LCHR

Labour Campaign for Human Rights

END-TO-END ENCRYPTION

APRIL 2017

Executive Summary

Following the tragic terrorist attack in Westminster in which the perpetrator is believed to have opened the WhatsApp messaging service just minutes before launching the attack, the home secretary has called for intelligence agencies and police to be given access to end-to-end encrypted messaging services.[1]

The Labour Campaign for Human Rights believes that the home secretary's plan to persuade internet and social media platforms to voluntarily put back-doors into encrypted services is not practical or proportionate.

Security

If companies like WhatsApp were to end their encrypted services, it would make millions of everyday users less secure. It is impossible to build a back door to encryption which only applies to some users and not all. That means that anyone could theoretically access data shared via an unencrypted platform, including cyber criminals. In 2015, £347m worth of payments were made through banking apps in Britain – an increase of 54%.[2] With more and more people using apps for things like banking, it is crucial that their online data is sufficiently protected.

In 2015, following a terrorist attack in San Bernardino, California, the FBI asked Apple for assistance in retrieving data from an iPhone used by one of the shooters. Apple refused to build a system that would allow authorities to effectively break into the phone. They argued that once built, that software could be used by anyone to unlock any number of devices and would expose their customers to greater levels of risk. In a statement to customers, Tim Cook, the Chief Executive of Apple wrote, "The implications of the government's demands are chilling…it would have the power to reach into anyone's device to capture their data".[3]

Amber Rudd is now making similar demands of companies in the UK. If companies like WhatsApp were to agree, it would open the door to hackers and cyber criminals to gain access to credit card details, medical data, passport scans, address, photographs and anything else users may have sent online.

Freedom of the Press

Encryption has also become useful protection for journalistic sources. UNESCO recently published a report on the topic as a result of "acknowledgement in both the UN General Assembly and the UN Human Rights Council of the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance or interception of communications in violation of their rights to privacy and to freedom of expression".[4] The report found that in 121 member states some form of source protection was being eroded by either anti-terrorism legislation, surveillance, both mass and targeted and data retention policies. This kind of erosion of privacy for journalists and their sources could result in "pre-publication exposure of journalistic investigations which may trigger cover-ups, intimidation, or destruction of information, revelation of sources' identities, sources of information running dry"[5] and

---

[1] Andrew Sparrow, 'WhatsApp must be accessible to authorities, says Amber Rudd', The Guardian, 26th March 2017. https://www.theguardian.com/technology/2017/mar/26/intelligence-services-access-whatsapp-amber-rudd-westminster-attack-encrypted-messaging

[2] Rupert Jones**, '**Mobile banking on the rise as payment via apps soars by 54% in 2015', The Guardian, 22nd July 2016. https://www.theguardian.com/business/2016/jul/22/mobile-banking-on-the-rise-as-payment-via-apps-soars-by-54-in-2015

[3] Tim Cook, 'A message to our customers', 16th February 2016. http://www.apple.com/customer-letter/

[4] UNESCO, 'Publishing in the Digital Age', UNESCO Series on Internet Freedom. http://www.unesco.org/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/protecting_journalism_sources_in_digital_age.pdf

[5] UNESCO, 'Publishing in the Digital Age', UNESCO Series on Internet Freedom. http://www.unesco.org/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/protecting_journalism_sources_in_digital_age.pdf

"self-censorship by journalists and citizens more broadly".[6] In Britain we have a 300 year tradition of press freedom and ending encryption would make that more difficult to maintain.

Practicality

Moreover, the practicality of Rudd's request is questionable. She has stated that she doesn't want to introduce legislation that would mean a blanket ban on end-to-end encryption. Agreeing that there is a necessity for protection online, she said, "end-to-end encryption has a place. Cybersecurity is really important and getting it wrong costs the economy and costs people money, so I support end-to-end encryption".[7] However, without a change in legislation, even if Rudd is able to persuade some companies to end their encrypted services it will simply mean that other servers will enter the market who do provide encryption and users will switch platforms. It would also be very difficult for companies like WhatsApp and Facebook to change their systems in one country and not another.

Most importantly, if popular messaging services cease to provide end-to-end encryption, terrorists and criminals are likely to develop their own messaging services that do, rendering the government's efforts obsolete.

Conclusion

It is absolutely right that social media platforms and apps help the authorities in whichever way they can in cases like the attack on Westminster. However, it is also right that the privacy of everyday users, of which there are 1.2 billion monthly users of WhatsApp worldwide, are protected. An end to encryption would put those users at risk. As David Davis said in an article for the Financial Times in 2015, "Such a move would have had devastating consequences for all financial transactions and online commerce, not to mention the security of all personal data. Its consequences for the City do not bear thinking about".[8] It seems that the home secretary even faces disagreement on this issue from within her own party. The surveillance powers that the government have as a result of the Investigatory Powers Act are already among the most intrusive in the world. We must not allow their reach to continue to grow at the cost of privacy and security for everyone.

---

[6] UNESCO, 'Publishing in the Digital Age', UNESCO Series on Internet Freedom. http://www.unesco.org/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/protecting_journalism_sources_in_digital_age.pdf

7 Jonathan Haynes, 'Backdoor access to WhatsApp? Rudd's call suggests a hazy grasp of encryption', The Guardian, 27th March 2017. https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption

8 Alan Travis, 'Call for encryption ban pits Rudd against industry and colleagues', The Guardian, 26th March 2017. https://www.theguardian.com/technology/2017/mar/26/amber-rudd-battle-tech-firms-cabinet-whatsapp-david-davis