Open Letter to GCHQ

Government Communications Headquarters
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

May 22, 2019

To Whom It May Concern:

The undersigned organizations, security researchers, and companies write in response to the proposal published by Ian Levy and Crispin Robinson of GCHQ in *Lawfare* on November 29, 2018, entitled "Principles for a More Informed Exceptional Access Debate."[1] We are an international coalition of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online; security researchers with expertise in encryption and computer science; and technology companies and trade associations, all of whom share a commitment to strong encryption and cybersecurity. We welcome Levy and Robinson's invitation for an open discussion, and we support the six principles outlined in the piece. However, we write to express our shared concerns that this particular proposal poses serious threats to cybersecurity and fundamental human rights including privacy and free expression.

The six principles set forth by GCHQ officials are an important step in the right direction, and highlight the importance of protecting privacy rights, cybersecurity, public confidence, and transparency. We especially appreciate the principles' recognition that governments should not expect "unfettered access" to user data, that the "trust relationship" between service providers and users must be protected, and that "transparency is essential."

Despite this, the GCHQ piece outlines a proposal for "silently adding a law enforcement participant to a group chat or call." This proposal to add a "ghost" user would violate important human rights principles, as well as several of the principles outlined in the GCHQ piece. Although the 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 and thereby also threaten fundamental human rights, including privacy and free expression. In particular, as outlined below, the ghost proposal would create digital security risks by undermining authentication systems, by introducing potential unintentional vulnerabilities, and by creating new risks of abuse or misuse of systems.[2] Importantly, it also would undermine the GCHQ principles on user trust and transparency set forth in the piece.

---

[1] Ian Levy and Crispin Robinson, "Principles for a More Informed Exceptional Access Debate," *Lawfare*, Nov. 29, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate. Levy is the Technical Director of the National Cyber Security Centre (NCSC) and Robinson is the technical director for cryptanalysis at GCHQ. The NCSC is the part of GCHQ that is responsible for protecting the U.K.'s critical services from cyber attacks, managing major cyber incidents, and improving the underlying security of the internet.

[2] Davis, Terry and Peha, Jon M. and Burger, Eric William and Camp, L. Jean and Lubar, Dan, Risking it All: Unlocking the Backdoor to the Nation's Cybersecurity (2014). Available at SSRN: https://ssrn.com/abstract=2468604 or http://dx.doi.org/10.2139/ssrn.2468604.

How the Ghost Proposal Would Work

The security in most modern messaging services relies on a technique called “public key cryptography.” In such systems, each device generates a pair of very large mathematically related numbers, usually called “keys.” One of those keys – the public key – can be distributed to anyone. The corresponding private key must be kept secure, and not shared with anyone. Generally speaking, a person’s public key can be used by anyone to send an encrypted message that only the recipient’s matching private key can unscramble. Within such systems, one of the biggest challenges to securely communicating is authenticating that you have the correct public key for the person you’re contacting. If a bad actor can fool a target into thinking a fake public key actually belongs to the target’s intended communicant, it won’t matter that the messages are encrypted in the first place because the contents of those encrypted communications will be accessible to the malicious third party.

Encrypted messaging services like iMessage, Signal, and WhatsApp, which are used by well over a billion people around the globe, store everyone’s public keys on the platforms’ servers and distribute public keys corresponding to users who begin a new conversation. This is a convenient solution that makes encryption much easier to use. However, it requires every person who uses those messaging applications to trust the services to deliver the correct, and **only** the correct, public keys for the communicants of a conversation when asked.

The protocols behind different messaging systems vary, and they are complicated. For example, in two-party communications, such as a reporter communicating with a source, some services provide a way to ensure that a person is communicating only with the intended parties. This authentication mechanism is called a “safety number” in Signal and a “security code” in WhatsApp (we will use the term “safety number”). They are long strings of numbers that are derived from the public keys of the two parties of the conversation, which can be compared between them – via some other verifiable communications channel such as a phone call – to confirm that the strings match. Because the safety number is per pair of communicators — more precisely, per pair of keys — a change in the value means that a key has changed, and that can mean that it’s a different party entirely. People can thus choose to be notified when these safety numbers change, to ensure that they can maintain this level of authentication. Users can also check the safety number before each new communication begins, and thereby guarantee that there has been no change of keys, and thus no eavesdropper. Systems without a safety number or security code do not provide the user with a method to guarantee that the user is securely communicating only with the individual or group with whom they expect to be communicating. group with whom they expect to be communicating. Other systems provide security in other ways. For example, iMessage, has a cluster of public keys – one per device – that it keeps associated with an account corresponding to an identity of a real person. When a new device is added to the account, the cluster of keys changes, and each of the user’s devices shows a notice that a new device has been added upon noticing that change.

