6 October 2020

Subject: European Digital Rights (EDRi) views on encryption

Dear staff members of the German Presidency,

We are writing you to provide written feedback on behalf of European Digital Rights (EDRi) on the LIMITE document 10728/20 published by Statewatch: https://www.statewatch.org/media/1352/eu-council-security-despite-encryption-10728-20.pdf

1. Introduction and executive summary

The German Presidency of the Council has asked for input on encryption policy. This is EDRi's response. In summary:

- European citizens, businesses, and governments rely on encryption to safeguard their data and resources. This is why European governments have supported the widespread use of encryption since the 1990s.
- In the face of broad deployment of full-disk and end-to-end encryption, and pressure from the US government, this position appears to be shifting. Some specific proposals have been made: covertly inserting a government participant to secure chats, detecting sexual child abuse material on user devices before these are shared, and allowing access to device encryption by governments, when a legal process has been followed.
- The German Presidency states that all proposals should not weaken the encryption used, or insert backdoors. But these three proposals all have the same effect of making users vulnerable to unlawful access. And they would inevitably be abused by governments that do not respect human rights.
- At the same time, we live in a "golden age of surveillance", where more information about individuals is collected than ever before. This far outweighs the possible loss of information by the wider use of encryption.
- The European Union should therefore fully embrace encryption. Encryption must become the default: software companies should be obliged to apply it where possible (as is strongly suggested by the GDPR). The use of freely available, open encryption protocols should become even more standard than it already is. Europe must further invest in the development of strong encryption and related software.

Europe must oblige governments to notify security vulnerabilitiesin encryption technologies. And lastly, it must abandon plans to weaken information security measures.

EDRi has already published several analyses of encryption policy. It has published a paper on encryption workarounds, explaining how law enforcement can retain access to information, even in the face of strong encryption (Annex 1). And it has published a paper setting out its position on encryption, noting that high-grade encryption is essential for our economy and our democratic freedoms (Annex 2). As the debate has developed since, EDRi would like to draw the German Presidency's attention to the following additional points.

2. Everyone uses encryption to protect information

Encryption is vital to Europe's information society. Governments use it, for example to protect highly political matters from leaking: internal deliberations on the Brexit talks would be less candid without strong encryption. Law enforcement uses encryption, for example, in the Dutch police's internal communication system C2000.[1]
Companies and other organisations use it, for example to restrict internal access to communications, to ensure that data is less likely to be breached when a laptop is lost; to defend against attacks on IT systems, including critical infrastructure such as industrial control systems; and to securely communicate with other organisations and customers. E-commerce depends on secure communications: the explosion of online financial transactions in the past decades could only happen due to strong encryption. Europe's world-leading banking infrastructure would be impossible without the application of strong encryption measures.
And everyone else uses it. These are ordinary citizens who want to make sure their pictures remain secure if they lose their phone. These are people with a special confidentiality obligation, such as journalists, lawyers and doctors, who must ensure that what they discuss remains secret. These are people who have to fear their government, from gay people in several African nations, to NGOs in Russia and activists in Hong Kong.

3. This is why EU governments support encryption

This is why European policymakers support encryption, for example as measures that are mandatory to consider under the GDPR, the ePrivacy rules, and the European Electronic Communications Code.[2] The Dutch government furthermore took a strong position on of

1 See C2000 communication system for emergency services, https://www.government.nl/topics/counterterrorism-and-national-security/c2000-communication-system-for-emergency-services

2 GDPR , Art. 32(1)(a), rec. 83, Art. 6(4)(e), and Art. 34(3)(a); ePrivacy Directive, rec. 40, 96 and 97; EECC Art. 40(1) . See further ENISA, Recommended cryptographic measures. Securing personal data, 2013; and EDPB Response to MEP Moritz Körner regarding the relevance of encryption bans in third countries, June 2020.

encryption in 2016, considering it impossible to weaken encryption for law enforcement and intelligence agencies, without compromising the security of digital systems in general. The Dutch government therefore did not consider it desirable to take restrictive measures relating to the development, availability and use of encryption in the Netherlands.[3] Similarly, the German government since 1999 has embraced strong principles on encryption, including that there will be no ban or limitation on encryption products, that encryption products shall be tested for their security to increase users' trust, and that the development of German encryption products is essential for the country's security.[4]

But two developments appear to be driving a change in this position. The application of full-disk encryption is in many cases becoming the default in consumer devices, such as smartphones and laptops. And end-to-end encryption – e.g. encryption used in communications where only the parties to the communication are able to decrypt and read messages – is applied in widely used chat services, including WhatsApp and Signal. Moreover, Facebook intends to add this to its Messenger and Instagram chat.

4. Proposed restrictions still make everyone vulnerable

In response, the German Presidency is reconsidering its hands-off approach, while attempting to address concerns about backdoors: "the weakening of encryption by any means (including backdoors) is not a desirable option". EDRi assumes this is because such measures affect not only those under investigation but to everyone using encryption.

