

Encryption: What's the Problem?

Victoria Baines, IT Livery Company Professor of IT







SWEET
TALK

PUPPY
LOVE

SWEET
PEA

FIRST
KISS

XOXO

HUG
ME

TRUE
LOVE

ME +
YOU

SWEET
PEA

FOR
ME









"If he had anything
confidential to say, he
wrote it in cipher, that is,
by so changing the order
of the letters of the
alphabet, that not a word
could be made out."

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	V
X	Y	Z	A	B



F	W	Q	B	P
I	A	Z	T	K
E	C	O	X	H
R	L	Y	G	N
M	U	D	V	S







La machine de Vigenère

La machine de Vigenère est une machine à rotor qui utilise une table de Vigenère pour chiffrer et déchiffrer les messages. Elle est considérée comme l'un des premiers chiffreurs mécaniques.

Le principe de la machine de Vigenère est basé sur l'addition et la soustraction de lettres. Le message à chiffrer est combiné avec une clé secrète (le mot de passe) pour produire le message chiffré.

La machine de Vigenère est une machine à rotor qui utilise une table de Vigenère pour chiffrer et déchiffrer les messages. Elle est considérée comme l'un des premiers chiffreurs mécaniques.

Le principe de la machine de Vigenère est basé sur l'addition et la soustraction de lettres. Le message à chiffrer est combiné avec une clé secrète (le mot de passe) pour produire le message chiffré.

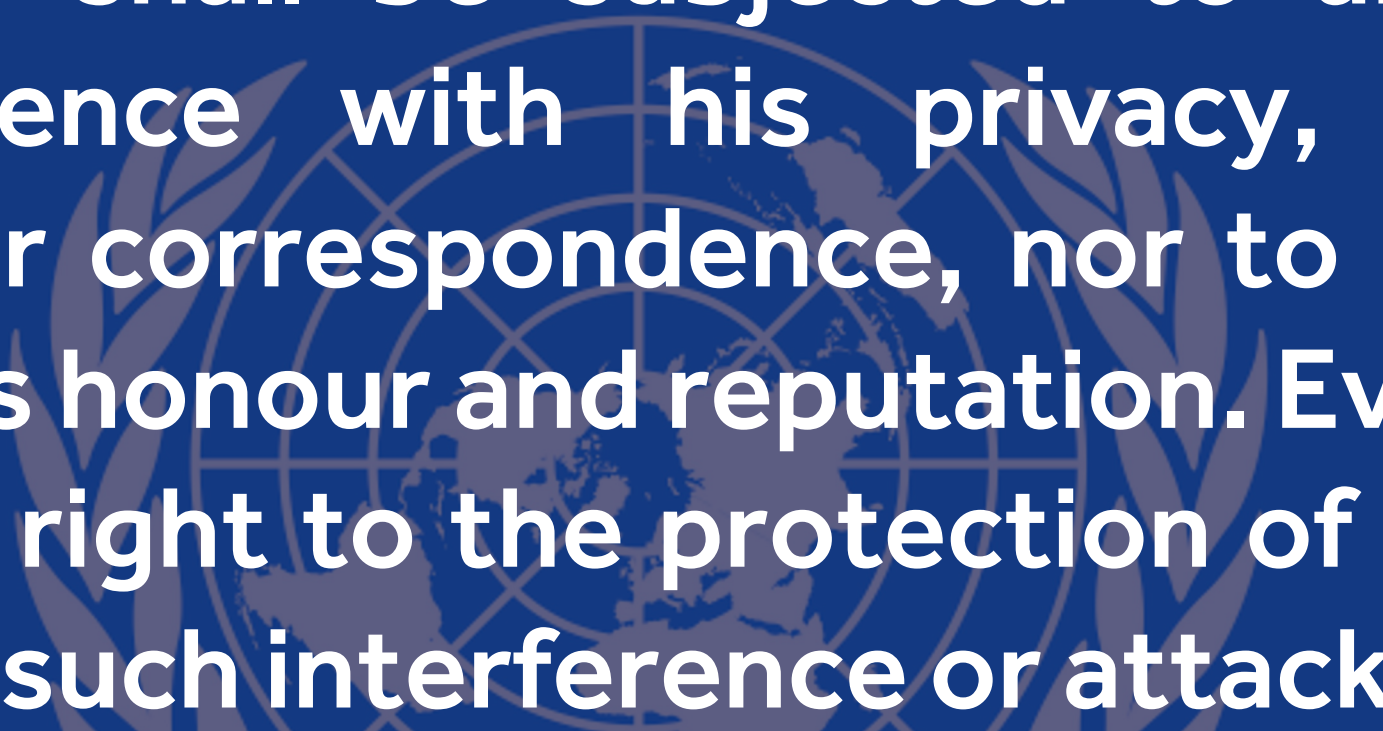


"If you have
nothing to hide..."



...you have
nothing to fear."





No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Universal Declaration of Human Rights, Article 12



1. Everyone has the right to respect for his private and family life, his home and his correspondence.

European Convention on Human Rights, Article 8



2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security,...

