13 February 2025

To The Rt Hon Yvette Cooper MP,

The undersigned civil society organizations, companies, and cybersecurity experts, including members of the Global Encryption Coalition,[1] call on the UK Home Office to rescind its demand that Apple create a backdoor into its end-to-end encrypted services. This demand jeopardizes the security and privacy of millions, undermines the UK tech sector, and sets a dangerous precedent for global cybersecurity.

Reports indicate that the UK Government has issued a technical capability notice (or TCN) to Apple under the Investigatory Powers Act 2016 s.253 (IP Act). If all had gone according to plan, the UK government would have forced Apple to build a backdoor into its end-to-end encrypted cloud services. The world's second-largest provider of mobile devices would be built on top of a systemic security flaw, putting all of its users' security and privacy at risk, not just in the UK but globally.

The consensus among cybersecurity experts could not be clearer: there is no way to provide government access to end-to-end encrypted data without breaking end-to-end encryption, thus putting every user's security and privacy at risk.

Strong encryption keeps information and communication confidential. In a digital society, encryption is critical to safeguarding citizens both online and off, to protecting the digital economy, and to ensuring national security. In late January, the UK's National Audit Office released a report that the "cyber threat to the UK government is severe."[2] As Ciaran Martin, former Director and founder of the UK Government's National Cybersecurity Center notes "E2EE [end-to-end encryption] must expand, legally unfettered, for the betterment of our digital homeland."[3] With cyberattacks becoming ever-more frequent and sophisticated,[4] the reliance of the UK government, citizens, and businesses on end-to-end encryption to keep themselves safe and secure has never been greater.

The UK Government has stressed the importance of digital technologies to the UK's economic growth, but by forcing a company to secretly undermine the security of their product, the UK government risks foreign companies leaving the market and casting doubt on the security of products from UK tech companies. For some global companies, they may choose to leave the UK market rather than face the global reputational

1 https://www.globalencryption.org/about/members/

2 https://www.nao.org.uk/press-releases/cyber-threat-to-uk-government-is-severe-and-advancing-quickly-spending-watchdog-finds/

3 https://www.bsg.ox.ac.uk/sites/default/files/2021-11/End-to-end%20Encryption%20Ciaran%20Martin%20Blavatnik%20School.pdf

4 https://cyberscoop.com/salt-typhoon-us-government-jen-easterly-cisa/

risks that breaking the security of their products would entail. UK companies will also suffer reputational damage, as foreign investors and consumers will consider whether their products are riddled with secret UK government-mandated security vulnerabilities.

International human rights bodies have recognised the importance of end-to-end encryption to protect the right to privacy and to promote the exercise of other rights. This is because being able to communicate safely and securely can be a precondition to being able to communicate and express one's views. The case law of the European Court of Human Rights (ECtHR) recognises the importance of anonymity in "promoting the free flow of ideas and information in an important manner" including by protecting people from reprisals for their exercise of freedom of expression.[5] In February 2024, the ECtHR found that Russia's order issued to Telegram requiring it to disclose "technical information" including encryption keys breached human rights law, as it was not proportionate.[6]

Undermining the confidentiality of cloud services would have the most harmful impact on those already at greatest risk: families, domestic violence survivors,[7] LGBTQ+ individuals,[8] and many more who rely on the safety and privacy provided by end-to-end encrypted services. For these and other at-risk groups, the confidentiality guaranteed by end-to-end encryption can be critical in preventing harassment and physical violence.

Similarly, encrypted communications protect the UK's national security. Government services benefit from encryption and providing backdoors in one instance can lead to encryption being weakened across the ecosystem of the public sector, as well. For national security professionals and government employees, access to end-to-end encrypted services allows them to safeguard their personal life. Ensuring the security and privacy of government officials is vital for helping prevent extortion or coercion attempts, which could lead to greater national security damage.

To ensure the national and economic security of the United Kingdom, the Home Office must end its technical capability notice forcing Apple to break its end-to-end encryption.

