28th of April, 2022

Dear European Commission President Ursula von der Leyen,
Dear Executive Vice-President Margrethe Vestager,
Dear Vice-President Věra Jourová,
Dear Vice-President Dubravka Šuica,
Dear Commissioner Ylva Johansson,
Dear Commissioner Thierry Breton,
Dear Commissioner Margaritis Schinas,

cc:

Commission President Head of Cabinet Bjoern Seibert;
Commission President Digital Adviser Anthony Whelan;
Executive Vice-President Vestager;
Head of Cabinet Kim Jørgensen;
Deputy Head of Cabinet Christiane Canenbley;
Vice-President Jourová;
Head of Cabinet Renate Nikolay;
Deputy Head of Cabinet Daniel Braun;
Vice-President Šuica;
Head of Cabinet Colin Scicluna;
Deputy Head of Cabinet Deša Srsen;
Commissioner Johansson;
Head of Cabinet Åsa Webber;
Deputy Head of Cabinet Tom Snels;
Commissioner Breton;
Head of Cabinet Valère Moutarlier;
Deputy Head of Cabinet Lucía Caldet;
Commissioner Schinas;
Head of Cabinet Despina Spanou;
Deputy Head of Cabinet Natasha Bertaud

Open letter and statement of support from business entities, industry associations, IT professionals, privacy, data protection, cyber security, and other experts operating across Europe and Globally.

Protecting rights and freedoms in the Legislation to effectively tackle child abuse

As business entities, industry associations, IT professionals, privacy, data protection, cyber security, and other experts operating across Europe and globally, we are joining together to reaffirm the call from civil society organisations to ensure the full protection of fundamental rights and freedoms in the upcoming EU Legislation to effectively tackle child abuse.[1]

The 2021 EU short-term ePrivacy derogation allowed a number of independent interpersonal communications providers to scan private messages for child sexual abuse material (CSAM); however, the upcoming EU proposal to replace the ePrivacy derogation would compel all providers to scan all private communications for the purpose of detecting CSAM.[2]

Generalised detection practices can threaten the rights to privacy and data protection of all users of a service. Last year, experts around the world highlighted how Apple's plans for monitoring all photos on Apple devices, as well as iMessage accounts belonging to children, risked "setting a precedent where our personal devices become a radical new tool for invasive surveillance, with little oversight to prevent eventual abuse and unreasonable expansion of the scope of surveillance.[3]"

Fortunately, Apple recognised the significant risks their plans would create. After agreeing with critics from around the world, Apple shelved the plan.[4]

Cybersecurity experts across the globe have detailed how client-side scanning methods like the one proposed by Apple create "serious security

and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic.[5]"

Other techniques for protecting private data — such as Steganography[6] — easily allow malicious actors to evade PhotoDNA and other detection systems, rendering their use ineffective and security assurances misleading. Furthermore, independent statistics on the accuracy and reliability of these tools are seriously lacking, while legislative changes to break Encryption[7] have been widely criticised, including by a United Nations Special Rapporteur[8] and an Australian Federal Police Commander[9]

The privatisation of law enforcement responsibilities to investigate and report the sharing of CSAM will not make the internet safer for young people. It will, however, eliminate private environments that are vital for free expression and democracy.

Providers compelled to scan for CSAM might be forced to use inaccurate or experimental tools — that create additional cyber security risks, weaken or undermine encryption, and facilitate significant harm. Similarly, mandatory routine examination would compromise the vital private communication services that providers offer their users, leading to a wide range of serious risks and harms, undermining trust in these services (regardless, whether or not the provider offers encrypted or unencrypted messaging services).

CSAM detection technologies disrupt Cryptography and/or Steganography, and will also impede national security, individuals, business entities, governments, domestic and international security agencies, as computing power increases — yet it will be unable to detect radical, hateful, or child sexual abuse material concealed by Cryptography and/or Steganography, or other techniques. Modern-day encryption methods like Cryptography and Steganography[6] are used by individuals, business entities, governments, domestic and international security agencies to prevent the harvesting of sensitive data by domestic and foreign adversaries.