European Convention on Human Rights, Article 8



...public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

European Convention on Human Rights, Article 8





Fig. 1a: Encryption in transit

Image: Martin Kleppmann

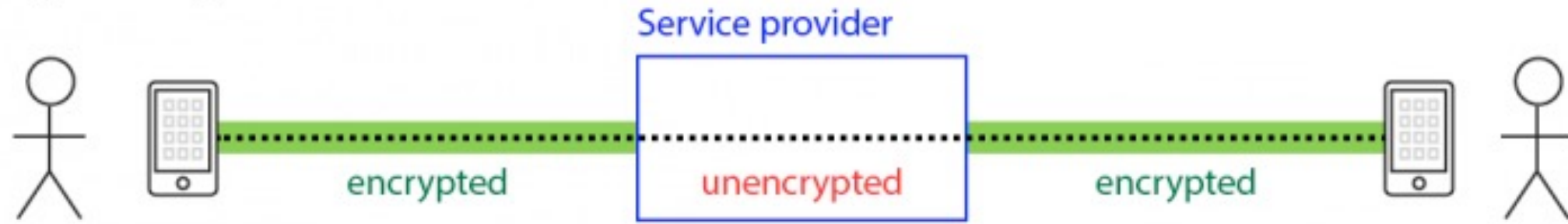


Fig. 1b: End-to-end encryption

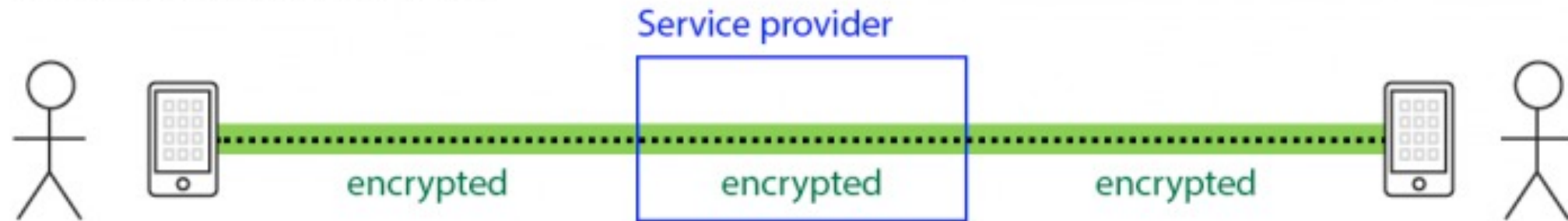


Fig. 1c: End-to-end encryption (no service provider)



