Rt Hon Priti Patel MP
United Kingdom Secretary of State for the Home Department

William P. Barr
United States Attorney General

Chad F. Wolf
United States Secretary of Homeland Security (Acting)

Hon Peter Dutton MP
Australian Minister for Home Affairs

December 10, 2019

To Whom it May Concern,

The undersigned organizations, security researchers, and companies write to express significant concerns raised by your recent statements against encryption. In both the joint letter to Facebook and the event hosted by the Department of Justice on October 4, you described encrypted communications tools as "lawless spaces," and requested that companies remove or delay the deployment of end-to-end encryption protections on their consumer messaging services.

Fulfilling this request would endanger the security and privacy of billions of internet users around the world. Strong encryption is essential for national security and public safety, and exceptional access mechanisms—commonly referred to as "backdoors"—would create significant security risks. Finally, while law enforcement agencies have raised concerns about their capabilities in the face of strong encryption, crime-fighting capacity remains robust given that we are in an age where technology generates so much digital information about individuals and their activities.

Strong Encryption is Essential for National Security and Public Safety

Proponents of exceptional access have argued that it is possible to build backdoors into encrypted consumer products that somehow let "good actors" gain surreptitious access to encrypted communications, while simultaneously stopping "bad actors" from intercepting those same communications.

This technology does not exist. To the contrary, technology companies could not give governments backdoor access to encrypted communications without also weakening the security of critical infrastructure, and the devices and services upon which the national security and intelligence communities themselves rely.[1]

[1] "Policy Statement on Mandatory Engineered Law Enforcement Access to Information Infrastructure and Devices," Association for Computing Machinery U.S. Technology Policy Committee, April 12, 2018, https://www.acm.org/binaries/content/assets/public-policy/usacm/2018-usacm-statement-law-enforcement-access.pdf.

Critical infrastructure runs on consumer products and services, and is protected by the same encryption that is used in the consumer products that proponents of backdoor access seek to undermine. Every day, millions of people connect to critical infrastructure—the power grid, transportation systems, the financial system—via their phones or computers. Employees at these entities often connect to internal sites to manage operations or exchange sensitive information that enables the smooth operation of lifeline services. The same encryption present on smartphones and tablets protects these interactions, and is vital to the security of critical infrastructure.

Moreover, government employees around the world, including at intelligence agencies, rely on consumer devices to communicate sensitive information. In fact, the US National Security Agency (NSA) developed a program called Commercial Solutions for Classified that allows US Department of Defense officials to transmit classified information using commercial encryption solutions.[2]

Recognizing these serious risks, high ranking officials from national security, intelligence, and cybersecurity agencies have voiced opposition to calls for companies to build exceptional access mechanisms. For example, former NSA and CIA director, Michael Hayden, warned that "The downsides of a front or back door outweigh the very real public safety concerns," and Mike McConnell, former director of the NSA and former Director of National Intelligence, urged that "with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security." Former Secretary of Defense Ash Carter cautioned that "for the Department of Defense data security including encryption is absolutely essential to us. None of our stuff works unless it's connected...I'm not a believer in back doors."[3] Robert Hannigan, the former Director of the United Kingdom's GCHQ, responded to a proposed plan to mandate encryption backdoors by saying "Encryption is an overwhelmingly good thing—it keeps us all safe and secure…Building in back doors is a threat to everybody and it's not a good idea to weaken security for everybody to tackle a minority."[4]

Most recently, Jim Baker, former general counsel of the FBI, who served during the San Bernardino investigation and represented the FBI during its litigation against Apple, published an article in *Lawfare* describing his change of opinion on encryption issues. He explained how he now recognizes that "a solution that focuses solely on law enforcement's concerns will have profound negative implications for the nation across many dimensions. I am unaware of a technical solution that will effectively and simultaneously reconcile all of the societal interests at stake in the encryption debate, such as public safety, cybersecurity and privacy as well as simultaneously fostering innovation and the economic competitiveness of American companies in a global marketplace."[5]

All of these officials agree – weakening consumer encryption would unavoidably harm national security, and these concerns have borne out time and again. Major data breaches, such as those at the Office of Personnel Management[6], where millions of federal employees' records were exfiltrated by the Chinese

