Experts challenge Govt's anti-encryption campaign

Leading cybersecurity experts and human rights activists say scaremongering tactics being used to mislead the public and make bogus case for weakening encryption. Over half a million pounds of taxpayers' money spent on advertising campaign.

The UK Home Office plans to force technology companies to remove the privacy and security of encrypted services such as WhatsApp and Signal as part of its Online Safety Bill. Even worse, the Home Office has launched a scaremongering campaign wasting hundreds of thousands of pounds on a London advertising agency to undermine public trust in a critical digital security tool to keep people and businesses safe online.

Undermining encryption would make our private communications unsafe, allowing hostile strangers and governments to intercept conversations. Undermining encryption would put at risk the safety of those who need it most. Survivors of abuse or domestic violence, including children, need secure and confidential communications to speak to loved ones and access the information and support they need. As Stephen Bonner, executive director for technology and innovation at the UK Information Commissioner's Office recently noted, end-to-end encryption "strengthens children's online safety by not allowing criminals and abusers to send them harmful content or access their pictures or location."[1]

Operation: Safe Escape[2] and LGBT Tech[3]—two organisations that represent and safeguard vulnerable stakeholders—stress the vital importance of encrypted communications victims of domestic abuse and for LGBTQ+ people in countries where they face harassment, victimisation and even the threat of execution. Far from making them safer, denying at-risk people a confidential lifeline puts them at greater and sometimes mortal risk.

Anti-encryption policies threaten the fundamental human right to freedom of expression. Compromising encryption would undermine investigative journalism that exposes corruption and criminality. According to the Centre for Investigative Journalism, without a secure means of communication, sources would go unprotected and whistleblowers will hesitate to come forward.[4]

Contrary to what the Home Office claims, leading cybersecurity experts conclude that even message scanning "creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic."[5] Backdoors create an entry point for hostile states, criminals and terrorists to gain access to highly sensitive information. Weakening encryption negatively impacts the global Internet[6] and means our private messages, sensitive banking information, personal photographs and privacy would be undermined. MI6 head, Richard Moore, used his first public speech to warn of the

1 https://www.infosecurity-magazine.com/news/privacy-tsar-defense-encrypti on/

2 https://safeescape.org/get-help/

3 https://www.lgbttech.org/post/lgbt-tech-internet-society-release-new-encryption-infographic

4 https://tcij.org/bespoke-training/information-security/

5 https://arxiv.org/abs/2110.07450

6 https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/

increased data security threat from hostile countries.[7] By Mr. Moore's analysis, the UK would be making things easier for hostile governments, in waging a war against our personal and national security.

The UK government must reassess their decision to wage war on a technology that is essential to so many people in the UK and beyond.

Signatories:

1. Access Now
2. ACLAC (Latin American and Caribbean Encryption Coalition)
3. Adam Smith Institute
4. Africa Media and Information Technology Initiative (AfriMITI)
5. Alec Muffett, Security Researcher
6. Annie Machon
7. ARTICLE19
8. Big Brother Watch
9. Centre for Democracy and Technology
10. Christopher Parsons, Senior Research Associate, Citizen Lab, Munk School of Global Affairs & Policy at the University of Toronto
11. Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
12. Cybersecurity Advisors Network (CyAN)
13. Dave Carollo, Product Manager, TunnelBear LLC
14. Derechos Digitales - Latin America
15. Digital Rights Watch
16. Dr. Duncan Campbell
17. Electronic Frontier Foundation
18. Faud Khan, CEO, TwelveDot Incorporated
19. Fundación Karisma
20. Global Partners Digital
21. Glyn Moody
22. Index on Censorship
23. Instituto de Desarrollo Digital de América Latina y el Caribe (IDDLAC)
24. Internet Society
25. Internet Society Brazil Chapter
26. Internet Society Catalonia Chapter
27. Internet Society Germany Chapter
28. Internet Society India Hyderabad
29. Internet Society Portugal Chapter
30. Internet Society Tchad Chapter
31. Internet Society UK England Chapter
32. Internet Freedom Foundation, India
33. JCA-NET (Japan)

7 https://www.bbc.com/news/uk-59470026

34. Jens Finkhaeuser, Interpeer Project
35. Prof. Dr. Kai Rannenberg, Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security
36. Kapil Goyal, Faculty Member, DAV College Amritsar
37. Khalid Durrani, PureVPN
38. Prof. Dr. Klaus-Peter Löhr, Freie Universität Berlin
39. LGBT Technology Partnership
40. Liberty
41. Luke Robert Mason
42. Mark A. Lane, Cryptologist, UNIX / Software Engineer
43. OpenMedia
44. Open Rights Group
45. Open Technology Institute
46. Peter Tatchell Foundation
47. Privacy & Access Council of Canada
48. Ranking Digital Rights
49. Reporters Without Borders
50. Riana Pfefferkorn, Research Scholar, Stanford Internet Observatory
51. Simply Secure
52. Sofía Celi, Latin American Cryptographers.
53. Dr. Sven Herpig, Director for International Cybersecurity Policy, Stiftung Neue Verantwortung
54. Tech For Good Asia
55. The Law and Technology Research Institute of Recife (IP.rec)
56. The Tor Project
57. Dr. Vanessa Teague, Australian National University
58. Yassmin Abdel-Magied