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

28 March 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 in relation to the above report (attached). The report examines the police's use of sophisticated and highly intrusive 'mobile phone extraction' technology. We believe you should share our alarm that:

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.

The reliance of some forces on section 20 of the Police and Criminal Evidence Act 1984 is unacceptable. This 34-year-old law significantly pre-dates the use of smartphones and indeed the entire digital era. Sir Peter Fahy, former Chief Constable of Greater Manchester Police agrees[1] 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 request that you urgently commission an independent review into the practice. This review must include a widespread 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.

We are concerned that in response to parliamentary questions posed by David Lammy MP, the Home Office appears to have little understanding of how this technology is used. This is unacceptable. The Home Office must lead from the front, and establish clear guidelines: 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

We encourage you to request a demonstration from the police to show you the volume of information that can be extracted from mobile phones, thus demonstrating the risks associated with use of this power. We have undertaken a number of mobile phone extractions using a Cellebrite UFED Touch 2 and invite you to meet with us so that we can 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.

Recommendations

We have made a number of recommendations in our report and urge you to give these serious and considered attention:

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

- 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.
- 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