---

[2] "Four Future Trends in Tactical Network Modernization," U.S. Army, January 14, 2019, https://www.army.mil/article/216031/four_future_trends_in_tactical_network_modernization.
[3] "Encryption Backdoors are a Dangerous Idea," *New America's Open Technology Institute, Nov. 27, 2018,* https://www.newamerica.org/oti/blog/encryption-backdoors-are-dangerous-idea/.
[4] "Encryption Backdoors are a Dangerous Idea," *New America's Open Technology Institute, Nov. 27, 2018,* https://www.newamerica.org/oti/blog/encryption-backdoors-are-dangerous-idea/.
[5] Jim Baker, "Rethinking Encryption," *Lawfare*, October 22, 2019, https://www.lawfareblog.com/rethinking-encryption.
[6] "Report from the Committee on Oversight and Government Reform on the OPM Breach," Committee on Oversight and Government Reform, U.S. House of Representatives, available at

government, and at the Department of Defense[7], where 10-20 terabytes of records were leaked, show how vulnerable our data can be. The same is true of data breaches at hotel chains, health insurers, banks, credit reporting agencies, and universities, which affect hundreds of millions of people around the world every year.[8] Whether they are national security secrets or individuals' personal records, strong encryption is, by far, the best security solution we have for protecting those data from unauthorized access and exfiltration.

Encryption is also essential to public safety and protecting vulnerable populations. A common, but problematic, argument law enforcement officials make in favor of encryption backdoors is that we must be willing to compromise the privacy and security protections offered by encryption in order to protect public safety. However, this argument fails to acknowledge that encryption, in fact, plays an essential role in ***protecting*** the public from crimes that cause physical injury and death. For instance, Cindy Southworth, the Executive Vice President at the U.S. National Network to End Domestic Violence (NNEDV), recently cautioned against introducing an exceptional access mechanism for law enforcement, in part, because of how it could threaten the safety of victims of domestic and gender-based violence and stalking. Specifically, she explained that she is "a proponent of encryption because it allows victims to control when and how they seek help, and that it is critical for protecting sensitive digital records, which have been stolen by abusers."[9] A recent fact sheet from LGBT Tech and the Internet Society states "without encryption, LGBTQ+ individuals living in or traveling to [countries where being LGBTQ+ is considered a criminal offense] may not be able to safely and comfortably find communities and outlets for self-expression and would be left vulnerable to prosecution and persecution."[10]

Beyond protecting national security and physical safety, encryption is also essential to reduction of other types of crime. Mobile devices like smartphones and communications services like email providers and messaging apps are increasingly used by people and businesses as a primary means for accessing and communicating sensitive and proprietary information like financial data, medical records, and intellectual property, in addition to ordinary personal communications. Whether protecting data at rest or in motion, encryption is central to reducing cybercrime, fraud, data breaches, and device theft. As noted in the 2018 report of the Technological Advisory Council (TAC) Mobile Device Theft Prevention (MDTP) Working Group, a decline in mobile device theft coincides with the deployment of the anti-theft and security

---

https://archive.org/stream/ReportFromTheCommitteeOnOversightAndGovernmentReformOnTheOPMBreach/Report%20from%20the%20Committee%20on%20Oversight%20and%20Government%20Reform%20on%20the%20OPM%20Breach_djvu.txt.

[7] Linda Qiu, "Largest Cyber Attack in History? Huckabee Claims it's OPM, But it's Probably Not," *Politifact*, June 16, 2015, https://www.politifact.com/truth-o-meter/article/2015/jun/16/largest-cyber-attack-history-huckabee-claims-its-o/.

[8] Asha Barbaschow, "Over 10 Million People Hit in Single Australian Data Breach: OAIC," *ZDNet*, May 13, 2019, https://www.zdnet.com/article/over-10-million-people-hit-in-single-australian-data-breach-oaic/.

[9] "How Encryption Saves Lives and Fuels our Economy," New America, Nov. 27, 2018, https://www.newamerica.org/oti/events/how-encryption-saves-lives-and-fuels-our-economy/.

[10] "Encryption: Essential for the LGBTQ+ Community," Internet Society and LGBT Tech, November 1, 2019, available at https://www.internetsociety.org/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community/.

measures.[11]" If mobile device security was weakened by an encryption backdoor, the negative consequences to the economy and to data security would be unavoidable.

