7 July 2021
MEAC-SIG

Encryption

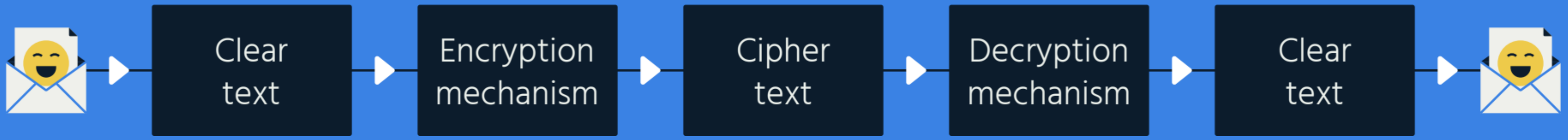
As an Internet Governance issue

Hanna Kreitem
Senior Advisor, Internet Technology and Development, MENA
kreitem@isoc.org

What is encryption?

01 What is encryption?

Encryption is a way to scramble information so that only those with ‘keys’ can understand what is being shared.



Clear text → Encryption mechanism → Cipher text → Decryption mechanism → Clear text

Encryption makes information unintelligible, not inaccessible. Someone can still access your data, but it appears meaningless.

I don’t expect anyone to read my messages, other than who I send them to!
Marcus

The importance of encryption

In our increasingly digital lives, the role of encryption has never been more essential.

Encryption is a crucial feature of a safe Internet. It ensures your private messages stay private.

From video calls to air traffic control and e-voting, encryption is vital for securing all aspects of our lives.

It keeps your identity safe and stops people from impersonating you, or the people that you trust.

It is critical to national security, protecting society from terrorists, criminals, and hostile governments.

Personal security depends on encryption. It keeps your confidential data out of the hands of criminals.

The importance of encryption

In our increasingly digital lives, the role of encryption has never been more essential.

Encryption is a crucial feature of a safe Internet. It ensures your private messages stay private.

From video calls to air traffic control and e-voting, encryption is vital for securing all aspects of our lives.

It keeps your identity safe and stops people from impersonating you, or the people that you trust.

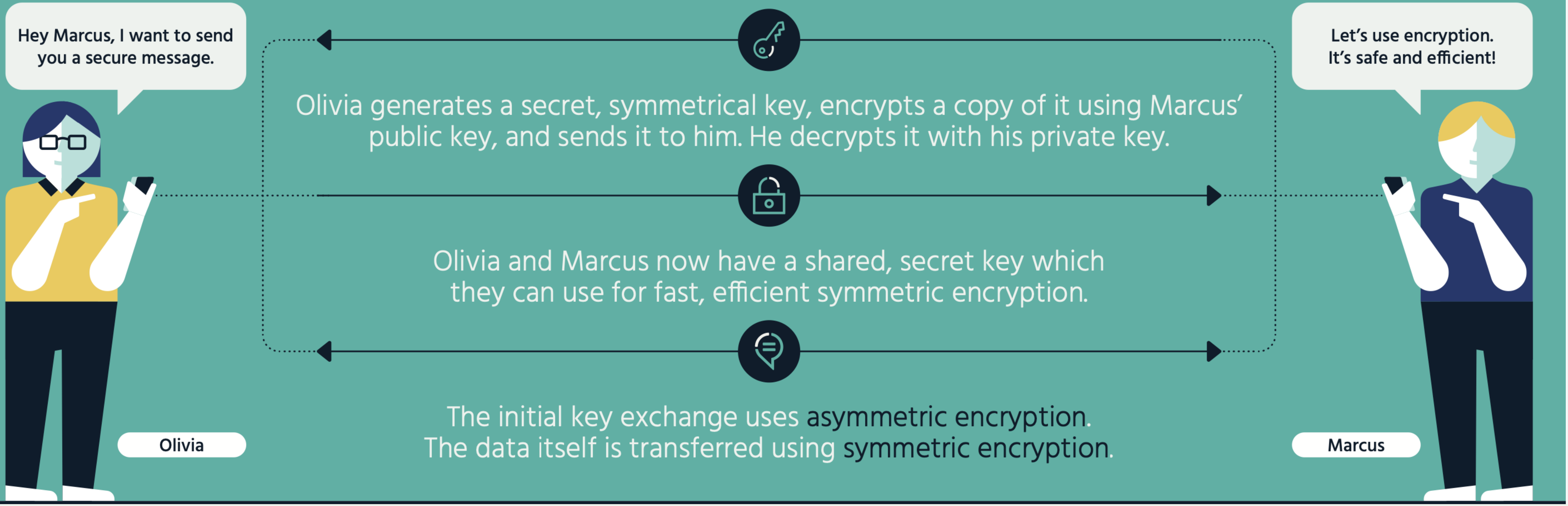
It is critical to national security, protecting society from terrorists, criminals, and hostile governments.

