24 July 2020

To: The House of Commons Science and Technology Committee

Via email only: scitechcom@parliament.uk and gregclarkmp@parliament.uk

Dear Chairperson and Committee Members,

Re: Development of the Law Enforcement Data Service (LEDS) by the Home Office and the College of Policing

Privacy International (PI) is an international NGO, based in London, which works with partners around the world to challenge state and corporate surveillance and data exploitation. As part of our work, we advocate for changes in the way police and other governmental agencies use new technology to gather data.

Since Autumn 2018, PI has been involved in Law Enforcement Data Service (LEDS) stakeholder meetings with the Home Office, the College of Policing, and others. LEDS is currently being developed by the Home Office National Law Enforcement Data Programme (NLEDP) and will replace the existing – and currently separate – Police National Computer (PNC) and Police National Database (PND) and allow for the addition of new data sources.

We are aware the Home Office notified you about the public consultation undertaken by the College of Policing in relation to the development of LEDS and its Code of Practice, a crucial policy which outlines how the database is to be used and protected.[1]

We urge the Committee to review the development of LEDS — the initial stages of which are due to be operational this year — and its Code of Practice because of the potential for LEDS to negatively impact on individuals' lives, as well as their fundamental rights and freedoms.

LEDS overview

As a direct result of the combination of multiple, currently separate databases, the information routinely provided by LEDS will be far broader than is possible with the current database searches. This directly results in an increased risk of infringement of individuals' right to privacy under Article 8 of the Human Rights Act 1998.

The Home Office currently expects the first stage of LEDS to be operational in the next five months and plans to continue adding further data sources through 2023, and beyond. The data that will be made available through a single search on the LEDS

[1] https://www.college.police.uk/What-we-do/Standards/Codes_of_practice/Pages/Law-Enforcement-Data-Service.aspx

interface is vast, ever-increasing, and worryingly mixes both evidential *and* intelligence material – which have traditionally been collected, kept, and searched for different reasons – in the same single search interface.

The Police National Computer, first introduced in 1974, holds information on citizens – such as their vehicles and property – as well as arrests, charges and court disposals (including but not limited to convictions). The PNC holds 12.6 million persons' records – the equivalent of approximately **1/5th** of the UK's population. This functionality is currently planned to be rolled into LEDS in 2021.

The Police National Database, introduced in 2009, receives daily intelligence data from "law enforcement" agencies (predominantly police constabularies) concerning persons, events, locations, organisations (including criminal) and objects. The number of records on PND is not easily established, as due to how it stores information there is no equivalent to a single person's record. The High Court of England and Wales has previously held that the way in which data is stored on PND breached individuals' rights to privacy, due to indefinite retention of individuals' images.[2]

The vision of the Home Office is to provide police and others a super-database, with on-demand, at the point of need access, containing up-to-date and linked information about individuals' lives.

The stated aim of LEDS is to "prevent crime and better safeguard the public".[3] As such it will be accessed by both police and a diverse range of agencies, including – but not limited to – the National Crime Agency, HMRC, and the Gangmasters and Labour Abuse Authority. LEDS will also be accessed by a number of private sector organisations.

The College of Policing published an initial, non-exhaustive list of organisations that will have access to LEDS.[4] In the longer term, the Home Office seeks to enable further data sharing between a range of organisations, by the addition of more systems to the platform or through links to systems owned by other organisations, such as Border Force, to enable a more "joined up" approach in the law enforcement field.[5]

PI's Concerns

[2] R (on the Application of RMC and FJ) v Commissioner of Police of the Metropolis [2012] EHWC 1681 (22 June 2012) http://www.bailii.org/ew/cases/EWHC/Admin/2012/1681.html

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

[4] https://www.college.police.uk/What-we-do/Standards/Codes_of_practice/Pages/Law-Enforcement-Data-Service.aspx

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721542/NLEDP_Privacy_Impact_Assessment_Report.pdf p. 6

We believe that the development of LEDS is problematic and should be subject to parliamentary oversight. We would like to draw your attention to our key concerns regarding LEDS.

Conflating intelligence and evidence

- LEDS will contain a ***significant*** amount of data previously reserved for intelligence rather than evidential purposes.
- 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 inaccurate, those inaccuracies may go un-corrected for a considerable period of time – if ever.
- Numerous agencies and organisations will have access to this information, which 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.
- Providing access to private sector organisations is particularly problematic in light of this intelligence-gathered material that will be available on LEDS.

Expanding watchlists for facial recognition

- There is a 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, many of which are currently retained unlawfully.[6] The prospect of the integration of these databases with other data sources provides a further, rich source of potential "watchlist" images.
- 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 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). It is also possible that constabularies build their own parallel databases (such as the Metropolitan Police's Gangs Matrix) and/or augment their existing local databases with data from LEDS.
- LEDS will maintain the facial matching capabilities which currently exist on the Police National Database.

[6] R (on the Application of RMC and FJ) v Commissioner of Police of the Metropolis [2012] EHWC 1681 (22 June 2012) http://www.bailii.org/ew/cases/EWHC/Admin/2012/1681.html

- The prospect of integrating 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).

The police are not the Border Force

- LEDS will facilitate access to immigration data, including biometric data. For example, the LEDS interface can show if an entry exists in the Immigration, Asylum and Biometrics System (IABS), as well as the IDENT1 (Law Enforcement and Security Biometrics System).
- The recent roll out of mobile scanning equipment by police forces across the UK combined with integration to backend databases has enabled rapid checks of people's immigration status. This is transforming police officers into border control agents, with little scrutiny or public consideration of the implications.
- The Home Office has emphasised that the information available on Home Office Biometrics (HOB) Programme and LEDS will be limited to role-based access controls. However, it remains to be seen how effective these will be.
- It is unclear how these controls will be allocated, who will oversee them and importantly, how access to information outside of a specific role might be gained. For example, it may be possible for a police officer without specific role-based access controls to simply contact the control centre to obtain the relevant information. As a result, it is unclear if this method of limiting access will be effective. Even if HOB and LEDS databases are kept "physically" separate, as soon as they become accessible through a common interface such as LEDS there is no longer any "logical" separation.

LEDS risks over-policing

- Granting such 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.

As a result of these concerns we urge the Committee to look into the development of LEDS, and its Code of Practice as published by the College of Policing.

While the technical development of LEDS is ongoing, questions relating to how the powers will be safeguarded and overseen are still to be finalised. This provides an opportunity for your committee to ensure that effective governance and safeguards exist over a system which will be central to UK policing for generations to come.

We further urge you to consider the impact that this will have on individuals' lives, and on their fundamental rights and liberties.

Your review would be the only parliamentary oversight the development of this 'super-database' will be subject to, and it is therefore crucial that this issue receives your full attention.

We look forward to hearing from you in relation to this request. Should you require any further information or have any questions please do not hesitate to contact us.

Yours faithfully,

Privacy International

Co-signed by the following organisations:

Baobab Women's Centre

Central Asylum Yorkshire

Coram Children's Legal Centre

Duncan Lewis Solicitors

Immigration Law Practitioners' Association (ILPA)

Joint Council for the Welfare of Immigrants

Migrants at Work

Migrants Rights Network