Exceptional Access Mechanisms Would Create Significant Security Risks

While some encryption opponents defend exceptional access by describing it as a "front door" rather than a "back door," this semantic argument only obscures the basic facts of their proposal. The outcome is the same, irrespective of terminology: law enforcement is asking companies to build a method of bypassing or weakening normal authentication processes that are essential to the security of encrypted communications. These exceptional access mechanisms for law enforcement agencies would be the same "backdoors" that provide an opportunity for terrorists, criminals, and other parties to gain unauthorized access. This is because technologists cannot build systems that are inherently able to tell when "bad" people use them, just as engineers cannot design sidewalks and highways to crumble underneath the feet of certain people. In both cases there is a chance that they would build something that is unsafe for all users. It is no different in communications infrastructure, and history has shown us that malicious actors will find and exploit vulnerabilities, whether created intentionally for law enforcement or left unintentionally by a software engineer.

Vulnerable populations like journalists and activists rely on encryption to protect themselves, their sources, and their communities.[12] For example, Chinese intelligence agencies have been exploiting a security failing in the encrypted messaging app Telegram to target activists in the recent Hong Kong protests.[13] A lack of digital security for these individuals can have real physical consequences. Governments with less respect for human rights take advantage of intentional vulnerabilities to surveil these populations, putting the vulnerable in danger absent the ability to communicate securely. In a recent example, Amnesty International supported a legal petition to revoke the export license of NSO Group, a company that has developed spyware products suspected of being used by law enforcement and/or intelligence agencies to exploit technical vulnerabilities to covertly take control of a person's phone, and which have been used against a number of human rights activists around the globe.[14] Exceptional access demands from countries such as the U.S., UK, and Australia also embolden repressive and authoritarian regimes in their attempts to pressure messaging apps and device manufacturers to build surveillance capabilities into their products and services.

---

[11]"Technological Advisory Council (TAC) Mobile Device Theft Prevention (MDTP) Working Group," available at https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2018/11.30.18-MDTP-WG-Report-and-Recommendations.pdf.

[12] Geoffrey King, "How Resistance to Encryption Jeopardizes Journalism," Committee to Protect Journalists, October 16, 2014, https://cpj.org/blog/2014/10/doj-resistance-to-encryption-jeopardizes-journalis.php.

[13] Zak Doffman, "Telegram Bug 'Exploited' By Chinese Agencies, Hong Kong Activists Claim," *Forbes*, August 25, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/25/chinese-agencies-crack-telegram-a-timely-warning-for-end-to-end-encryption/#239082e46342. Danny Vincent, "How Apps Power Hong Kong's 'Leaderless' Protests," June 30, 2019, https://www.bbc.com/news/technology-48802125.

[14] Dan Sabbagh, "Israeli Firm Linked to WhatsApp Spyware Attack Faces Lawsuit," *The Guardian*, May 18, 2019, https://www.theguardian.com/world/2019/may/18/israeli-firm-nso-group-linked-to-whatsapp-spyware-attack-faces-lawsuit.

For example, the Government Communications Headquarters (GCHQ), the U.K.'s intelligence agency, proposed an exceptional access mechanism that would involve adding a "ghost" user into encrypted chats so they could see the plaintext of the encrypted conversation.[15] This proposal would require messaging providers to add a law enforcement participant into encrypted chats and to suppress normal notifications to users, meaning users would be unaware when a law enforcement participant had been added. Although GCHQ officials claim that "you don't even have to touch the encryption" to implement their plan, the "ghost" proposal would pose serious threats to cybersecurity.

Among other problems, the "ghost" proposal would undermine authentication systems, so that people could no longer know who they were communicating with.[16] The ghost proposal would introduce a security threat to all users of a targeted encrypted messaging application. In order for providers to be able to suppress notifications when a ghost user is added, messaging applications would need to rewrite the software that every user relies on. This means that the development of this new function could create an unintentional vulnerability that affects every single user of that application. Proposals to build backdoors into encrypted devices have shown similar fatal flaws that could result in malicious exploitation of the vulnerability, or otherwise harm non-targeted users.[17]