Fig. 1a: Encryption in transit

Image: Martin Kleppmann

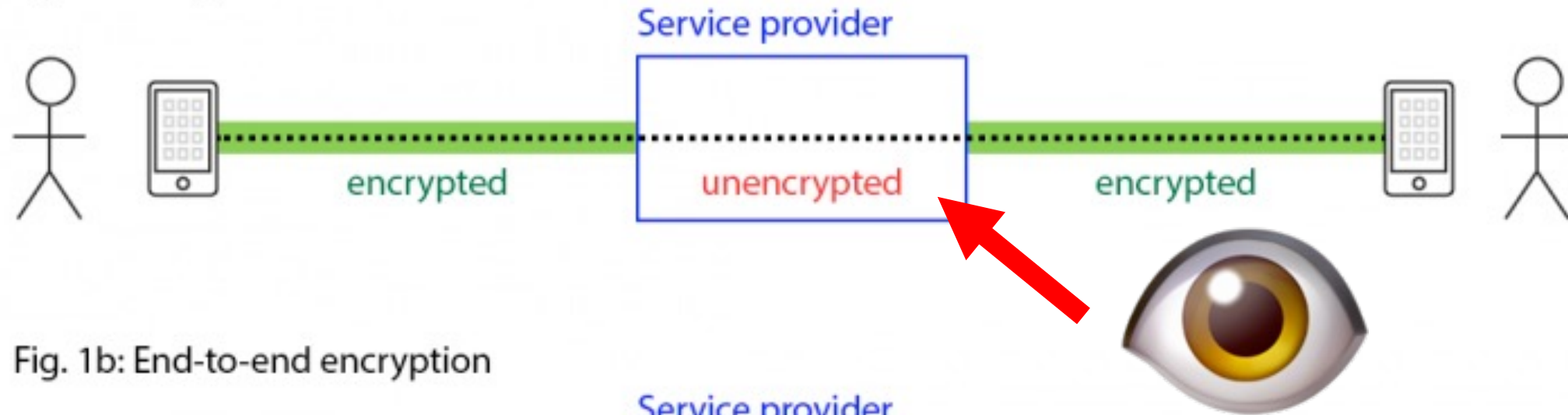


Fig. 1b: End-to-end encryption

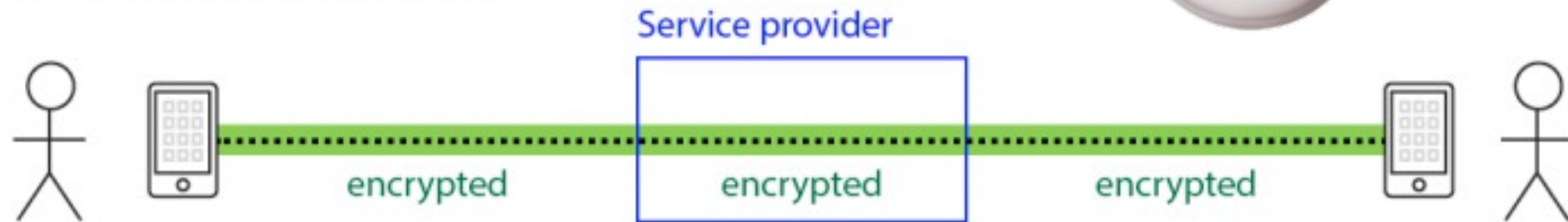
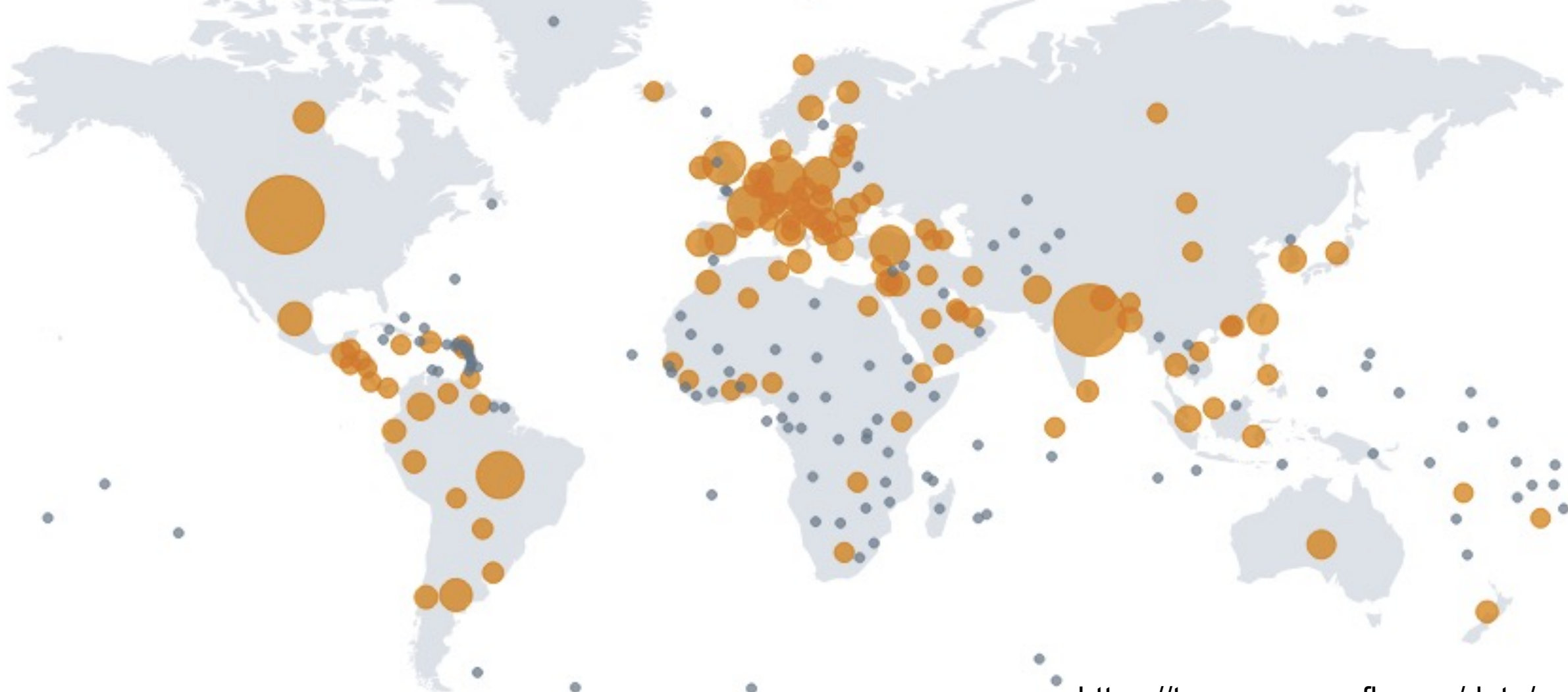


Fig. 1c: End-to-end encryption (no service provider)





<https://transparency.fb.com/data/>

237,414

Total requests

412,285

Users/accounts requested

76.10%

Of requests where some data
produced

CyberTipline 2021: Reports of online sexual exploitation are on the rise.

