how those organisations should process personal data?
(A list of organisations with access to LEDS data is available on the college.police.uk consultation page.)

Answer: Disagree

We are aware that the current list of organisations with access to LEDS that is available on the on the college.police.uk consultation page is not exhaustive. As a result, other organisations could be added to the list at a future date, as deemed necessary. We also note that in the longer term, the Home Office seeks to enable further data sharing between a range of organisations through the addition and integration of more systems to the platform or through links to systems owned by other organisations. Given the serious risk of function creep, any addition of new data sources or access rights must be subject to parliamentary and public scrutiny and transparency.

This is very problematic, considering the impact that being wrongly entered into or accessed through the database can have on an individual's private life. The breadth of personal, highly sensitive and inaccurate information that can be available on LEDS poses significant risks. It can be utilised in a way negatively affecting individuals' lives, employment, state benefits, immigration status, and will only become more intrusive as data sources continue to be added to the LEDS interface.

For these reasons, the Code and guidance document should be very clear on how additional organisations will be given access to LEDS and should include a consultation process for such addition where the organisation proposed serves a purpose different from core law enforcement, such as the Border Force or state benefit organisations.

Further, there is no mention of either how or if the UK's intelligence agencies will have access to LEDS. If GCHQ, MI5 or MI6 is to have access to LEDS, the Code should make this clear and outline their powers and responsibilities.

Similarly, there is no mention of either how or if contractors and companies involved in developing, maintaining, or providing staff for the use of LEDS will have access. Given that commercial organisations are involved in the development of LEDS and provide staff to the Home Office and other government bodies, they should be included in the Code.

Q5 Thinking about privacy laws and regulations, do the Code and Guidance Document clearly set out the performance expectations and behaviours for LEDS users?

Answer: Strongly disagree

No, because the Code and the Guidance Document is restricted to principles and does not deal in detail with any problems that LEDS poses for privacy rights and data protection.

We are concerned the creation of LEDS leads to the spectre of access by default to incredibly powerful wide-ranging capabilities, far greater than the sum of their parts. This is not a theoretical risk either – we have already seen local authorities using powers under the 'anti-terror law', Regulation of Investigatory Powers Act (RIPA) 2000, to spy on the public in secret [18]– spying on citizens walking their dogs, feeding pigeons and those suspected of 'bin crimes'.[19] This demonstrates the ease with which broad access to a vast amount of information will be exploited without any meaningful safeguards..

As we have unfortunately seen, Police forces have a long history of retaining personal data unlawfully, including DNA and Fingerprint data, and photographs. There's an equally long history of the destruction of records and evidence around Police missteps and outright illegality (Operation Hibiscus,[20] Operation Herne et al).[21] The Police seem slow to learn from previous investigations, reports, or recommendations.[22]

Further, as mentioned above, the ICO found that the Metropolitan Police had contravened data protection principles in relation to its investigation into the Gangs Matrix and in Mobile Phone Extraction of complainants. It found that data was retained for longer than is necessary, personal data was not erased and the Met Police failed to apply a consistent retention policy.

Worryingly, the data subjects were never truly removed from the Gangs Matrix.

The ICO also found that there was an excessive sharing of information with a wide array of third parties and organisations.[23] Considering this track record and culture of retention, PI is concerned that LEDS will be subject to the same failures as the Gangs

[18] https://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public
[19] https://www.telegraph.co.uk/news/uknews/3333366/Half-of-councils-use-anti-terror-laws-to-spy-on-bin-crimes.html
[20] https://policeconduct.gov.uk/sites/default/files/Op_Hibiscus_Final_report_for_publication.pdf
[21] https://www.met.police.uk/cy-GB/SysSiteAssets/foi-media/metropolitan-police/priorities_and_how_we_are_doing/corporate/operation-herne---terms-of-reference
[22] https://www.independent.co.uk/news/uk/home-news/met-police-cressida-dick-racism-bianca-williams-stop-search-a9607671.html
[23] https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf, p 12.

Matrix database. This is in spite of the fact that the Code and Guidance Documents refer to the relevant data protection legislation.

The Home Office will not be able to control how local constabularies and other relevant bodies will use LEDS. This ultimately means any and all images accessible via LEDS could be considered "fair game" to create or augment watchlists or other local police databases, such as the Metropolitan Police's Gangs Matrix.

Further, we believe that LEDS will also facilitate rapid checks of people's immigration status. For example, police already use mobile fingerprint devices linked to IABS.[24] These devices comprise software produced by the Metropolitan Police staff, used on an Android smartphone handset and paired with a fingerprint reader.

If a suspect has a criminal record or is known to immigration enforcement their identity can be confirmed at the roadside. An officer, with relevant access levels, can also use the device to check the Police National Computer to establish if they are currently wanted for any outstanding offences. Linking IABS to mobile biometric devices allows officers to instantly query someone's immigration status, possibly in the near future via their facial biometrics. It would also enable them to populate any watchlist with immigration enforcement-based individuals of interest.

As a result, we do not believe that the Code and Guidance Document clearly set out the performance expectations for LEDS users with respect to privacy law and data protection legislation. It does not prevent them from misusing and exploiting individual's private information and personal data. We recommend:

- There should be clear querying and escalation guidelines against LEDS, in line with minimum access controls. The police should not be regularly accessing information outside their immediate policing need.
- That appropriate safeguards are put in place to ensure that LEDS is not used for immigration enforcement
- LEDS must not be compiled with AFR technology or used to create local police databases and 'watchlists'.
- A mandatory Data Protection Impact Assessment should be made public to increase transparency about the use of LEDS and replace the existing privacy impact assessment.[25] This should be implemented across England and Wales, to increase public confidence in the accountability of the police and the criminal justice process when using this intrusive 'mega-database'.