Personal security depends on encryption. It keeps your confidential data out of the hands of criminals.

02 How does encryption work?

Internet Society

Each user has two keys: a public one and private one.
Olivia finds Marcus' public key and copies it to her device.


Hey Marcus, I want to send you a secure message.
Let's use encryption. It's safe and efficient!
Olivia
Marcus

Olivia generates a secret, symmetrical key, encrypts a copy of it using Marcus' public key, and sends it to him. He decrypts it with his private key.

Olivia and Marcus now have a shared, secret key which they can use for fast, efficient symmetric encryption.

The initial key exchange uses asymmetric encryption.
The data itself is transferred using symmetric encryption.

Different types of encryption

Not all encryption is equal. The best systems balance safety and efficiency.

Symmetric encryption is like a cash box, where all users have the same secret key to see what's inside.

✓ Fast and efficient

✗ Vulnerable to interception

With asymmetric encryption each user has their own public and private keys, providing additional security.

✓ Safe and secure

✗ Complexity means less efficiency

In hybrid systems, a mixture of encryption processes provides the best of both worlds. Asymmetric encryption is used for a secure key exchange, with the more efficient system of symmetric encryption used to transfer the data itself.

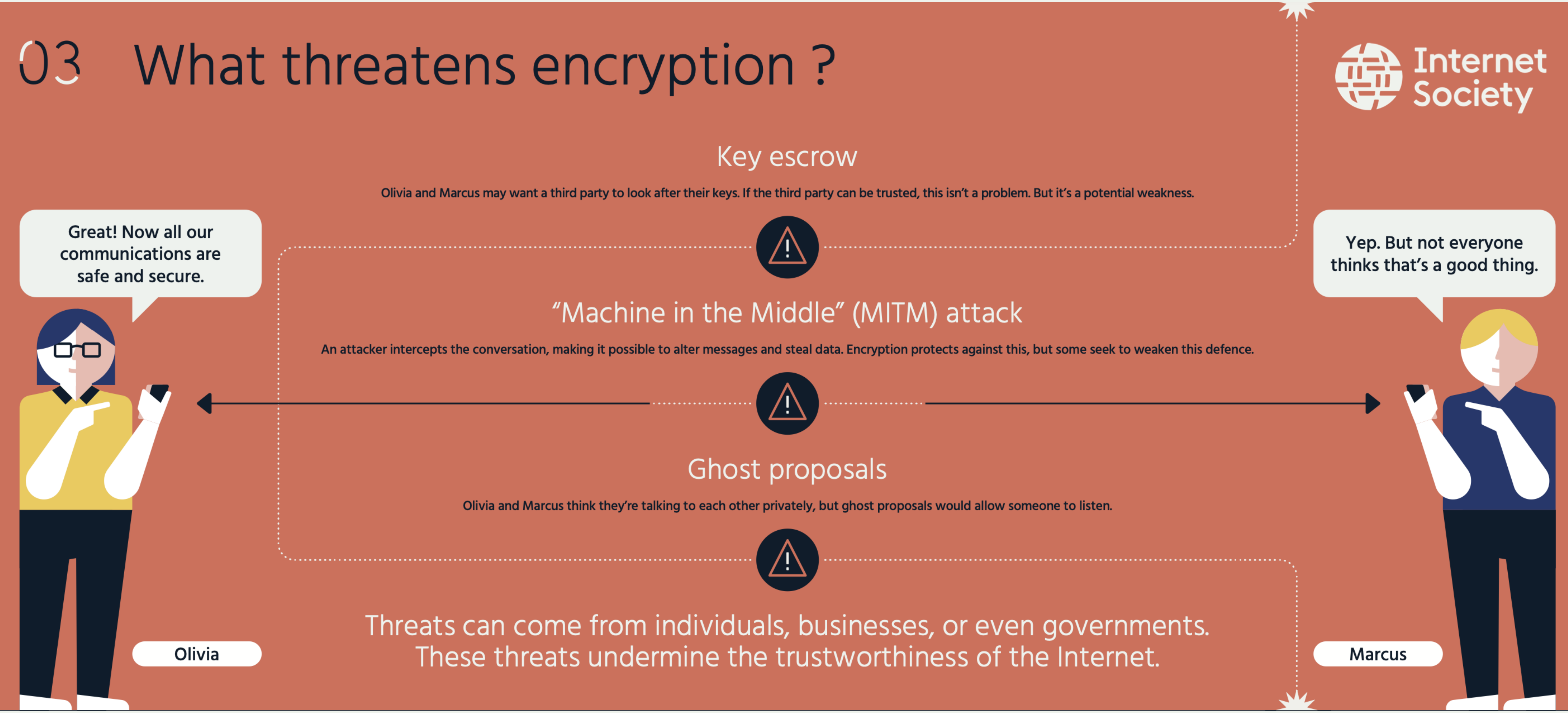