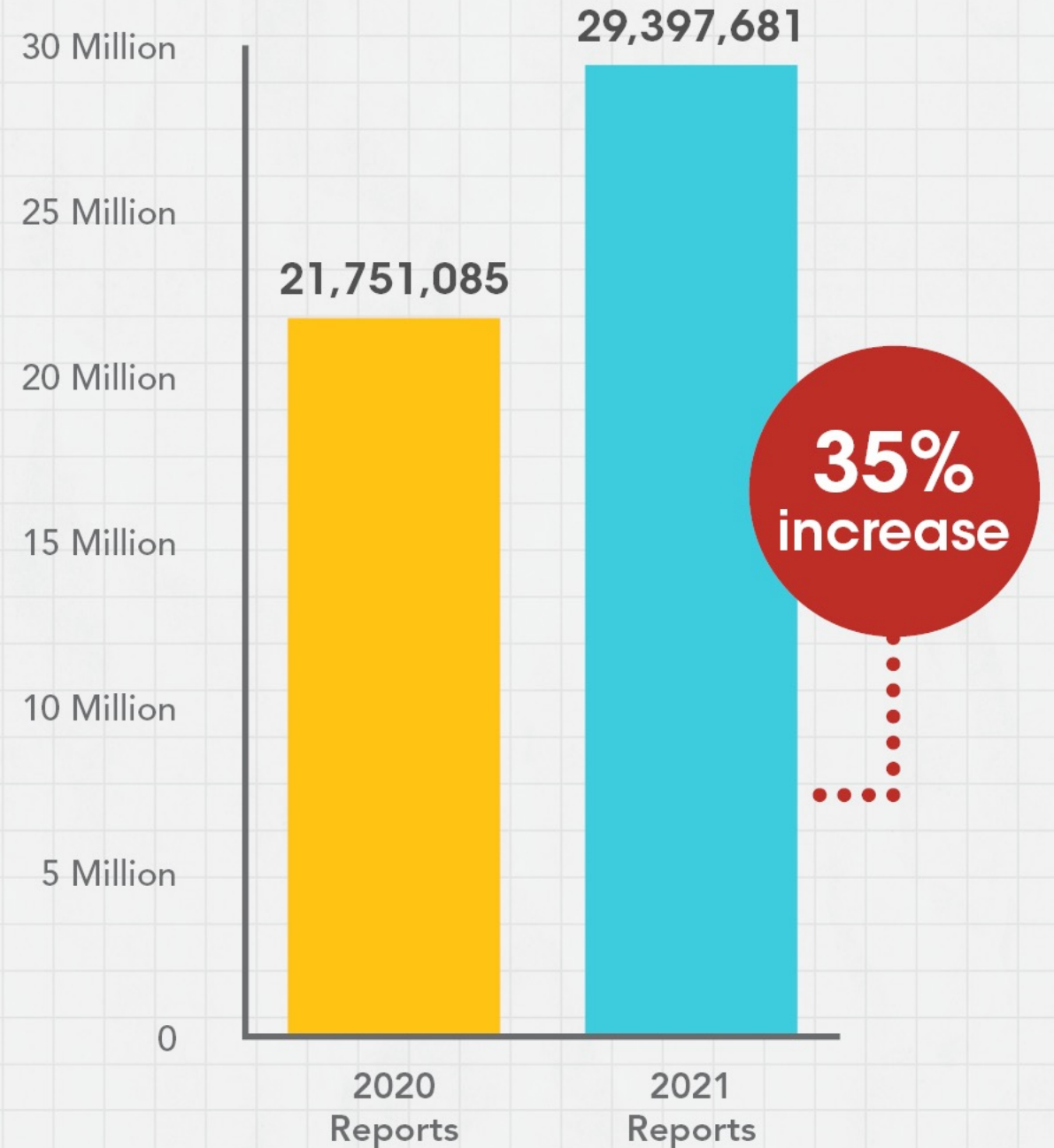


Fig. 1a: Encryption in transit



Fig. 1b: End-to-end encryption

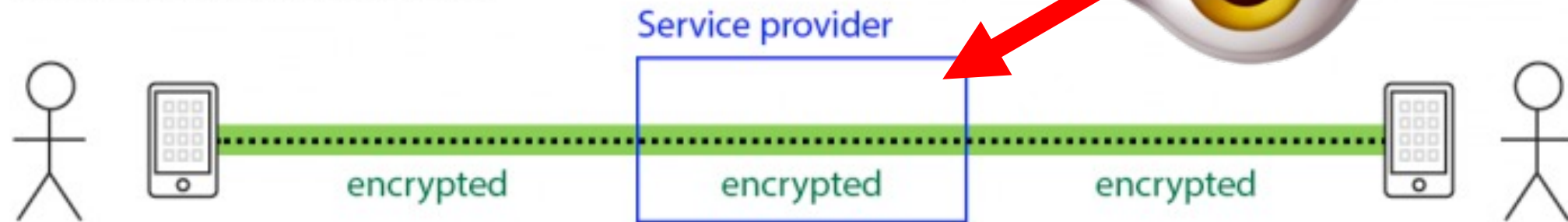


Fig. 1c: End-to-end encryption (no service provider)



Fig. 1a: Encryption in transit

Image: Martin Kleppmann



Fig. 1b: End-to-end encryption

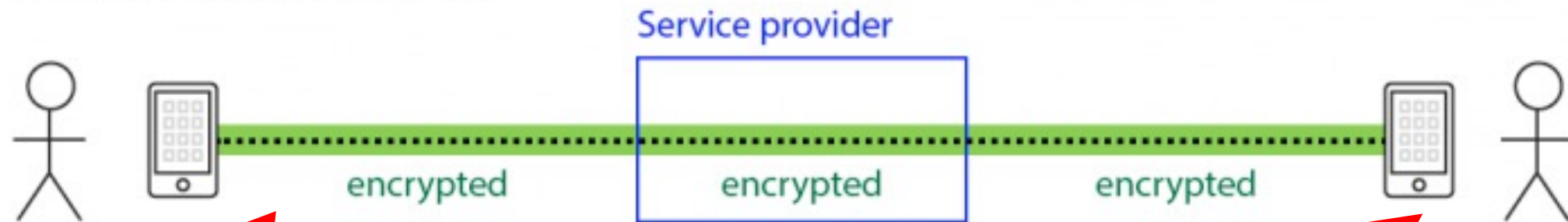


Fig. 1c: End-to-end encryption (no service provider)