Q6 Do the Code and Guidance Document clearly set out that all LEDS users should be given appropriate initial and refresher training?

[24] http://news.met.police.uk/news/met-develops-mobile-fingerprint-device-to-save-time-and-public-money-317200
[25] https://www.gov.uk/government/publications/law-enforcement-data-service-privacy-impact-assessment

Answer: Disagree.

Whilst the Code sets out that all LEDS users should be given appropriate training, we are concerned that this training without due regard risks being little more than a tick-box exercise.

It is crucial that training is effective and deals with issues such as what data would be deemed accurate and reliable, when the data from LEDS should be deleted, when it should be accessed and to what extent it should be shared. It is also necessary that there are no discrepancies in the understanding of the relevant data protection legislation and human rights amongst local police forces and constabularies.

Appropriate and effective training is crucial considering that LEDS will contain a *significant*[26] amount of data previously reserved for intelligence rather than evidential purposes. This may include subjective information from first-hand experience of the reporting officer, from covert human intelligence sources, and from lawfully authorised technical deployments such as trackers or listening devices. The nature of intelligence material is such that it is very unlikely to ever be subject to scrutiny or challenge. As a result, training should also address how and when intelligence material should be recorded, as well as the limitations on its reliability, and when it should be shared with other organisations, if at all.

Q7 Does the Code state clearly that users have a responsibility to ensure that data held in LEDS is of the highest possible quality?

Answer: Disagree.

The Code and its Guidance document do state this, but again talk is in the abstract, failing to explain to the users *how* they can comply with their responsibility that data held in LEDS is of highest possible quality, what this means in practice, or how this will be measured.

Considering the broad nature of sources of data, outlined above, together with the fact that data will consist of intelligence material, it is very difficult, if not impossible, to ensure that data entered is of highest quality and accurate.

As noted above, the relevance of intelligence material is often subjective, and its nature is such that it is very unlikely to ever be subject to scrutiny or challenge. To the extent that the intelligence material is inaccurate, those inaccuracies may go un-corrected for a considerable period of time – if ever. Considering that LEDS will consist

26 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721542/NLEDP_Privacy_Impact_Assessment_Report.pdf

of both evidence and intelligence data, the code fails to provide sufficient safeguards to ensure that the data is of highest possible quality.

Granting broad access to information, absent further legal safeguards, will negatively affect the trust between citizens, the police, and other agencies. Establishment of LEDS risks leading to over-policing, further embedding distrust in the police of individuals from ethnic minorities and migrant backgrounds, as well as those who are in vulnerable positions, such as trafficking victims or missing persons.

By developing the technical capability in the backend to converge disparate data and make it more easily accessible, it will allow more authorities to access more data. This means that whatever access controls are put in place at the moment, they are subject to change and at the discretion of decisions made by whoever is in power in the future. It is essential therefore to ensure the system and decision-making process is as transparent as possible and subject to sufficient oversight. Potential biases in the system must be routinely interrogated and eliminated.

Q8 Does the Code clearly set out that personal data collected for law enforcement purposes and stored in LEDS needs to be lawful, adequate, relevant and not excessive in relation to the purpose for which it is processed?

Answer: Strongly Disagree.

As pointed out previously, the data on LEDS will be drawn from a broad range of sources and will include intelligence as well as evidential material. Further, LEDS will not just provide access to information contained in the PND and the PNC, but also a number of different other data systems used by forces. As a result, it is difficult to understand how it will be ensured that the data stored in LEDS will be lawful, adequate, relevant, and not excessive.

The very nature of LEDS appears to be to combine data in an excessive form, without necessarily understanding its relevance to a particular operation, especially when subjective intelligence material is included. The covert nature of the collection and use of intelligence material also raises questions as to its adequacy and accuracy, especially if it cannot be challenged by the data subject.

It is also difficult to see how data processed and stored in LEDS will be lawful, adequate, relevant and not excessive considering the lack of clarity as to what images will exist on LEDS once the PND and PNC are combined. There are currently about 12 million images enrolled into the PND gallery, some of which are retained unlawfully.[27]

[27] R (RMC and FJ) v Commissioner of Police of the Metropolis [2012] EWHC 1681 (Admin)

Absent further legal control, all of the information on LEDS will be liable for integration with locally-held databases used for other purposes, including potentially automated facial recognition technology (AFR). The prospect of integrating the information obtained from LEDS with AFR technology drastically expands the potential range of source images available for use in AFR watchlists. This would include information held in databases:
(i) comprising solely, or primarily, intelligence material; rather than evidential material; and
(ii) collected on the basis of an individual's wholly lawful conduct (e.g. immigrating to the United Kingdom).

Considering that the Code and the Guidance document fails to address these issues, it cannot be said that it clearly sets out that the data in LEDS needs to be lawful, adequate, relevant and not excessive.

Q9 Are the governance arrangements for maintaining the Code clear and easy to understand?

Answer: Strongly Disagree.

No, they are not. The Code and its Guidance Document clearly state the exact governance structure for LEDS is still under discussion, therefore the documents *by definition* lack sufficient detail for this to be clear and easy to understand.

As LEDS goes 'live', it is essential that the governance framework is finalised without delay and incorporated into the Code.

Q10 Do the Code and Guidance Document clearly explain the types of activity that will be exempt from the Code?

Answer: Strongly Disagree.

None of the consultation documents (the Code, the Guidance and the Public Guide) contain a section outlining what the exemptions are. As a result, the exempt activities are not clear.