Encryption technologies do not function in isolation, but are part of a system many of whose components provide an avenue for weakening the information security available to users. Restrictions on these systems, even if not directed towards the encryption technologies as such, still make every user of the system more vulnerable. Therefore**, the Presidency should not take measures which weaken information security measures for all users, whether in the encryption algorithm, implementation, operating system, or any other components.**
For example:

- The UK's GCHQ intelligence agency has proposed to covertly add participants (e.g. law enforcement or intelligence agencies) to chats, suggesting this is more targeted, only affecting the individuals under investigation. This is incorrect: covertly adding chat participants requires changing the software for *all* users by making it impossible for users to get a true picture of which other users are party to a call or

3 See Kamerbrief over kabinetsstandpunt encryptie, 4 January 2016, https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie
4 See Sven Herpig and Stefan Heumann, *The Encryption Debate in Germany*, https://carnegieendowment.org/2019/05/30/encryption-debate-in-germany-pub-79215

a chat, thus placing every user at risk of surveillance and undermining the confidence of all.

- Similarly, the recent proposal to filter child sexual abuse material on user devices is also intended to circumvent the effect of encryption. But again, this requires changing the software for all users, introducing new avenues for access which directly undermine trust by introducing real-time censorship into communications that users expect to be private.
- Lastly, it has been suggested that operating-system full-disk encryption implementations is weakened, to allow for access by governmental agencies when legally authorised (e.g Apple providing access to an encrypted iPhone). Again, this would require changing the encryption implementation, so as to provide a key to an organisation other than the user. This carries similar risks as above.

These measures all expose users to the risks of unlawful access. First, third parties will have to maintain the code or keys that give governments access to encrypted information. These repositories will be hacked. The US National Security Agency (NSA) broke into French SIM card producer Gemalto to gain access to all its encryption keys, and TLS certificate provider Diginotar was hacked to gain access to fake TLS certificates, with Iranian intelligence services as a likely culprit. NSA also managed to lose control of vulnerabilities it found in Windows, which were then exploited by two of the most devastating attacks on information systems in history (WannaCry and NotPetya), leading to many billions of euros of damage. Microsoft's General Counsel Brad Smith commented:

> *"We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage.... This most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action."*[5]

Second, secure implementation is very difficult, and this added complexity will make the software more vulnerable. It is already very difficult to create cryptographic protocols which are secure; to implement these securely in software is even more difficult; to then allow exceptional access securely to third parties is nearly impossible. Putting companies in charge of identifying the best solution for securing government access to encrypted information will not work when no acceptable technological solution exists. In addition, existing software would have to be 'updated' in order to change the current encryption implementations. In reality this would be a forced downgrade, which would undermine

5 The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack Microsoft on the Issues, 14 May 2017.

trust in vendors in particular and security updates in general. And lastly, insider threats cannot be excluded. Corrupt police or intelligence officers selling keys to criminals or foreign governments are a real risk.
But these solutions also pose significant issues regarding lawful access. All these technologies are deployed globally. A lawful access regime will thus have a global impact. But many regimes which do not respect human rights use lawful access options. Can regimes such as China and Russia gain access to this functionality? And if so, under what circumstances may they gain access? Can China use it to investigate the Uyghur community or dissidents in Hong Kong?

6. Meanwhile, we live in a golden age of surveillance

Fortunately, governments do not have to restrict information security measures, in order to retain access to information in law enforcement and intelligence investigations. While some information may have become less accessible as a result of encryption technologies in last decade, other sources of information for investigations have grown exponentially. We refer to the discussion of how we are living in "golden age of surveillance" in our previous reports (Annex 1 and 2).

Moreover, organised crime has moved to digital messaging, some of which are advertised as being secure. As a result, law enforcement has had success gaining access to badly protected services, reading large volumes of messages exchanged by criminals (see the EncroChat and Ennetcom investigations).[6] The aforementioned cases underline that law enforcement so far has gained more than it lost by the move of most human activities online. If anything, the problem facing law-enforcement agencies is that their existing digital forensic tools and capabilities cannot keep up with the cornucopia of data that are already lawfully available to them.

7. The EU should embrace encryption

Given the important role that encryption plays for privacy, communications freedom, politics and commerce, the European Union should fully embrace encryption:

- Encryption must become the norm: software companies should be obliged to apply it by default where possible (as already suggested in EU law).
- The use of freely available, open protocols should become the norm.
- Europe must further invest in the development of strong encryption and related software.

6 See European Police Malware Could Harvest GPS, Messages, Passwords, More, https://www.vice.com/en/article/k7qjkn/encrochat-hack-gps-messages-passwords-data and Info on dozens of criminal cases found on PGP phones, https://nltimes.nl/2019/01/30/info-dozens-criminal-cases-found-pgp-phones

- Europe must also invest in the development of better tools for digital forensics so that investigators can make proper use of material to which they have lawful access.
- Europe must oblige governments to notify security vulnerabilities, including in encryption technologies, in order to protect the public .
- And lastly, it must abandon plans to weaken other information security measures, via the components in which encryption is embedded and on which it relies.

Sincerely,

Diego Naranjo
Head of Policy
European Digital Rights (EDRi)
diego.naranjo@edri.org