PEGASUS BY THE NUMBERS



GLOBAL SCALE

36

LIKELY OPERATORS

45

COUNTRIES WITH
LIKELY INFECTIONS

10

OPERATORS WITH
INFECTIONS IN
ANOTHER COUNTRY

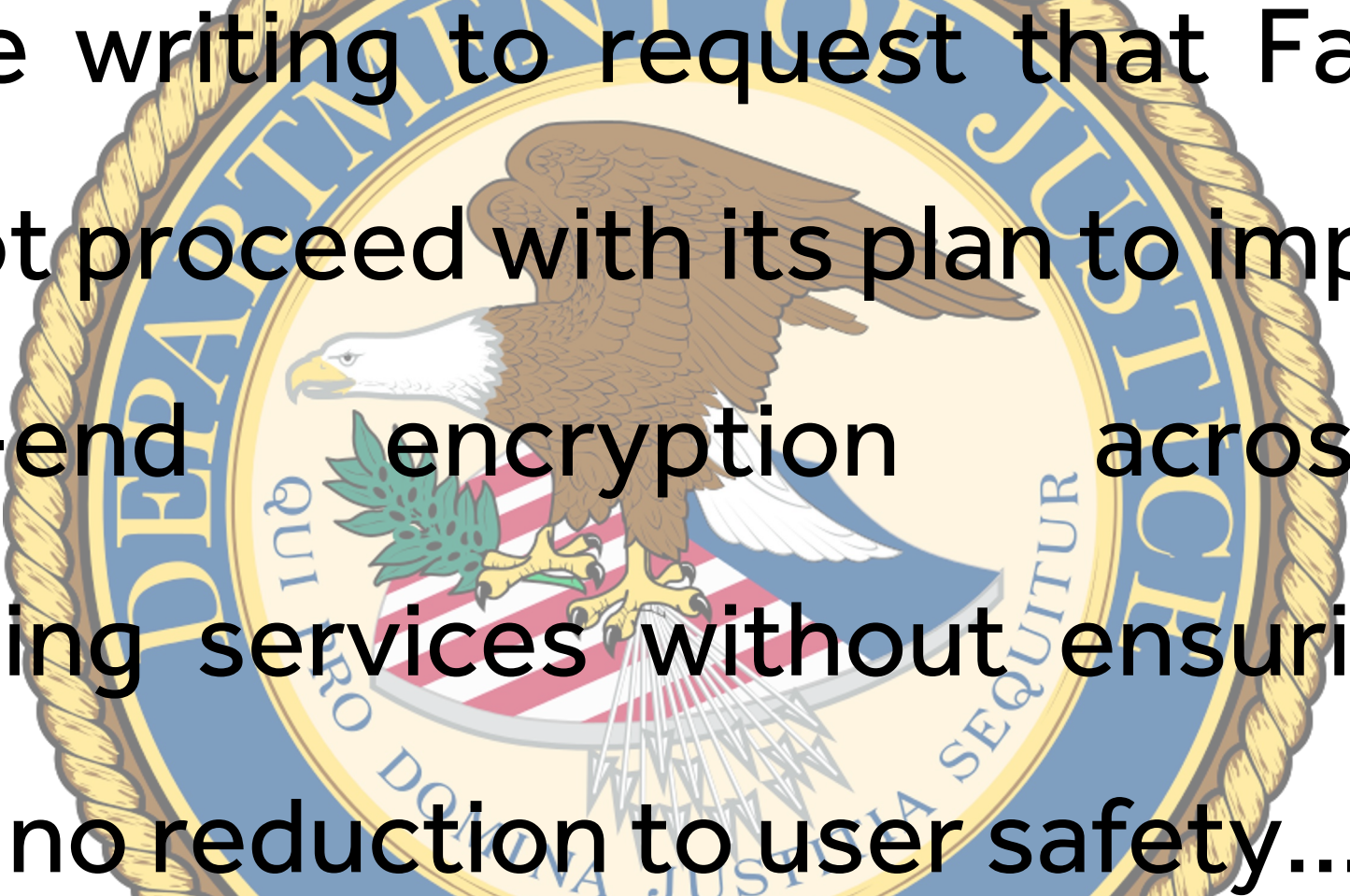


HUMAN RIGHTS

6

OPERATORS LINKED
TO COUNTRIES
WITH A HISTORY OF
ABUSING SPYWARE
TO TARGET CIVIL
SOCIETY



The seal of the Department of Justice is centered in the background. It features an eagle with spread wings, perched on a shield with red and white stripes. The eagle is holding an olive branch in its right talon and arrows in its left. The shield is set against a blue background with white stars. The words "DEPARTMENT OF JUSTICE" are written in a blue arc at the top, and "QUI PRO DOMINA JUSTITIA SEQUITUR" is written in a blue arc at the bottom. The entire seal is encircled by a gold rope border.

"We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety..."

and without including a means for lawful access to the content of communications to protect our citizens."



The seal of the United States Department of Justice is centered in the background. It features an eagle with wings spread, perched on a shield with red and white stripes. The eagle holds an olive branch in its right talon and arrows in its left. The shield is set against a blue background with white stars. The words "DEPARTMENT OF JUSTICE" are written in a blue arc at the top, and "QUI PRO DOMINA JUSTITIA SEQUITUR" is written in a blue arc at the bottom. The entire seal is encircled by a gold rope border.

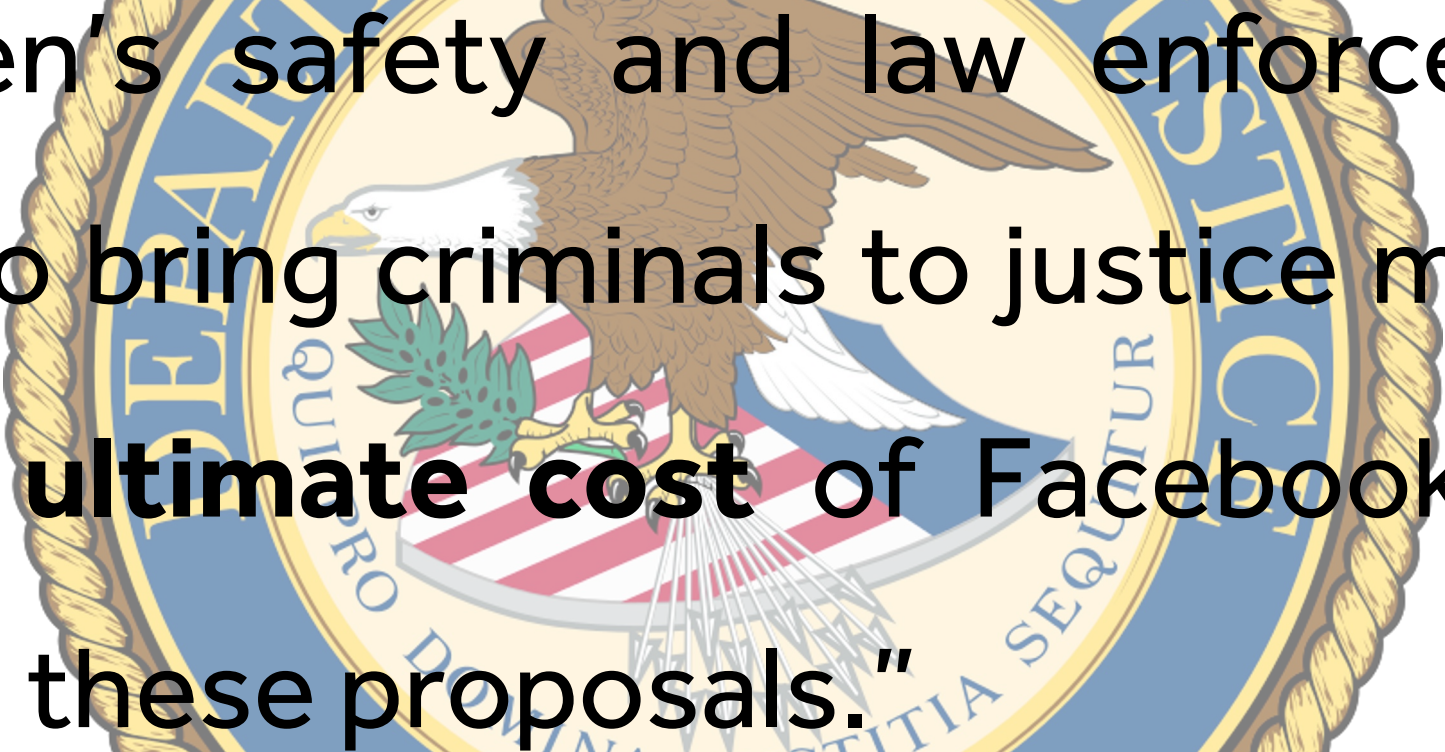
“Companies should not **deliberately design** their systems to preclude any form of access to content...

