PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

Rt Hon Amber Rudd MP
Secretary of State for the Home Department
Home Office
2 Marsham Street
London SW1P 4DF

and via email: public.enquiries@homeoffice.gsi.gov.uk;
amber.rudd.mp@parliament.uk

26th April 2018

Dear Home Secretary,

RE: Privacy International report, *'Digital stop and search: how the UK police can secretly download everything from your mobile phone'*

We write further to our letter dated 28 March 2018 (copy enclosed). We note that you have failed to respond to this letter in which we requested that you:

1. Undertake an independent review into the use of mobile phone extraction technologies used by the police;
2. Conduct a consultation with the public, civil society, industry and government authorities to identify the extent to which it is necessary and proportionate to utilise this technology.

In response[1] to parliamentary questions[2] posed by David Lammy MP, the Home Office appears to have little understanding of how this technology is

[1] Mr Nick Hurd responded to questions on behalf of the Home Office
[2] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-questions-answers/?dept=1&house=commons&max=20&member=206&page=2&questiontype=AllQuestions 123001, 132003, 132004, 132008, 132209,

used. This is unacceptable. The Home Office must lead from the front, and establish clear guidelines.

We are concerned that your failure to take action results in the continuation of activities by the police in a situation where:

1. there is no clear legislation, policy framework, regulation or independent oversight in place for the police's use of this technology;
2. there are no protections for the public from abuse of this technology;
3. the police are taking data from people's phones without obtaining a warrant;
4. this is often taking place secretly, without individuals - whether they are suspects, witnesses or even victims of crime - being informed that content and data from their phone is being downloaded and stored indefinitely by the police.
5. without any kind of record keeping or national statistics, abuse of this technology and unfair targeting of minority groups is likely to go unnoticed.

In relation to the final point, David Lammy, MP for Tottenham and author of the 2017 Lammy Review into the treatment of, and outcomes for Black, Asian and Minority Ethnic individuals in the criminal justice system, said of Privacy International's report on mobile phone extraction:

> *"The lack of transparency around new policing tools such as mobile phone extraction is a serious cause for concern. There are no records, no statistics, no safeguards, no oversight and no clear statement of the rights that citizens have if their mobile phone is confiscated and searched by the police.*
>
> *My Review of our criminal justice system found that individuals from ethnic minority backgrounds still face bias in parts of our justice system, and it is only because we have transparency and data collection for everything from stop and search incidents to crown court sentencing decisions that these disparities are revealed and we are able to hold those in power to account. Without the collection and audit of data about the use of mobile phone extraction powers scrutiny will be impossible.*
>
> *Given the sensitive nature and wealth of information stored on our mobile phones there is significant risk of abuse and for conscious or*

unconscious bias to become a factor without independent scrutiny and in the absence of effective legal safeguards.

We entrust so much personal information to our phones that the police having the power to download every message and photo we have sent or received without any rights and protections is another worrying example of regulations not keeping up with advances in technology."

We enclose a copy of our complaint to the Information Commissioner's Office. In addition to the absence of clear legislation, unacceptable reliance by some forces on Police and Criminal Evidence Act 1984, confusion between forces as to the appropriate legal basis, we believe the use of mobile phone extraction is in breach of the Data Protection Act 1998 and will breach the Data Protection Bill currently progressing through Parliament.

Sir Peter Fahy, former Chief Constable of Greater Manchester Police, has agreed[3] that legislation has not kept up with technology and some officers are unaware of how they should and should not be using mobile phone extraction tools. There must be new legislation which addresses the nature of modern policing and the sophisticated new technology available to the police.

We repeat our invitation for you to meet with us. We have undertaken a number of mobile phone extractions using a Cellebrite UFED Touch 2 and are willing to show you the information that has been extracted from our personal phones to give you an idea about the intrusive nature of this power, and why it demands your attention.

<u>Recommendations</u>

As stated in our previous correspondence, we have made a number of recommendations in our report and urge you to give these serious and considered attention:

- An immediate independent review into this practice should be initiated by the Home Office with consultations taken from the public, civil society, and industry as well as government authorities.
- Guidance aimed at the public regarding their rights must be published.
- The police must have a warrant issued on the basis of reasonable suspicion by a court before forensically examining anyone's smartphone, or otherwise accessing any content or communications data stored on the phone.

[3] http://www.bbc.co.uk/news/uk-43507661

- A clear legal basis must be in place to inspect, collect, store and analyse data from devices. It must be considered whether such intrusive technology should only be used in serious crimes.
- There must be adequate safeguards to ensure intrusive powers are only used when necessary and proportionate.
- The analysis of necessity and proportionality should include any effect the police action may have on the security and integrity of the mobile phone examined, or mobile devices more generally.
- The owner and user(s) of any phone examined should be notified that the examination has taken place.
- Anyone who has had their phone examined shall have access to an effective remedy where any concerns regarding lawfulness can be raised.
- Cybersecurity standards should be agreed and circulated, specifying how data must be stored, when it must be deleted, and who can access.
- There must be independent oversight of the compliance by government authorities of the lawful use of these powers.
- All authorities who use these powers must purchase relevant tools through procurement channels in the public domain and regularly update a register of what tools they have purchased, including details on what tools they have, the commercial manufacturer, and expenditure amounts.

Yours faithfully,

Camilla Graham Wood
Privacy International

Cc Mr Nick Hurd
nick.hurd.mp@parliament.uk