✓ Safe and secure

✓ Fast and efficient

May 2021

03 What threatens encryption ?

Internet Society


Great! Now all our communications are safe and secure.
Yep. But not everyone thinks that's a good thing.
Olivia
Marcus

Key escrow

Olivia and Marcus may want a third party to look after their keys. If the third party can be trusted, this isn't a problem. But it's a potential weakness.

"Machine in the Middle" (MITM) attack

An attacker intercepts the conversation, making it possible to alter messages and steal data. Encryption protects against this, but some seek to weaken this defence.

Ghost proposals

Olivia and Marcus think they're talking to each other privately, but ghost proposals would allow someone to listen.

Threats can come from individuals, businesses, or even governments.
These threats undermine the trustworthiness of the Internet.

Where threats come from

Knowing who wants to access your data highlights the importance of keeping it safe.

Some areas of law enforcement want backdoors to catch criminals. This creates access for bad actors, not just good ones.

Many governments think they should be able to break encryption in order to access their citizens' messages.

Blackmailers would like to break encryption to target people's private messages, photos and videos.

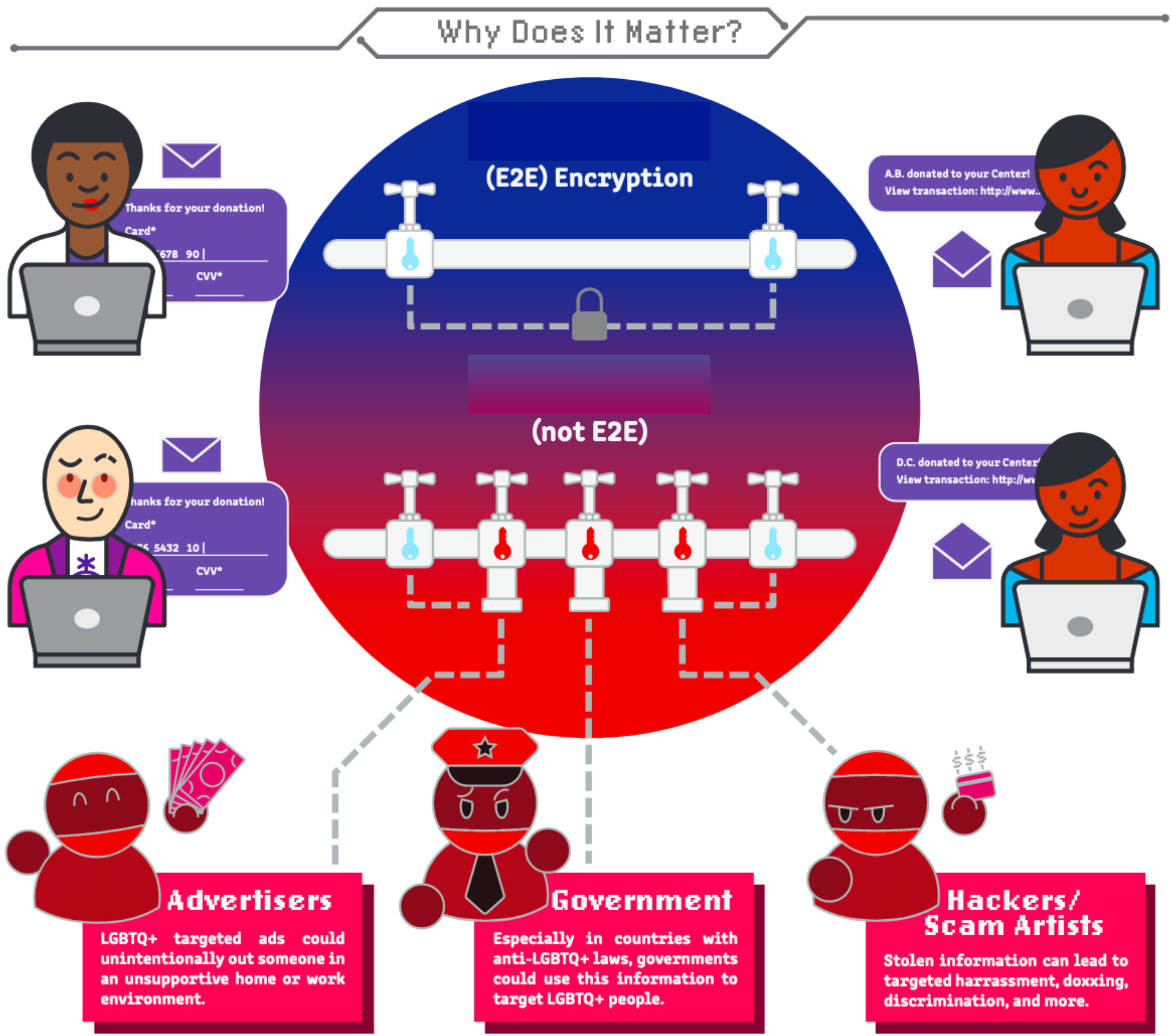
Personal banking and national economies rely on encryption. Vulnerabilities could lead to stolen money and financial data.