The seal of the United States Department of Justice is centered in the background. It features an eagle with wings spread, perched on a shield with red and white stripes. The eagle is surrounded by a blue ring with the words "DEPARTMENT OF JUSTICE" in gold. Below the eagle is a banner with the Latin motto "QUI PRO DOMINA JUSTITIA SEQUITUR". The entire seal is encircled by a gold rope-like border.

“This puts our citizens and societies at risk by severely eroding a company’s ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse, terrorism...”

The seal of the United States Department of Justice is centered in the background. It features an eagle with wings spread, perched on a shield with red and white stripes. The eagle is surrounded by a blue ring with the words "DEPARTMENT OF JUSTICE" in gold. Below the eagle is a banner with the Latin motto "QUI PRO DOMINA JUSTITIA SEQUITUR". The entire seal is encircled by a gold rope-like border.

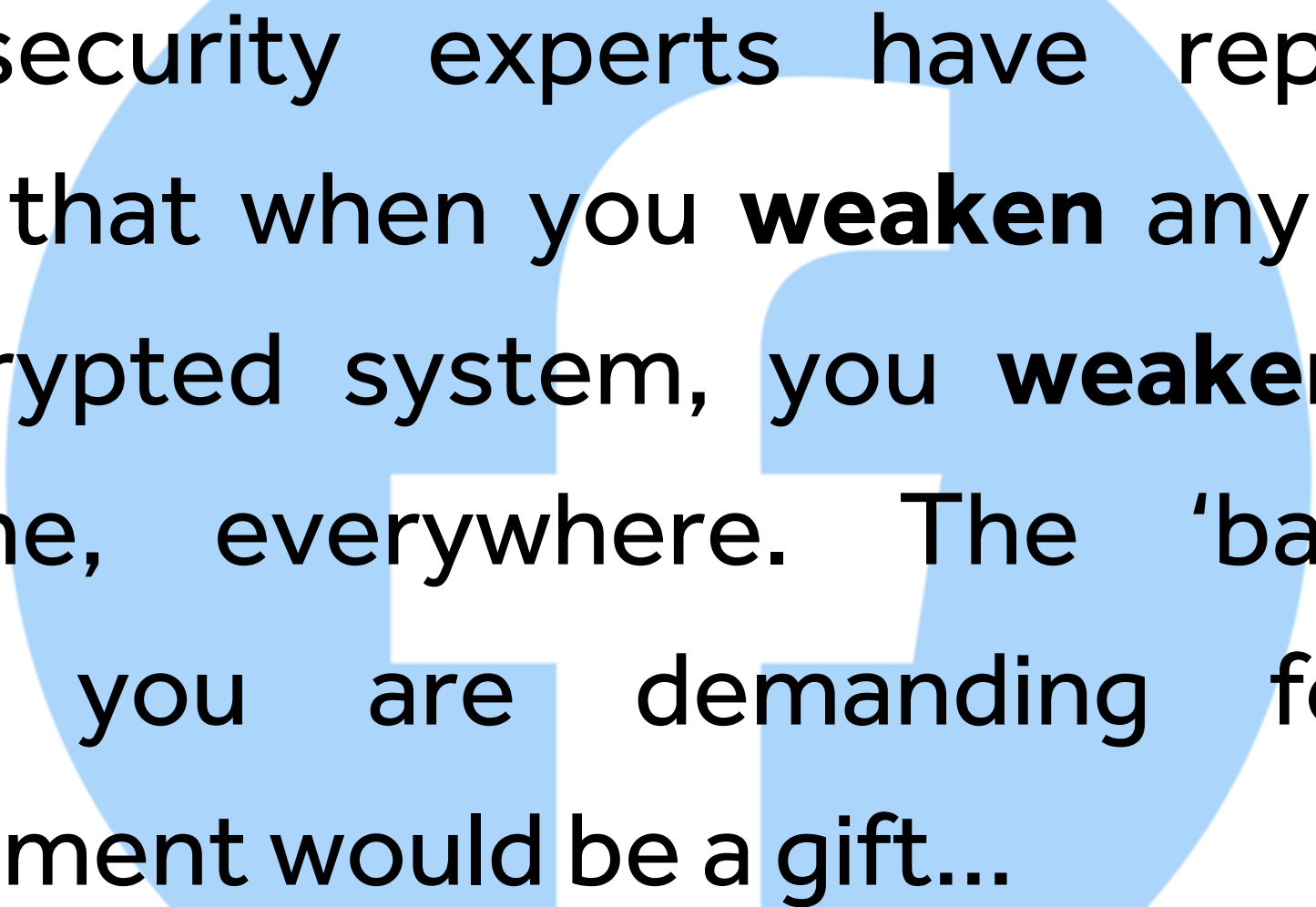
and foreign adversaries' attempts to
undermine democratic values and
institutions, **preventing the prosecution of
offenders and safeguarding of victims."**

The seal of the United States Department of Justice is centered in the background. It features an eagle with wings spread, perched on a shield with red and white stripes. The eagle holds an olive branch in its right talon and arrows in its left. The shield is set against a blue background with white stars. The words "DEPARTMENT OF JUSTICE" are written in a blue arc at the top, and "QUI PRO DOMINA JUSTITIA SEQUITUR" is written in a blue arc at the bottom. The entire seal is encircled by a gold rope border.