The flaws in these proposals highlight another concern with the direction the "going dark" debate has taken. Law enforcement officials advocating for exceptional access have begun suggesting that building such a mechanism would be possible if companies and users would sacrifice just a small percentage of their digital security, going from 99.5% secure to 99% secure.[18] This assertion, that exceptional access would result in a miniscule and measurable—and therefore manageable—loss in security, runs counter to a wealth of evidence produced by numerous studies.[19]

Strong Encryption Will Not Unreasonably Hobble Law Enforcement Investigations

One of the most common justifications cited in support of restrictions on encryption is the overwhelming barriers that it poses to law enforcement investigators. This common claim has repeatedly been shown to be overstated. During the *Apple v. FBI* litigation, the FBI claimed that relevant and critical communications data resided on a locked phone that they could not access due to encryption.[20] A subsequent Office of Inspector General report detailed that the FBI did not diligently pursue all options for accessing data on

---

[15] Ian Levy, Crispin Robinson, "Principles for a More Informed Exceptional Access Debate," *Lawfare*, November 29, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.
[16] Open Coalition Letter to GCHQ Regarding the "Ghost" Proposal, May 22, 2019, available at https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.
[17] Matthew Green, "A few thoughts on Ray Ozzie's "Clear" Proposal," *A Few Thoughts on Cryptographic Engineering*, April 26, 2018, https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/.
[18] Attorney General William P. Barr, "Keynote Address at the International Conference on Cyber Security,"New York, NY, Tuesday, July 23, 2019, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.
[19] Abelson, Harold, Ross Anderson, Steven M. Bellovin, et al, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Computer Science and Artificial Intelligence Laboratory Technical Report*, 2015, available at https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.
[20] Aaron Pressman, "The Secret History of the FBI's Battle Against Apple Reveals the Bureau's Mistakes," Fortune, March 27, 2018, https://fortune.com/2018/03/27/fbi-apple-iphone-encryption-san-bernardino/.

the locked phone, and instead chose to sue Apple to compel the company to develop a workaround that would have circumvented the security on all their devices.[21] Moreover, press reporting has made it known that after the FBI unlocked the phone by hiring a private contractor, it contained no useful data.[22]

In addition in 2017, the FBI tried to illustrate the impact of encryption on law enforcement when it told Congress that it had seized 7,800 phones that were inaccessible due to encryption. In 2018, this figure was contradicted when an internal FBI estimate of 1,200 phones became public. The FBI committed to providing a revised number, but has not yet done so.

Moreover, a survey of law enforcement investigators shows that encryption is not the biggest digital evidence challenge they face. In fact, the problem is often much simpler—police officers don't know what data is available, which provider has it, and how to go about acquiring and making sense of it. According to the Center for Strategic & International Studies, their survey of federal, state, and local law enforcement officials "suggests that challenges in accessing data from service providers—much of which is not encrypted—is the biggest problem that they currently face in terms of their ability to use digital evidence in their cases."[23] In fact, there is an enormous amount of unencrypted data available to law enforcement today that has not been available in the past. For example, encryption typically does not protect metadata, and therefore poses no barrier for law enforcement agents to access information like email addresses, mobile-device location information, IP address, browsing data, and other information that can be extremely valuable to investigators.[24]

In practice, if companies build law enforcement access mechanisms into encrypted products, some targets of investigations will simply move to using different encrypted services. Thus, while any of the small number of nefarious actors who are targeted by law enforcement will still be able to avail themselves of other services, the vast majority of users who are law-abiding—who may still choose different services—will disproportionately suffer the consequences of degraded security and trust.

As former FBI General Counsel Jim Baker wrote in his recent piece on *Rethinking Encryption,* public safety officials should consider protecting cybersecurity an essential part of their mission, and therefore, "public safety officials should embrace encryption." We urge you to similarly rethink your calls for exceptional access and to recognize the important role encryption plays in keeping us all safe.