Client-side content-scanning technologies capture, store, and classify steganographic images in ways that allow adversaries to exploit the images and potentially gain access to the embedded data — making it easy for adversaries to expose the sensitive data and jeopardise the privacy of individuals, governments, and business entities.

In effect, the use of client-side scanning would enable adversarial actors to break encryption.

As the EU Agency for Cybersecurity, ENISA, asserts:

> "***If you encrypt data that needs to be kept confidential for more than 10 years and an attacker could gain access to the cipher text, you need to take action now to protect your data. Otherwise, security will be compromised as soon as the attacker also gets access to a large quantum computer.***[10]"

Similar warnings are made by authorities including the US White House[11] and Department for Homeland Security[12], the United Nations International Telecommunications Union Telecommunication Standardisation Sector (ITU-T)[13] and many other cyber security experts who specialise in Post-Quantum Cryptography / Steganography solutions.

- Cryptography[17]
  - Symmetric Ciphers : Encrypting any data type
    - OpenSSL : AES 128 - 256 Bit Keys[14]
    - QRCrypto : eAES(R) 256 - 1024 Bit Keys[15]
    - FooCrypt <= 200 layers of Symmetric Ciphers per run time[16]

- Steganography[6] : Embedding any data type
  - FooSteg[16]
    - <= Infinity Bit Strength, In-Situ and/or In Transit[16]
    - Quantum+ Secure / Proof[16]

Commissioner for Home Affairs Ylva Johnasson, who is responsible for this legislation to effectively tackle child abuse, assured Members of the European Parliament (MEPs) on the 9th of March, 2022, that:

> ***"I would finally like to recall again the commitment made by the Commission to consider solutions that would not prohibit or generally weaken encryption. The Commission is not considering proposing any mechanisms or solutions in its proposal that will break this commitment."***[2]

The EU and its allies must avoid introducing mandatory detection requirements that, by necessity and definition, threaten Cryptography and Steganography, thereby undermining all users privacy and data protection rights.

Encryption is vital in modern societies for protecting individuals, industries and governmental security and privacy.[17] Many of the scanning methods that service providers will be compelled to use under the new legislation will break Commissioner Johansson's commitment not to undermine encryption — and instead will threaten the fundamental core of encryption.

The undersigned business entities, industry associations, IT professionals, privacy, data protection, cyber security, and other experts operating across Europe and globally welcome the legal certainty that can be provided by the legislation to effectively tackle child abuse, and;

- We urge the European Commission to ensure that imposed obligations are genuinely proportionate, closely targeted, and protect the sanctity of privacy and of private communications as a fundamental tenet of all democratic societies, and;

- We affirm that it would be appropriate for the European Union to reconsider its technical solutions, due to their significant and profoundly negative impacts on current Cryptography and Steganography solutions, and;

- We urge the European Commission to recognise the critical importance of Cryptography and Steganography in protecting the privacy of individuals, entities and governments, not only for today, but also in the Post Quantum Era.

Signed,

The International Chat Control v2 Working Group

Mark A. Lane (Australia)
Sharon Polsky MAPP (Canada)
Stiepan A. Kovac (Switzerland)

Web : https://ChatControlv2.EU/Contributors
Email : ICCWG@ChatControlv2.Info

In conjunction with current signatories @ https://chatcontrolv2.eu/signatories/

Bolch Webworks

Cryptopocalypse : https://foocrypt.xyz

Encryption Europe : https://www.encryptioneurope.eu

FooCrypt : https://foocrypt.xyz

FooCrypt, A Tale of Cynical Cyclical Encryption : https://foocrypt.xyz

Giordano-Bruno-Stiftung : https://giordano-bruno-stiftung.de

Global Institute for Structure relevance, Anonymity and Decentralisation i.G. : https://gisad.eu