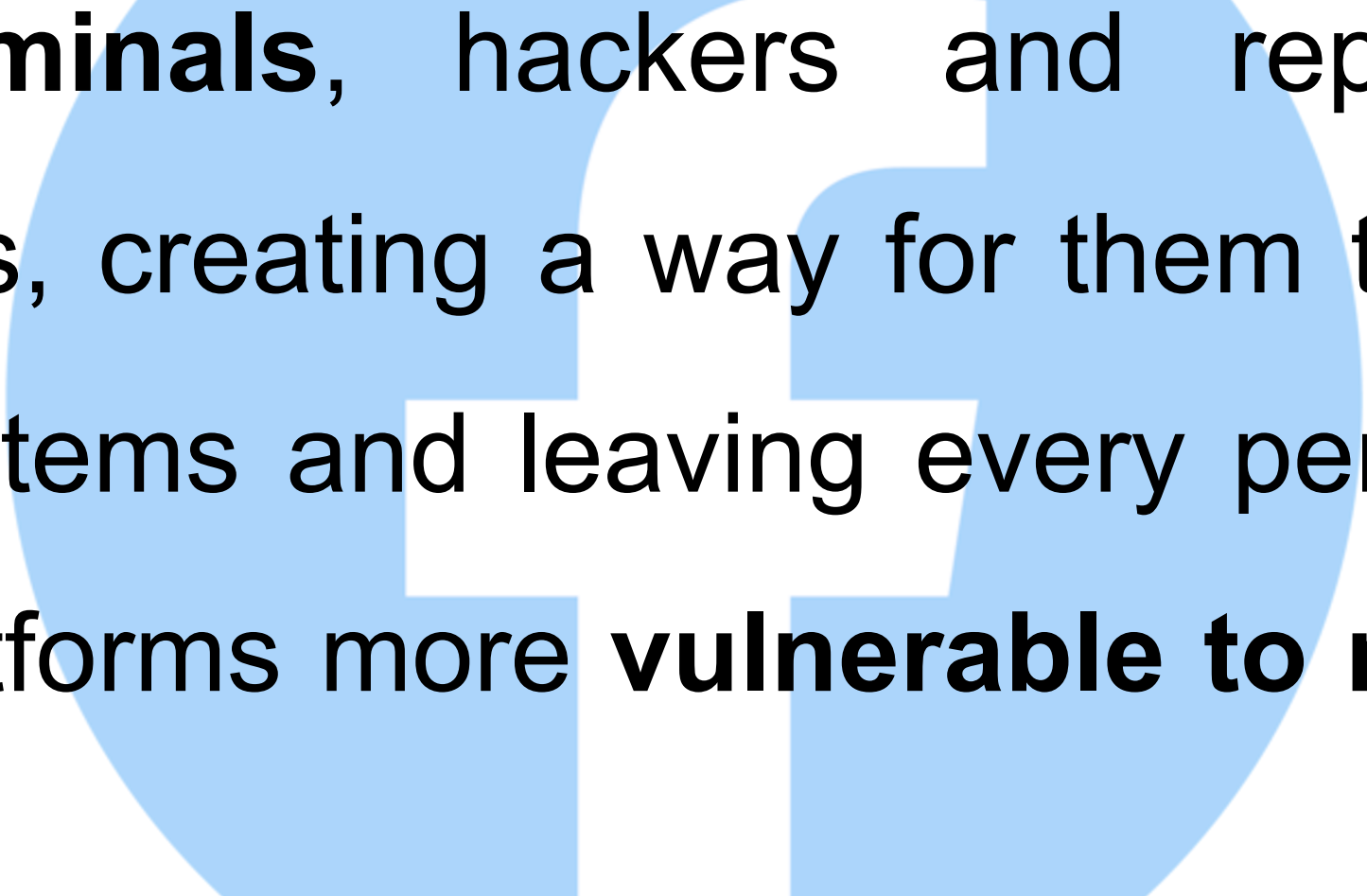
"Children's safety and law enforcement's ability to bring criminals to justice must not be **the ultimate cost** of Facebook taking forward these proposals."

A large, light blue Facebook logo is centered in the background of the slide. It consists of a white lowercase 'f' inside a light blue circle.

“We all want people to have the ability to communicate privately and safely, **without harm or abuse from hackers, criminals or repressive regimes.”**



“Cybersecurity experts have repeatedly proven that when you **weaken** any part of an encrypted system, you **weaken** it for everyone, everywhere. The ‘backdoor’ access you are demanding for law enforcement would be a gift...

A large, light blue Facebook logo watermark is centered in the background of the slide. It consists of a blue circle with a white 'f' inside.

to criminals, hackers and repressive regimes, creating a way for them to enter our systems and leaving every person on our platforms more vulnerable to real-life harm.”





BOOKED! Facebook plot to encrypt ALL chats 'will help child abusers to hide', former police chief warns

Sean Keach, Digital Technology and Science Editor

Published: 10:48, 27 May 2020 | Updated: 10:48, 27 May 2020



FACEBOOK risks helping child abusers to hide their sick online activities, a former police chief has warned.

The alarm has been raised over Facebook's plans to encrypt more of our private chats – shutting out hackers, but also the police.

SUN POLL Do you think Facebook should encrypt all chats?

Definitely!