Criminals steal people's identities, to commit crimes and evade capture. Weak encryption would enable this.

Helpful references/factsheets:
internetsociety.org/encryption/internet-community-stands-up-for-encryption/

Connect: Encryption for everyone group – library

Photo courtesy of James Eades via Unsplash


Thanks for your donation!
Card*
678 90
CVV*
(E2E) Encryption
A.B. donated to your Center!
View transaction: http://www...
(not E2E)
hanks for your donation!
Card*
6 5432 10
CVV*
D.C. donated to your Center
View transaction: http://ww
$$$

Why Does It Matter?

Advertisers

LGBTQ+ targeted ads could unintentionally out someone in an unsupportive home or work environment.

Government

Especially in countries with anti-LGBTQ+ laws, governments could use this information to target LGBTQ+ people.

Hackers/ Scam Artists

Stolen information can lead to targeted harrassment, doxxing, discrimination, and more.

What we learned in 2020/2021

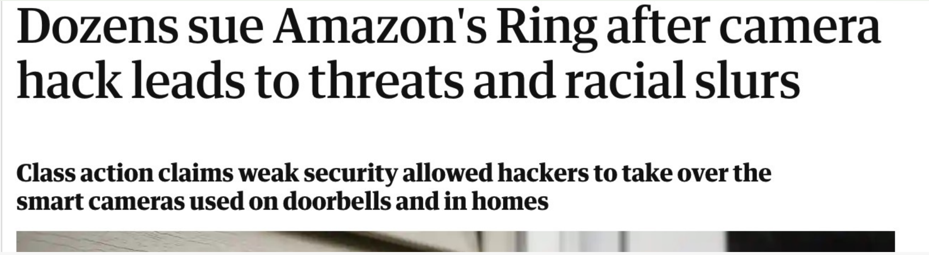
COVID-19 helped us change the narrative on encryption in a big way.

And it help us create a global movement to protect and defend encryption.