The “ghost key” proposal put forward by GCHQ would enable a third party to see the plain text of an encrypted conversation without notifying the participants. But to achieve this result, their proposal requires two changes to systems that would seriously undermine user security and trust. First, it would require service providers to surreptitiously inject a new public key into a conversation in response to a government demand. This would turn a two-way conversation into a group chat where the government is the additional participant, or add a secret government participant to an existing group chat. Second, in order to ensure the government is added to the conversation in secret, GCHQ’s proposal would require messaging apps, service providers, and operating systems to change their software so that it would 1)

change the encryption schemes used, and/or 2) mislead users by suppressing the notifications that routinely appear when a new communicant joins a chat.

The Proposal Creates Serious Risks to Cybersecurity and Human Rights

The GCHQ's ghost proposal creates serious threats to digital security: if implemented, it will undermine the authentication process that enables users to verify that they are communicating with the right people, introduce potential unintentional vulnerabilities, and increase risks that communications systems could be abused or misused. These cybersecurity risks mean that users cannot trust that their communications are secure, as users would no longer be able to trust that they know who is on the other end of their communications, thereby posing threats to fundamental human rights, including privacy and free expression. Further, systems would be subject to new potential vulnerabilities and risks of abuse.

Integrity and Authentication Concerns

As explained above, the ghost proposal requires modifying how authentication works. Like the end-to-end encryption that protects communications while they are in transit, authentication is a critical aspect of digital security and the integrity of sensitive data. The process of authentication allows users to have confidence that the other users with whom they are communicating are who they say they are. Without reliable methods of authentication, users cannot know if their communications are secure, no matter how robust the encryption algorithm, because they have no way of knowing who they are communicating with. This is particularly important for users like journalists who need secure encryption tools to guarantee source protection and be able to do their jobs.[3]

Currently the overwhelming majority of users rely on their confidence in reputable providers to perform authentication functions and verify that the participants in a conversation are the people they think they are, and only those people. The GCHQ's ghost proposal completely undermines this trust relationship and the authentication process.

Authentication is still a difficult challenge for technologists and is currently an active field of research. For example, providing a meaningful and actionable record about user key transitions presents several known open research problems,[4] and key verification itself is an ongoing subject of user interface research.[5] If, however, security researchers learn that authentication systems can and will be bypassed by third parties like government agencies, such as GCHQ, this will create a strong disincentive for continuing research in this critical area.

---

[3] Reporters Without Borders, "World Press Freedom Index 2019," available at: https://rsf.org/en/ranking/2019.

[4] Marcela Melara, "Why Making Johnny's Key Management Transparent is So Challenging," March 31, 2016 https://freedom-to-tinker.com/2016/03/31/why-making-johnnys-key-management-transparent-is-so-challenging/

[5] Kemal Bicakci et al, "How Safe Is Safety Number? A User Study on SIGNAL's Fingerprint and Safety Number Methods for Public Key Verification", August 15, 2018 https://link.springer.com/chapter/10.1007/978-3-319-99136-8_5

Potential for Introducing Unintentional Vulnerabilities

Beyond undermining current security tools and the system for authenticating the communicants in an encrypted chat, GCHQ's ghost proposal could introduce significant additional security threats. There are also outstanding questions about how the proposal would be effectively implemented.

The ghost proposal would introduce a security threat to all users of a targeted encrypted messaging application since the proposed changes could not be exposed only to a single target. 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 any mistake made in the development of this new function could create an unintentional vulnerability that affects every single user of that application.

As security researcher Susan Landau points out, the ghost proposal "involves changing how the encryption keys are negotiated in order to accommodate the silent listener, creating a much more complex protocol—raising the risk of an error."[6] (That actually depends on how the algorithm works; in the case of iMessage, Apple has not made the code public.) A look back at recent news stories on unintentional vulnerabilities that are discovered in encrypted messaging apps like iMessage,[7] and devices ranging from the iPhone[8] to smartphones that run Google's Android operating system,[9] lend credence to her concerns. Any such unintentional vulnerability could be exploited by malicious third parties.

Possibility of Abuse or Misuse of the Ghost Function

The ghost proposal also introduces an intentional vulnerability. Currently, the providers of end-to-end encrypted messaging applications like WhatsApp and Signal cannot see into their users' chats. By requiring an exceptional access mechanism like the ghost proposal, GCHQ and U.K. law enforcement officials would require messaging platforms to open the door to surveillance abuses that are not possible today.