57.6%

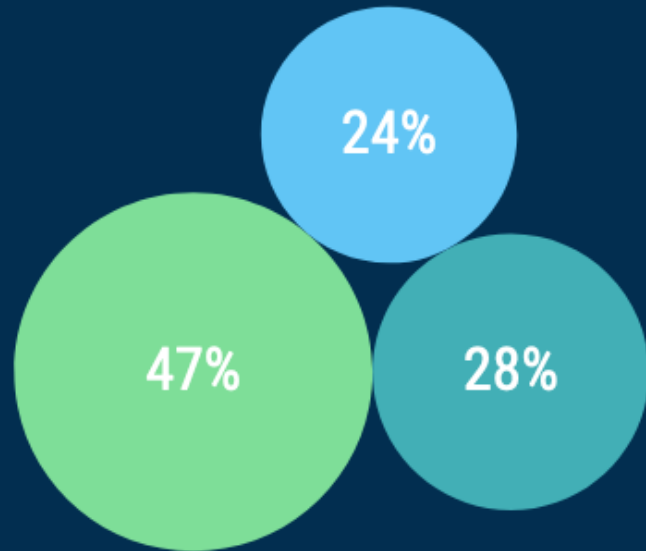
No, absolutely not

18.2%

I'm not sure

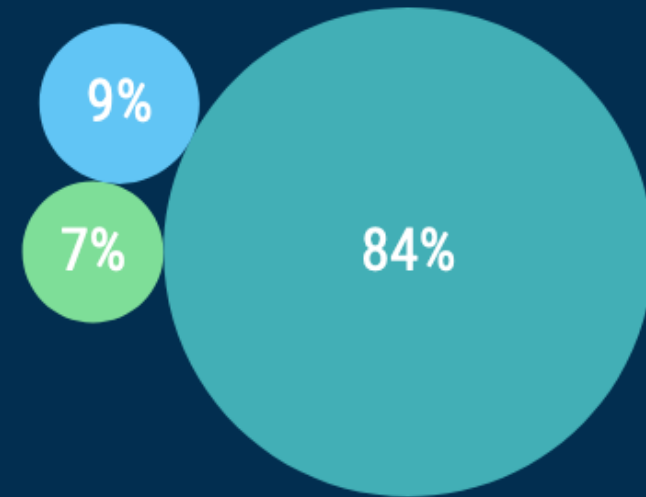
24.2%

Should Facebook encrypt all of your chats?

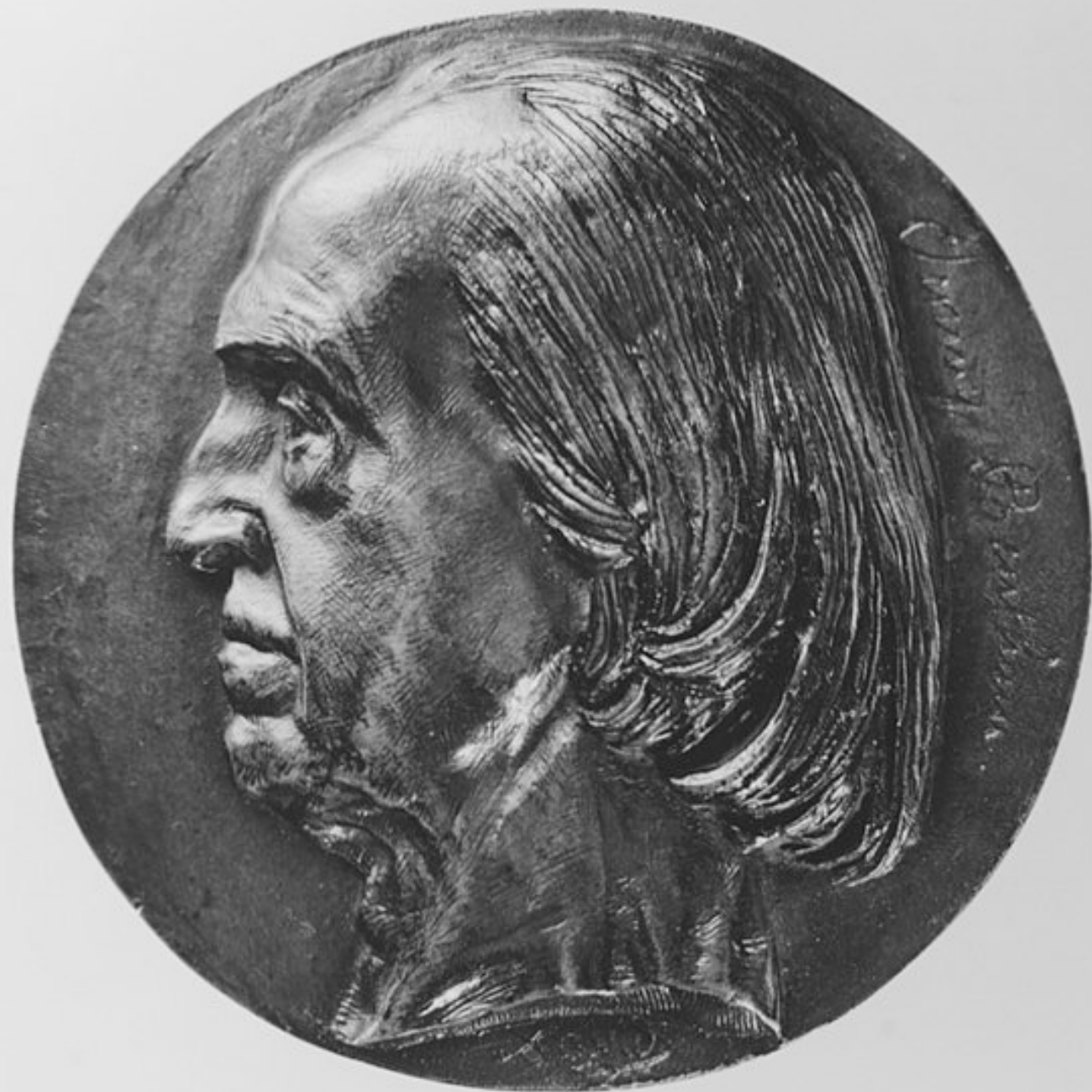


- ★ Definitely
- ★ No, absolutely not
- ★ I'm not sure

Should the government have access to your online chats?



- ★ Yes, they should
- ★ No, absolutely not
- ★ Hmm... I'm not sure





GRAMMES

25 20 15 10 5 0

PORTEE MINIMUM PORTEE MAXIMUM 2 KILOG.

LE POIDS LU SUR LE CADRAN N'EST EXACT QUE SI L'AIGUILLE SE TROUVE EN FACE DU ZERO LORSQU'IL N'Y A AUCUN POIDS DANS LES PLATEAUX.

AVERY

Societe Belge des Balances & Bascules

RUE DE L'INTENDANT, 43 - BRUXELLES







Change

Who will guard
the guards
themselves?



open



www.Gresham.ac.uk
@GreshamCollege



**FOR THE LOVE OF LEARNING
SINCE 1597**



GRESHAM

COLLEGE