Hellmich IT

Lang IT

mailbox.org : https://mailbox.org

Neue Richtervereinigung e.V. : https://www.neuerichter.de

Nitrokey GmbH : https://www.nitrokey.com

Privacy & Access Council of Canada (PACC) : https://pacc-ccap.ca

Simply Secure : https://simplysecure.org

Statewatch : https://www.statewatch.org

Tutanota : https://tutanota.com

Alexander Leonhardt

Alex Stephan

Andreas Hellmich

André Uckel

Anna Egold

Benjamin Zielke

Christian Pelka

Daniel Laber

David Bruder

Denis Debroize

Dominik Lenhardt : https://lenhardt.cc

Dominik Wenninger

Dr. Arne Babenhauserheide

Endres Puschner : https://mpi-sp.org

Fabian Stens

Felix Düring

Felix Lang

Florian Gmeinwieser

Florian Menzel

Florian W

Franca Schmitt

Herr huer Hær

Hyrum Davis

Jacques Schneider

Jan Schnitker

Jonas Görgen

Jonas Hochstrat

Jorim Ben Kowalewski

Julius Hackel

Korbinian Bonauer

Lea Berberich

Marco Hellmann

Marius Janzetic

Mark A. Lane : https://www.linkedin.com/in/fookey

Maximilian Hengl

Maximilian Pluskat

Mirjan Junge

Ole Seifert

Oliver Pifferi : https://pifferi.info

Oliver Welz

Prof. Dr. Klaus-Peter Löhr

Rafael Sundorf

Ralph Klenke

Recke Silvio

Rene Lutz

Robert Saade

Robin Gentz

Sebastian Schiessl

Simon Reichle

Simon Steinmetz

Sotiris Ehmann

Tobias Conze

Tobias Hoge

Tobias Joachimsmeyer

And in perpetuity, with ongoing signatories located @ https://chatcontrolv2.eu/signatories/

References

1. https://edri.org/our-work/protecting-digital-rights-and-freedoms-in-the-legislation-to-effectively-tackle-child-abuse/
(EDRi : Open letter: Protecting digital rights and freedoms in the Legislation to effectively tackle child abuse)

2. https://twitter.com/echo_pbreyer/status/1503327511480086529
(Tweet : 10:09 PM · Mar 14, 2022 : @echo_pbreyer
Dr. Patrick Breyer, Europaabgeordneter/Member of the European Parliament)

3. https://appleprivacyletter.com/
(An Open Letter Against Apple's Privacy-Invasive Content Scanning Technology)

4. https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf
(Apple's CSAM Detection : technical Summary. August. 2021)

5. https://arxiv.org/abs/2110.07450
(Bugs in our Pockets: The Risks of Client-Side Scanning. 14th of October, 2021)

6. https://www.youtube.com/watch?v=GPdIY6ObKJU
(National Security Agency : National Cryptologic Museum | Introduction to Steganography)

7. https://youtu.be/ADg7x2Buw0s?t=72s
(End-to-End Encryption: What is it and why is it important ? | Dr. Vanessa Teague, Dr. Chris Culnane)

8. https://news.un.org/en/audio/2015/06/601622
(UN Special Rapporteur David Kaye)

9. https://youtu.be/4V9cPHq4TZw?t=2881s
(AI in Law Enforcement | Monash Tech Talks | Doug Boudry - Commander, Australian Federal Police)

10. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
(ENSIA : European Union Agency For CyberSecurity : Post-Quantum Cryptography: Current state and quantum mitigation)

11. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/?s=09
(USA White House : President JOSEPH R. BIDEN JR. Memorandum : January 19, 2022)

12. https://www.dhs.gov/quantum & https://www.dhs.gov/publication/memorandum-preparing-post-quantum-cryptography
(USA : Homeland Security : Post Quantum Cryptography Statement & Memorandum)

13. https://www.itu.int/rec/T-REC-X.1811-202104-P & https://www.itu.int/rec/T-REC-X.1714/en
(United Nations, International Telecommunications Union : Quantum Safe Algorithms & Quantum Key Distribution Networks, Standards)

14. https://wiki.openssl.org/index.php/Enc
(OpenSSL Cryptography and SSL/TLS Toolkit)

15. https://QRCrypto.ch
(Quantum Safe Mobile Encryption Technology)

16. https://FooCrypt.XYZ/White_Paper
(FooCrypt, A Tale of Cynical Cyclical Encrypt, A Quantum+ Secure / Proof, Cryptography and Steganography Software Solution)

17. https://rwc.iacr.org/2022/
(International Association For Cryptographic Research, Real World Crypto, April 13-15 2022. Amsterdam)