---

[5] Delfi AS v Estonia [2015] EMLR 26, [147] and [149]: https://hudoc.echr.coe.int/eng#{"itemid":["001-155105"]}

[6] Podchasov v Russia [2024] ECHR 134 [79]: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

[7] https://www.internetsociety.org/wp-content/uploads/2021/05/NNEDV_Survivor_FactSheet-EN.pdf

[8] https://www.lgbttech.org/encryption-privacy-security

Global Encryption Coalition

Signatories*

3 Steps Data

Access Now

ARTICLE 19

AT Worthy Technology

Professor Subhajit Basu, School of Law, University of Leeds

Steven M. Bellovin, Columbia University

BETAPERSEI SC

Big Brother Watch

Bits of Freedom

British Columbia Civil Liberties Association

Ian Brown, Visiting Professor, Fundaçao Getulio Vargas Direito

Randy Bush, Internet Initiative Japan & Arrcus Inc

Jon Callas, Indiana University

Duncan Campbell, University of Sussex

Sofía Celi, Brave

Center for Democracy & Technology

Chaos Computer Club

Chayn

Richard Clayton, University of Cambridge

Andrew Clement, Faculty of Information, University of Toronto

Ben Collier, University of Edinburgh

Comunitatea Internet Association

Global Encryption Coalition

Community Focus Foundation Ghana

Cryptography Consulting LLC

Cybersecurity Advisors Network (CyAN)

cyberstorm.mu

Javier Ruiz Diaz, Associate, University of Sussex Centre for Law and Technology

Digital Rights Ireland

Zakir Durumeric, Stanford University

Egyptian Initiative for Personal Rights (EIPR)

Electric Coin Co.

Electronic Frontiers Australia Inc

Electronic Frontier Norway

Nicola Fabiano, Studio Legale Fabiano

Stephen Farrell, Trinity College Dublin

Filecoin Foundation

Foundation for Information Policy Research

Fundación Karisma

Simson L. Garfinkel, Association for Computing Machinery Technology Policy Committee

Gate 15

Global Partners Digital

Wendy M. Grossman, Author, net.wars

Masayuki Hatta, Surugadai University

Guy Herbert, NO2ID

Homo Digitalis

Global Encryption Coalition

Dr Monica Horten, Iptegrity.com

Dr Julian Huppert, University of Cambridge

International Civil Liberties Monitoring Group

Institute for Research on Internet and Society

Internet Society

Internet Society India Hyderabad Chapter

Internet Society Manitoba Chapter Inc.

Internet Society Portuguese Chapter

Internet Society Switzerland Chapter

Internet Society Tanzania Chapter

Internet Society UK England

Irish Council for Civil Liberties

ISOC Brazil - Brazilian Chapter of the Internet Society

ISOC-CAT Catalan Chapter

JCA-NET

David R. Jefferson

Kenya Human Rights Commission

Mallory Knodel, NYU

Susan Landau, Tufts University

Law and Technology Research Institute of Recife

Legal Resources Centre

LGBT Tech

Jean Linis-Dinco

Global Encryption Coalition

Michelle L. Mazurek, University of Maryland

Eran Messeri

Eric Mill

Kathleen Moriarty, SecurityBias

Alec Muffett, Security Researcher & Writer

Myntex

NetTek Ltd

OpenMedia

OPTF

Osservatorio Balcani Caucaso Transeuropa (OBCT)

Palmer Computer Services Inc.

Colin Perkins, University of Glasgow and Internet Research Task Force

Phoenix R&D

Prague Centre for Media Skills

Riana Pfefferkorn, Stanford University

Privacy & Access Council of Canada

Privacy International

Quilibrium Inc

Ronald L. Rivest, Insitute Professor, MIT

Bruce Schneier, Harvard Kennedy School

SECURECOM

SECURECRYPT

Wendy Seltzer

Global Encryption Coalition

Adam Shostack, author of Threat Modeling: Designing for Security

Kris Shrishak, ICCL - Enforce

Jessica Shurson, University of Sussex

SkypLabs

Software Freedom Law Center India (SFLC.IN)

Professor Peter Sommer, Birmingham City University

Eugene H. Spafford, Professor, Purdue University

Michael A. Specter, Georgia Institute of Technology

Surfshark

Tech for Good Asia

TEDIC

The Tor Project

The Zcash Foundation

Tuta Mail

Prof. J.W. Verret, George Mason University Antonin Scalia Law School

David Wagner, University of California, Berkeley

Kenneth White, Cryptography Engineer

Philip Zimmermann

*Affiliations listed for identification purposes only