However…

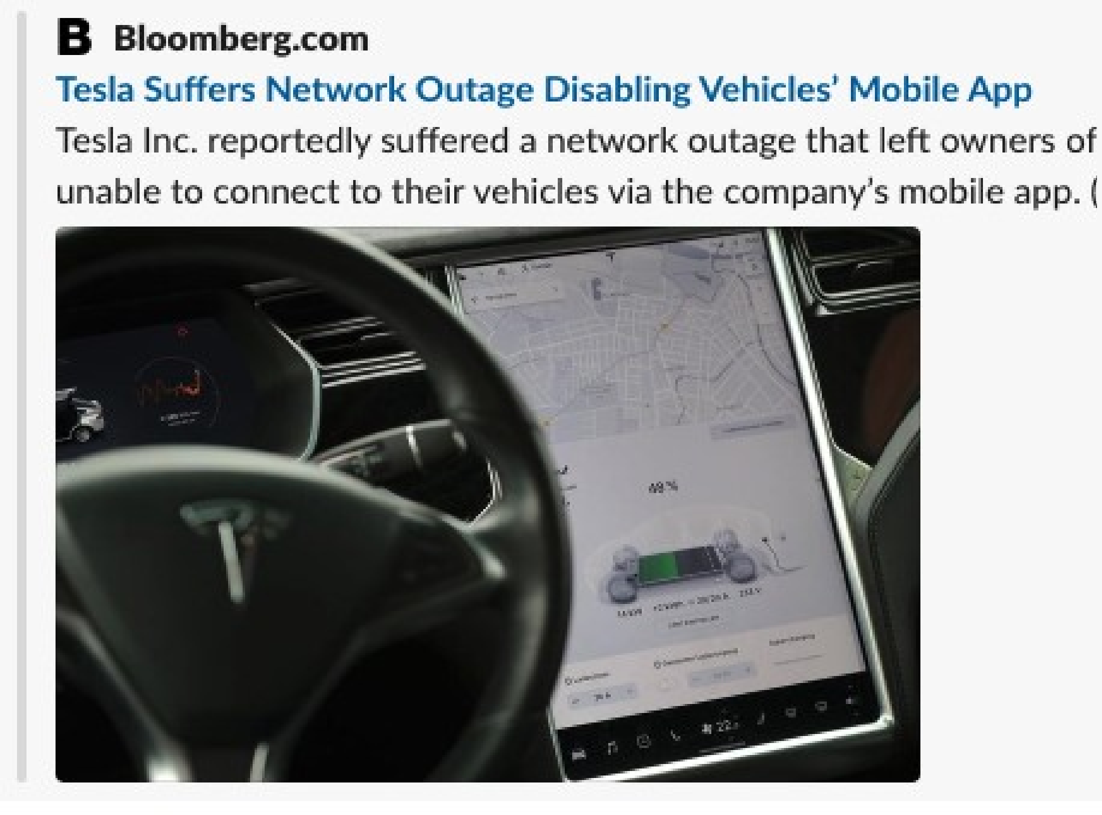
2020/2021 also saw governments continue to try undermine or prevent the use of strong encryption.

When encryption is under threat… so are we.



Dozens sue Amazon's Ring after camera hack leads to threats and racial slurs

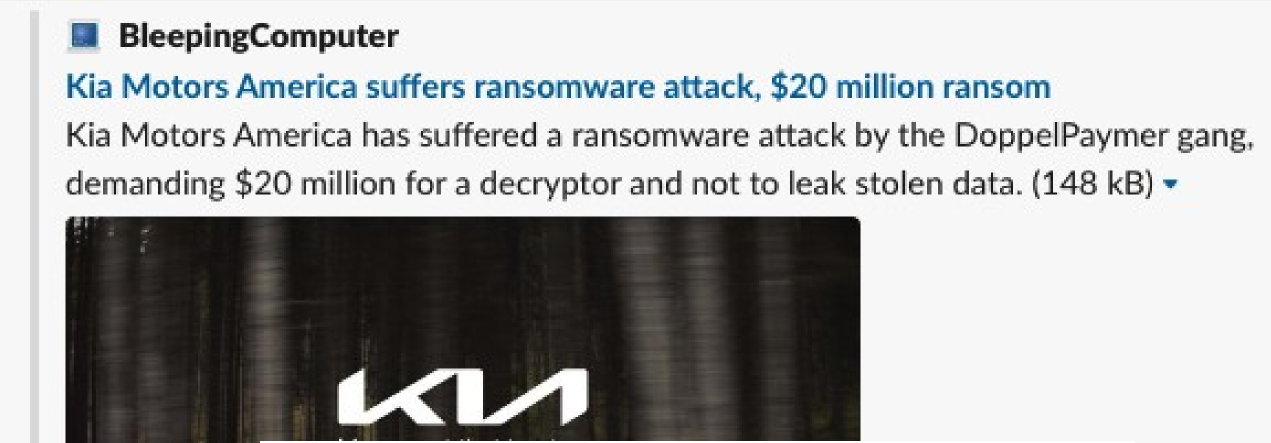
Class action claims weak security allowed hackers to take over the smart cameras used on doorbells and in homes