At a recent conference on encryption policy, Cindy Southworth, the Executive Vice President at the U.S. National Network to End Domestic Violence (NNEDV), 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. Specifically, she warned that "[w]e know that not only are victims in every profession, offenders are in every profession...How do we keep safe the victims of domestic

---

[6] Susan Landau, "Exceptional Access: The Devil is in the Details," *Lawfare,* Dec. 26, 2018, https://www.lawfareblog.com/exceptional-access-devil-details-0#

[7]Ellen Nakashima, "Johns Hopkins Researchers Poke a Hole in Apple's Encryption," *Washington Post,* Mar. 21, 2016, https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccdbc5f74e_story.html?utm_term=.2485b9a99233

[8] "The Cat-and-Mouse Game Between Apple and the Manufacturer of an iPhone Unlocking Tool," *Motherboard,* April 18, 2018, https://motherboard.vice.com/en_us/article/ne95pg/apple-iphone-unlocking-tool-graykey-cat-and-mouse-game

[9] Brian Barrett, "Millions of Android Devices are Vulnerable Right Out of the Box," *Wired,* Aug. 10 2018, https://www.wired.com/story/android-smartphones-vulnerable-out-of-the-box/

violence and stalking?"[10] Southworth's concern was that abusers could either work for the entities that could exploit an exceptional access mechanism, or have the technical skills required to hack into the platforms that developed this vulnerability.

While companies and some law enforcement and intelligence agencies would surely implement strict procedures for utilizing this new surveillance function, those internal protections are insufficient. And in some instances, such procedures do not exist at all. In 2016, a U.K. court held that because the rules for how the security and intelligence agencies collect bulk personal datasets and bulk communications data (under a particular legislative provision) were unknown to the public, those practices were unlawful.[11] As a result of that determination, it asked the agencies - GCHQ, MI5, and MI6 - to review whether they had unlawfully collected data about Privacy International. The agencies subsequently revealed that they had unlawfully surveilled Privacy International.[12]

Even where procedures exist for access to data that is collected under current surveillance authorities, government agencies have not been immune to surveillance abuses and misuses despite the safeguards that may have been in place. For example, a former police officer in the U.S. discovered that "104 officers in 18 different agencies across the state had accessed her driver's license record 425 times, using the state database as their personal Facebook service."[13] Thus, once new vulnerabilities like the ghost protocol are created, new opportunities for abuse and misuse are created as well.[14]

Finally, if U.K. officials were to demand that providers rewrite their software to permit the addition of a ghost U.K. law enforcement participant in encrypted chats, there is no way to prevent other governments from relying on this newly built system. This is of particular concern with regard to repressive regimes and any country with a poor record on protecting human rights.

The Proposal Would Violate the Principle That User Trust Must be Protected

The GCHQ proponents of the ghost proposal argue that "[a]ny exceptional access solution should not fundamentally change the trust relationship between a service provider and its users. This means *not* asking the provider to do something fundamentally different to things they already do to run their business."[15] However, the exceptional access mechanism that they describe in the same piece would

---

[10] Remarks by Cindy Southworth, Executive Vice President, U.S. National Network to End Domestic Violence (NNEDV) at public forum "How Encryption Saves Lives and Fuels our Economy," Nov. 27, 2018, recording available at: https://www.newamerica.org/oti/events/how-encryption-saves-lives-and-fuels-our-economy/

[11] Privacy International, "BPD/BCD: IPT Judgment October 2016", Oct. 17, 2016, https://privacyinternational.org/feature/1694/bpdbcd-ipt-judgment-october-2016.

[12] Privacy International, "Press Release: UK Intelligence Agency Admits Unlawfully Spying on Privacy International," Sept. 25, 2018, https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy

[13] Kim Zetter, "Cops Trolled Driver's License Database for Pic of Hot Colleague," *Wired,* Feb. 23, 2012, https://www.wired.com/2012/02/cop-database-abuse/

[14] Nate Cardozo, "Give up the Ghost: A Backdoor by Another Name," *Just Security,* Jan. 4, 2019, https://www.justsecurity.org/62114/give-ghost-backdoor/

[15] Ian Levy and Crispin Robinson, "Principles for a More Informed Exceptional Access Debate," *Lawfare*, Nov. 29, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

have exactly the effect they say they wish to avoid: it would degrade user trust and require a provider to fundamentally change its service.