Sincerely,

---

[21] Office of the Inspector General U.S. Department of Justice, "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation," March, 2018, available at https://oig.justice.gov/reports/2018/o1803.pdf.
[22] Russell Brandom, "The FBI has gotten no new leads from the San Bernardino iPhone," *The Verge,* April 19, 2016, https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads.
[23] William A. Carter and Jennifer C. Daskal, "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," *Center for Strategic and International Studies*, July 2018, available at https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN.
[24] Zittrain, Jonathan L., Matthew G. Olsen, David O'Brien, and Bruce Schneier. 2016. "Don't Panic: Making Progress on the "Going Dark" Debate." Berkman Center Research Publication 2016-1, available at https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Civil Society Organizations

Access Now
American Civil Liberties Union
Amnesty International
ARTICLE 19
Association for Computing Machinery U.S. Technology Policy Committee
Berkman Klein Center for Internet & Society
Blueprint for Free Speech
Center for Democracy & Technology
CETYS Center for Law and Society San Andres University (Buenos Aires, Argentina)
Committee to Protect Journalists
Constitutional Alliance
DATAS | Technology Governance
Defending Rights & Dissent
Derechos Digitales
Demand Progress
Digital Empowerment Foundation (DEF)
Digital Liberty
Digital Rights Watch
EIT
Electronic Frontier Foundation
Electronic Frontiers Australia
Engine
Freedom of the Press Foundation
Future of Privacy Forum
Global Forum for Media Development
Global Partners Digital
Human Rights Watch
Index on Censorship
Information Technology and Innovation Foundation (ITIF)
Instituto Beta para Internet e Democracia
International Civil Liberties Monitoring Group
Internet Society
Internews
IPANDETEC Centroamérica
Irish Council for Civil Liberties
Kenya Human Rights Commission
LGBT Technology Partnership & Institute
Linux Australia
National Association of Data Protection Officers of the Philippines (NADPOP)
New America's Open Technology Institute
Observatorio de Derecho Informático Argentino (ODIA)
OpenMedia
Open Rights Group

Privacy International
Prostasia Foundation
Ranking Digital Rights
Reporters Without Borders (RSF)
Restore The Fourth
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
S.T.O.P. - The Surveillance Technology Oversight Project
TechFreedom
TEDIC - Paraguay
X-Lab

Technology Companies and Trade Associations

ACT | The App Association
BaysNet
Computer & Communications Industry Association
Ensignia P/L
Private Internet Access
Rakuten Viber
Wipro

Security and Policy Experts*

Adam Shostack, author Threat Modeling: Designing for Security
Adam Holland, Project Manager, Berkman Klein Center for Internet & Society
Amie Stepanovich
Aria Shanker
Ben Parkinson, Chief Information Security Advisor, SecureWorx
Bruce Schneier
Cameron Kerry, former General Counsel & Acting Secretary, U.S. Commerce Dept.
Corch, Managing Director, Shogun Cybersecurity
Declan Finlay
Domen Savič, Državljan D
Garrett Schumacher, MS; Director of Communications and Strategy; Lecturer; Technology, Cybersecurity and Policy Program; University of Colorado Boulder
Hal Abelson, Professor of Computer Science and Engineering, Massachusetts Institute of Technology
Helaine Leggat, Board Member Australian Information Security Association (AISA)
Jabir Jonuzi
James Munro, Cybersecurity Consultant
Jeffrey J. Blatt, Founder, X Ventures
Jon Callas
Kate Carruthers
Katie McAuliffe, Executive Director, Digital Liberty
Malcolm Gregory
Maon Catzel, ISC2 Associate
Mark Kahn, Former Deputy General Counsel of WhatsApp
Matthew D. Green, Associate Professor, Computer Science Department, Johns Hopkins University

Michael Hardlee, Senior Solutions Consultant, Team Lead
Michael Kafoa, MISM CISSP CRISC, Information Security Advisor
Mike Godwin, Trustee, Internet Society
Rafe Hart
Riana Pfefferkorn, Stanford Center for Internet and Society
Dr. Richard Forno, Senior Lecturer, UMBC
Rik Farrow, Editor, USENIX
Robert Marazzato, CISSP
Rob McDowall, Equality Council
Russell Border
Sam Hitchiner
Sascha Meinrath, Director, X-Lab, Palmer Chair in Telecommunications, Penn State University
Simon Smith, eVestigator
Simon Stahn, Adrenalan
Steve Wildman, former FCC Chief Economist
Dr. Suelette Dreyfus, Academic Specialist, School of Computing and Information Systems, University of Melbourne
Sven Herpig, Stiftung Neue Verantwortung (SNV)
Theo Karner
Vikas Raina

*Affiliations provided for identification purposes only