Bloomberg.com

Tesla Suffers Network Outage Disabling Vehicles' Mobile App

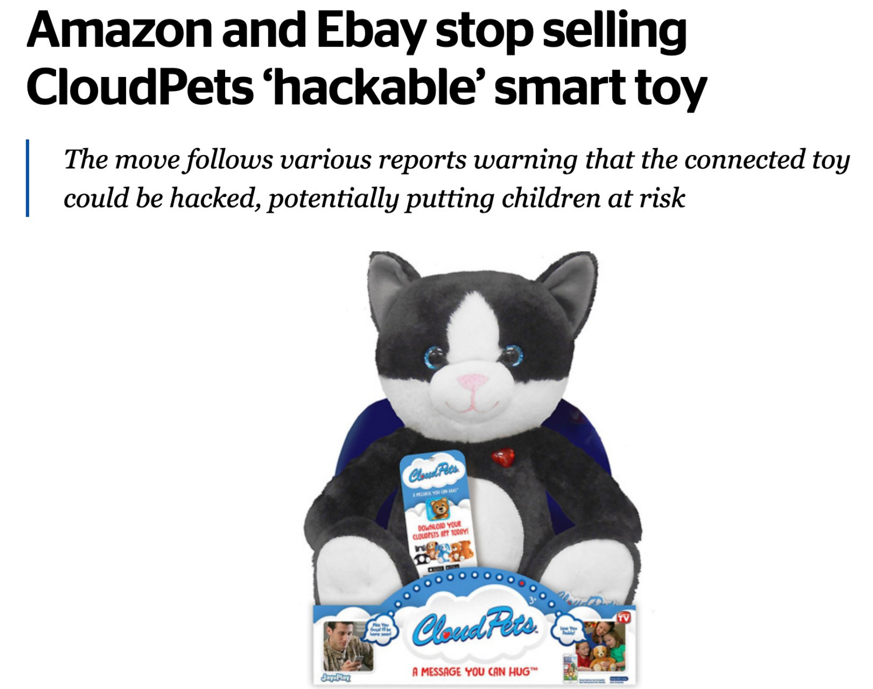
Tesla Inc. reportedly suffered a network outage that left owners of
unable to connect to their vehicles via the company's mobile app. (



BleepingComputer

Kia Motors America suffers ransomware attack, $20 million ransom

Kia Motors America has suffered a ransomware attack by the DoppelPaymer gang, demanding $20 million for a decryptor and not to leak stolen data. (148 kB) ▾



Amazon and Ebay stop selling CloudPets 'hackable' smart toy

> *The move follows various reports warning that the connected toy could be hacked, potentially putting children at risk*

ISOC advocacy goals

We want to:

- Grow the use of end-to-end encryption.
- Stop government attempts to undermine encryption in target countries.
- Get 1M people participating in our campaign.

Our approach to advocacy

- Thought leadership
- Building a movement
- Raising new heroes
- Direct advocacy and mobilization

Together, we can advocate for strong encryption every day.