The moment users find out that a software update to their formerly secure end-to-end encrypted messaging application can now allow secret participants to surveil their conversations, they will lose trust in that service. In fact, we've already seen how likely this outcome is. In 2017, the *Guardian* published a flawed report in which it incorrectly stated that WhatsApp had a backdoor that would allow third parties to spy on users' conversations. Naturally, this inspired significant alarm amongst WhatsApp users, and especially users like journalists and activists who engage in particularly sensitive communications. In this case, the ultimate damage to user trust was mitigated because cryptographers and security organizations quickly understood and disseminated critical deficits in the report,[16] and the publisher retracted the story.[17]

However, if users were to learn that their encrypted messaging service intentionally built a functionality to allow for third-party surveillance of their communications, that loss of trust would understandably be widespread and permanent. In fact, when President Obama's encryption working group explored technical options for an exceptional access mechanism, it cited loss of trust as the primary reason not to pursue "provider-enabled access to encrypted devices through current update procedures." The working group explained that this could be dangerous to overall cybersecurity, since "its use could call into question the trustworthiness of established software update channels. Individual users aware of the risk of remote access to their devices, could also choose to turn off software updates, rendering their devices significantly less secure as time passed and vulnerabilities were discovered [but] not patched."[18] While the proposal that prompted these observations was targeted at operating system updates, the same principles concerning loss of trust and the attendant loss of security would apply in the context of the ghost proposal.

Any proposal that undermines user trust penalizes the overwhelming majority of technology users while permitting those few bad actors to shift to readily available products beyond the law's reach. It is a reality that encryption products are available all over the world and cannot be easily constrained by territorial borders.[19] Thus, while the few nefarious actors targeted by the law will still be able to avail themselves of other services, average users -- who may also choose different services -- will disproportionately suffer consequences of degraded security and trust.

The Ghost Proposal Would Violate the Principle That Transparency is Essential

Although we commend GCHQ officials for initiating this public conversation and publishing their ghost proposal online, if the U.K. were to implement this approach, these activities would be cloaked in secrecy. Although it is unclear which precise legal authorities GCHQ and U.K. law enforcement would rely upon,

---

[16] Zeynec Tufekci, "In Response to Guardian's Irresponsible Reporting on WhatsApp: A Plea for Responsible and Contextualized Reporting on User Security," http://technosociology.org/?page_id=1687
[17] "Flawed Reporting About WhatsApp," *Guardian,* June 28, 2017, https://www.theguardian.com/technology/commentisfree/2017/jun/28/flawed-reporting-about-whatsapp
[18] "Read the Obama Administration's Draft Paper on Technical Options for the Encryption Debate, *Washington Post,* Sept. 24, 2015, http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/
[19] Bruce Schneier, Kathleen Seidel & Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," Feb. 11, 2016, https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

the Investigatory Powers Act grants U.K. officials the power to impose broad non-disclosure agreements that would prevent service providers from even acknowledging they had received a demand to change their systems, let alone the extent to which they complied. The secrecy that would surround implementation of the ghost proposal would exacerbate the damage to authentication systems and user trust as described above.

Conclusion

For these reasons, the undersigned organizations, security researchers, and companies urge GCHQ to abide by the six principles they have announced, abandon the ghost proposal, and avoid any alternate approaches that would similarly threaten digital security and human rights. We would welcome the opportunity for a continuing dialogue on these important issues.

Sincerely,

Civil Society Organizations

Access Now

Big Brother Watch

Blueprint for Free Speech

Center for Democracy & Technology

Defending Rights and Dissent

Electronic Frontier Foundation

Engine

Freedom of the Press Foundation

Government Accountability Project

Human Rights Watch

International Civil Liberties Monitoring Group

Internet Society

Liberty

New America's Open Technology Institute

Open Rights Group

Principled Action in Government

Privacy International

Reporters Without Borders

Restore The Fourth

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

TechFreedom

The Tor Project

X-Lab

Technology Companies and Trade Associations

ACT | The App Association

Apple

Google

Microsoft

Reform Government Surveillance (RGS is a coalition of technology companies)

Startpage.com

WhatsApp

Security and Policy Experts*

Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science; Affiliate faculty, Columbia Law School

Jon Callas, Senior Technology Fellow, ACLU

L Jean Camp, Professor of Informatics, School of Informatics, Indiana University

Stephen Checkoway, Assistant Professor, Oberlin College Computer Science Department

Lorrie Cranor, Carnegie Mellon University

Zakir Durumeric, Assistant Professor, Stanford University

Dr. Richard Forno, Senior Lecturer, UMBC, Director, Graduate Cybersecurity Program & Assistant Director, UMBC Center for Cybersecurity

Joe Grand, Principal Engineer & Embedded Security Expert, Grand Idea Studio, Inc.

Daniel K. Gillmor, Senior Staff Technologist, ACLU

Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab

Dr. Christopher Parsons, Senior Research Associate at the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

Phillip Rogaway, Professor, University of California, Davis

Bruce Schneier

Adam Shostack, Author, Threat Modeling: Designing for Security

Ashkan Soltani, Researcher and Consultant - Former FTC CTO and Whitehouse Senior Advisor

Richard Stallman, President, Free Software Foundation

Philip Zimmermann, Delft University of Technology Cybersecurity Group

**Affiliations are for identification purposes only*

CC: Sir Adrian Fulford
Investigatory Powers Commissioner
Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU