The Encryption Dilemma:

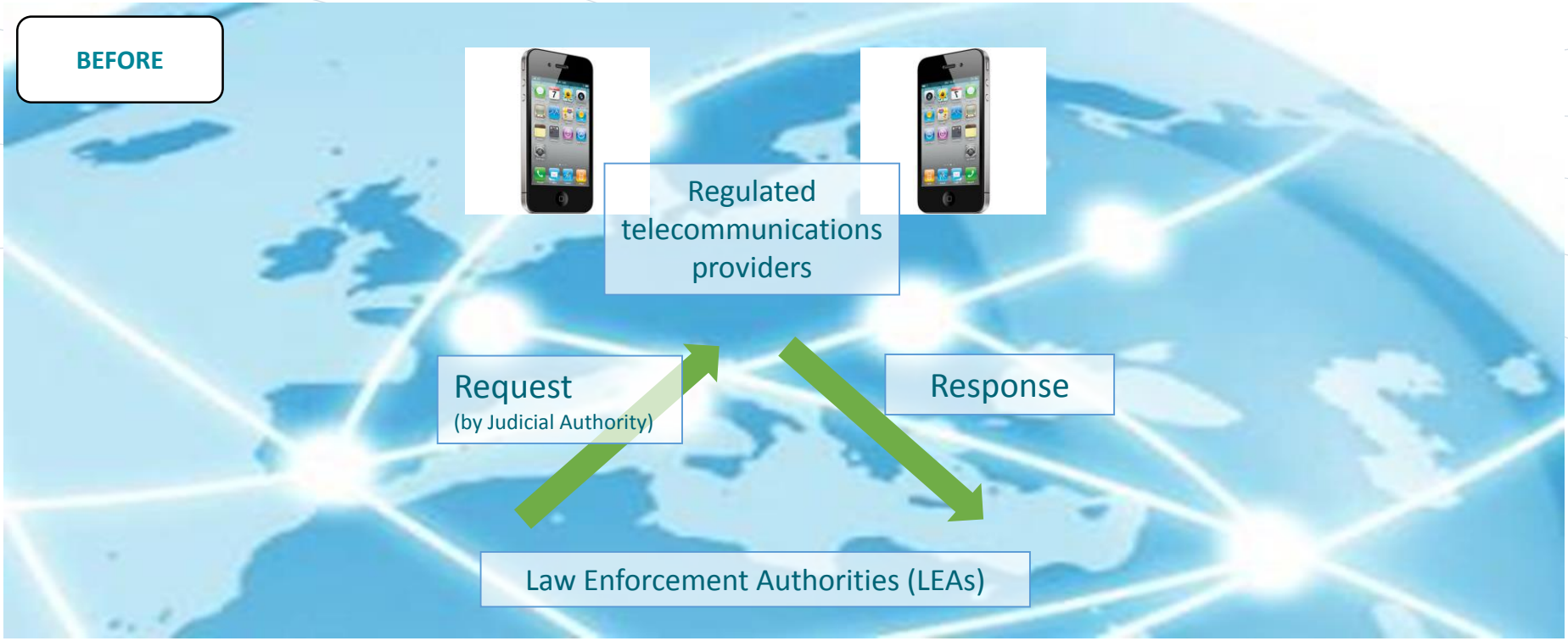
A European perspective

CEPS
26 October 2017

THINK DIGITAL – REFORM – PROSPER

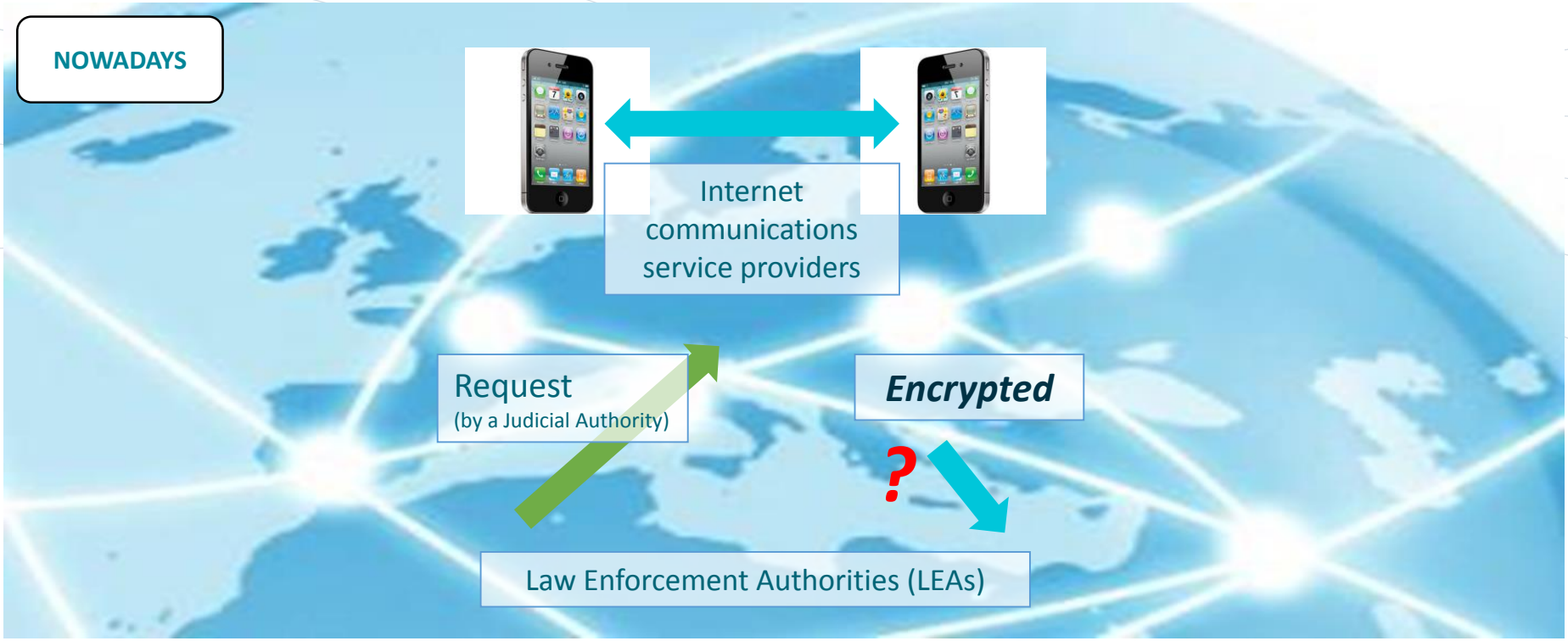
etno

In the fight against crime, the legal interception of communications has always been vital



etno

However, new communications services and current encryption make former procedures unworkable



etno

However, new communications services and current encryption make former procedures unworkable

This situation has already happened

Brazil

17th December 2015

- A judge in Sao Paolo **ordered telecommunications operators to block *WhatsApp*** because no cooperation on a drug traffic investigation. *WhatsApp* does not have an office in Brazil so the judge's order was delivered to cellphone operators.

2nd May 2016

- A regional judge **ordered telecommunications operators to block *WhatsApp*** messaging service for failing to cooperate in a criminal investigation.

7th July 2016

- A judge in Rio de Janeiro **ordered telecommunications operators to block *WhatsApp*** after did not turn over user data requested by authorities as part of a criminal investigation.

WhatsApp

"As we've said in the past, we cannot share information we don't have access to."

(a *WhatsApp* spokesperson in a public statement).

CONSEQUENCES

to justice:

- Judges's anger
- Criminal investigations harmed

to customers:

- 100 millions users affected

to market:

- The blame falls on ISPs
- More than 6 millions new users of other instant messaging services in one day (*Viver* & *Telegram*)

etno

Encryption on instant messages shows the trend: users will be the only ones who have the key for de-encryption

NO ENCRYPTION

- Anyone can intercept the messages, and even change them

➢ **Lack of privacy, confidentiality and security**

ENCRYPTION

- Messages are processed and **stored** in providers' infrastructure

➢ **Privacy depends on providers' infrastructure security**

➢ **Storage requirements for providers**

END-TO-END ENCRYPTION

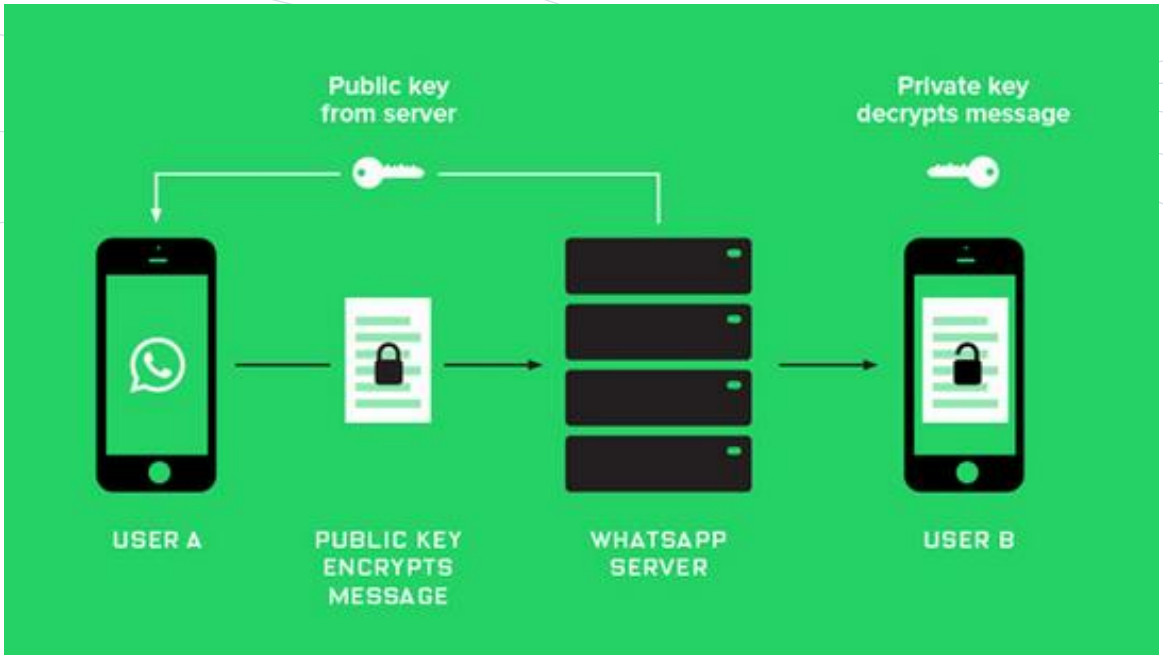
- Messages are processed in each customers' device, though not stored in providers' infrastructure
- Providers can not de-encrypt messages, nor store them

➢ **LEAs & Courts will not be able to interpret intercepted messages**

etno

End-to-End encryption makes impossible the interception

Provider can or not store messages, although **“could not” de-encrypt** the stored messages



The **messages in clear only** “live” really **in the terminals…**

that’s why FBI is so interested in unblocking terminals…

Governments push encrypted communications to be the norm, or not…

Germany Wants to Become Encryption Site Number One

Posted on: 2015-12-08

In November, the Interior Minister of Germany, Thomas De Maizière, signed a charta to strengthen confidential communication online. This charta states that is supports and promotes strong end-to-end encryption. While around the world surveillance measures are on the rise, Germany become 'Encryption Site Number One'.

This is great news for Tutanota, and we welcome the in taken by the German government. It is good to see tha are politicians who understand the importance of our r privacy.

End-to-end encryption shou become the standard

- **Encryption** is **essential** to keep **privacy**
- **End-to-end encryption** will become the **standard**
- **Freedom** should **prevail** over surveillance

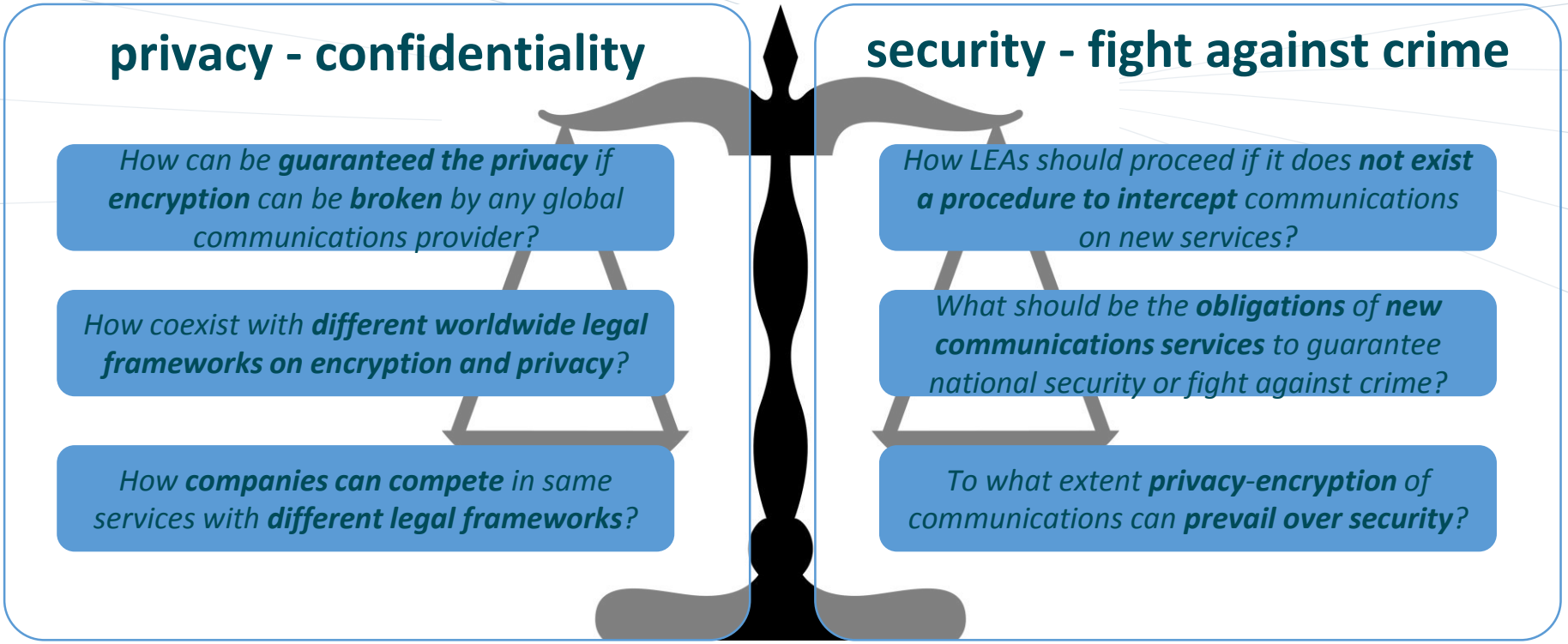
Encryption under fire in Europe as France and Germany call for decrypt law

Posted Aug 24, 2016 by Natasha Lomas (@riptari)

A fresh chapter of the crypto wars looks to be opening up in Europe, after the French and German interior ministers took to a podium yesterday to lobby for a law change that would enable courts to demand that Internet companies decrypt data to help further criminal investigations.

etno

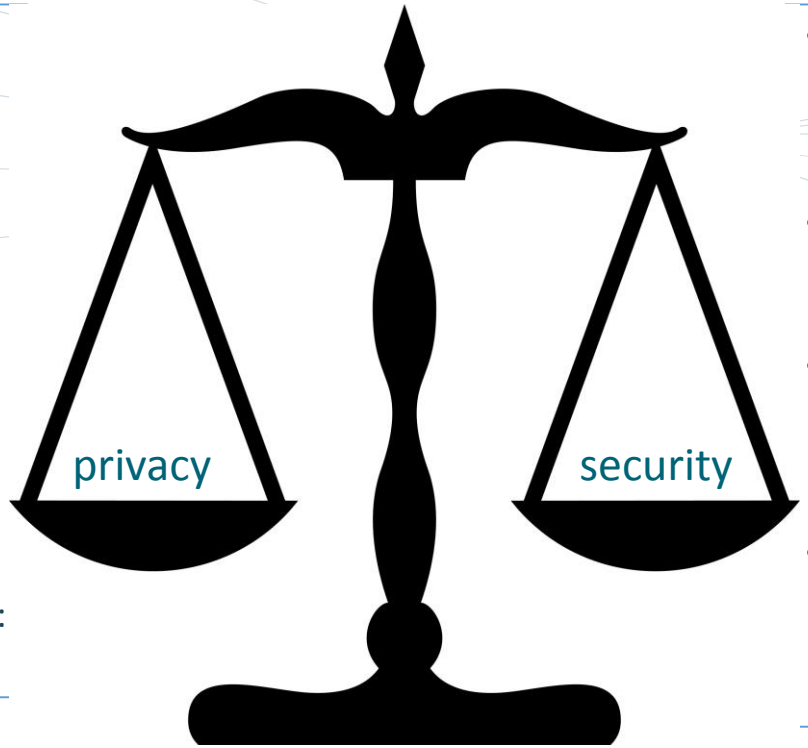
Encryption opens (again) the debate on privacy versus security



etno

Encryption should be in the balanced equation among privacy rights and security

- Data privacy as a Fundamental Right: protection of privacy via à vis Authorities and Governments
- Encryption as a common procedure: protection of privacy vis à vis companies and wrongdoers
- User friendliness of services: keep the current agility



- LEAs and judicial requests: based on criminal investigations and not in mass surveillance
- Possibility of de-encryption: define procedures to allow de-encryption
- Same rules for all companies: do not apply different requirements to companies that can affect competition
- Availability of services: without technical requirements that make them impossible to deploy

etno