How to talk about encryption and actions you can take

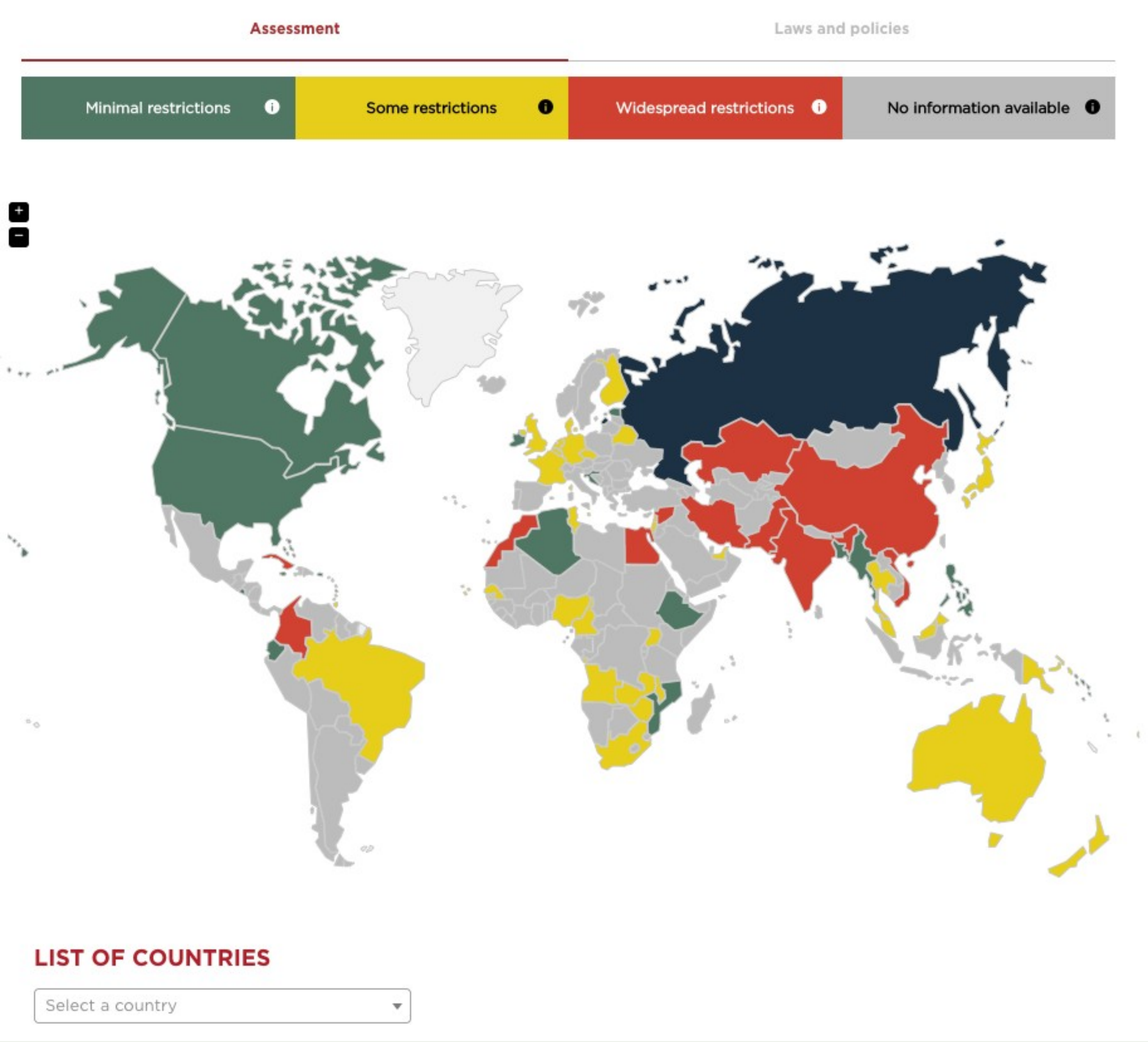
Key Messages

1. Encryption keeps billions of people safe and secure every day.
2. Efforts to weaken encryption will create a dangerous precedent — giving a green light to criminals, terrorist organizations, and hostile governments to access and exploit sensitive information.
3. Weakening encryption creates openings for criminal activity — with devastating consequences for both personal safety and national security.
4. The best way to prevent crime and protect countries is to adopt stronger encryption policies and industry practices.
5. We must push for strong encryption policies and industry practices to prevent crime, protect citizens, and safeguard nations.

Update the World Map of Encryption Laws

The more we know, the more
we can protect/defend encryption
worldwide.

HOW TO PARTICIPATE:
Update World Map of Encryption Laws with regional input: gp-digital.org/world-map-of-encryption/



Global
Encryption
Coalition

Join & recruit for the Global Encryption Coalition

HOW TO PARTICIPATE:

Step 1: Get your org/group to join the GEC.

Step 2: Contact ge-admin@globalencryption.org to get GEC Slack account.

1 thing you can do right now – Register & share:

https://internetsociety.org/learning/encryption

Thank you.

Hanna Kreitem
kreitem@isoc.org

Rue Vallin 2
CH-1201 Geneva
Switzerland

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

Science Park 400
1098 XH Amsterdam
Netherlands

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internetsociety.org
@internetsociety