ISOC Gambia Chapter Workshop
28th October 2022

Defending End-to-end Encryption

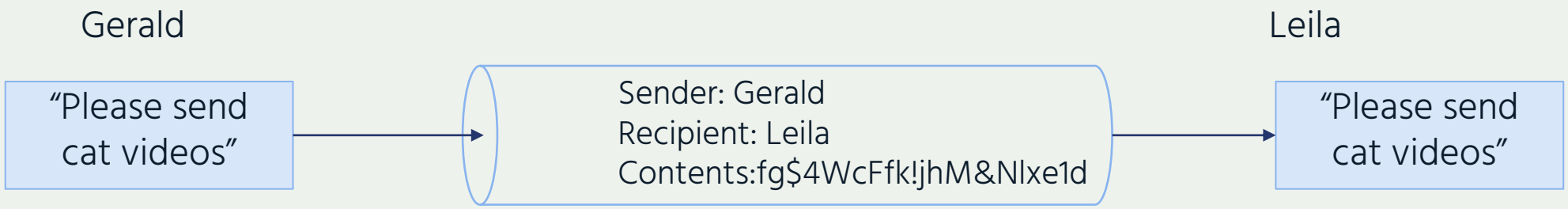
Robin Wilton - Director, Internet Trust
wilton@isoc.org

Topics

- What is encryption *really* about?
- Why should we care?
- What can we do next?

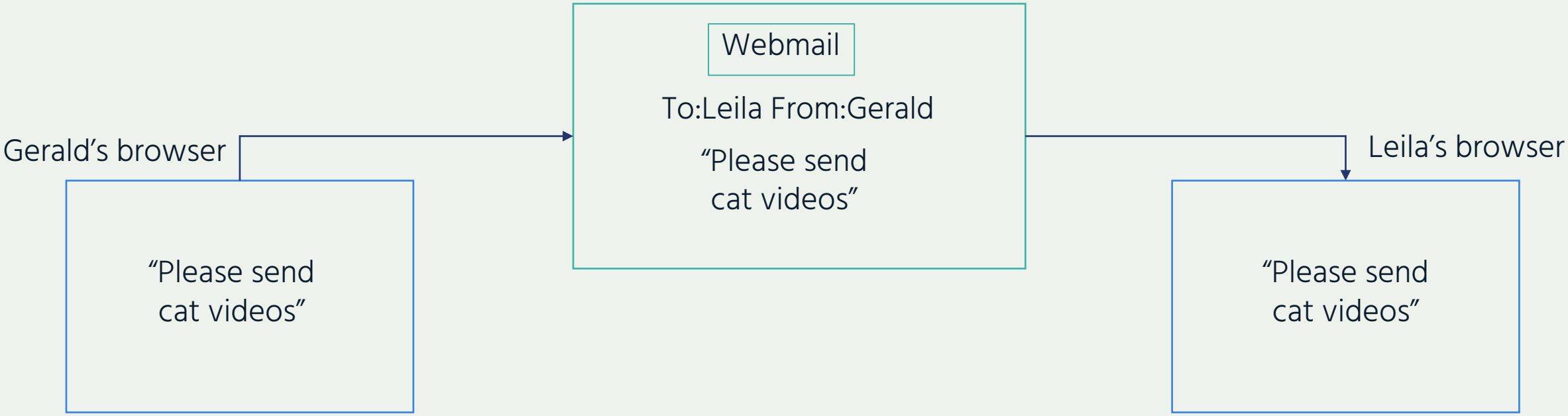
We often think of encryption as a two-party process.

- Here's a simple diagram of an encrypted exchange between Gerald and Leila.
- We can assume that Gerald and Leila's intent is to keep their conversation confidential, even if it has to pass through other hands…
- And it will.



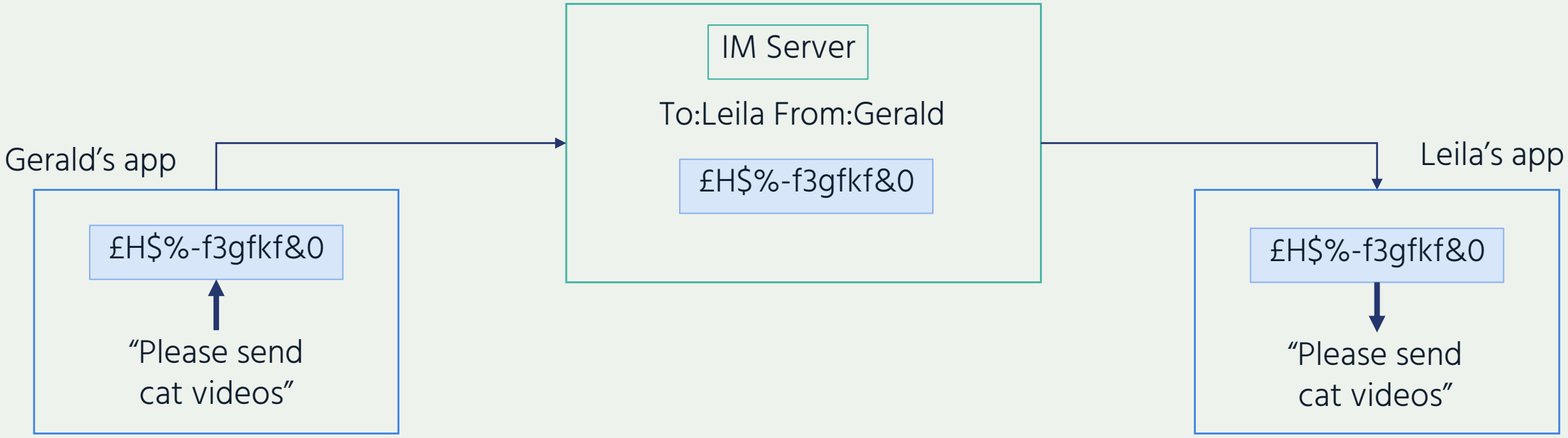
All our online activities pass through at least one intermediary.

By default, intermediaries see the message and who is talking to whom – even if Gerald and Leila are both using https.



E2E Encryption protects the message throughout its journey.

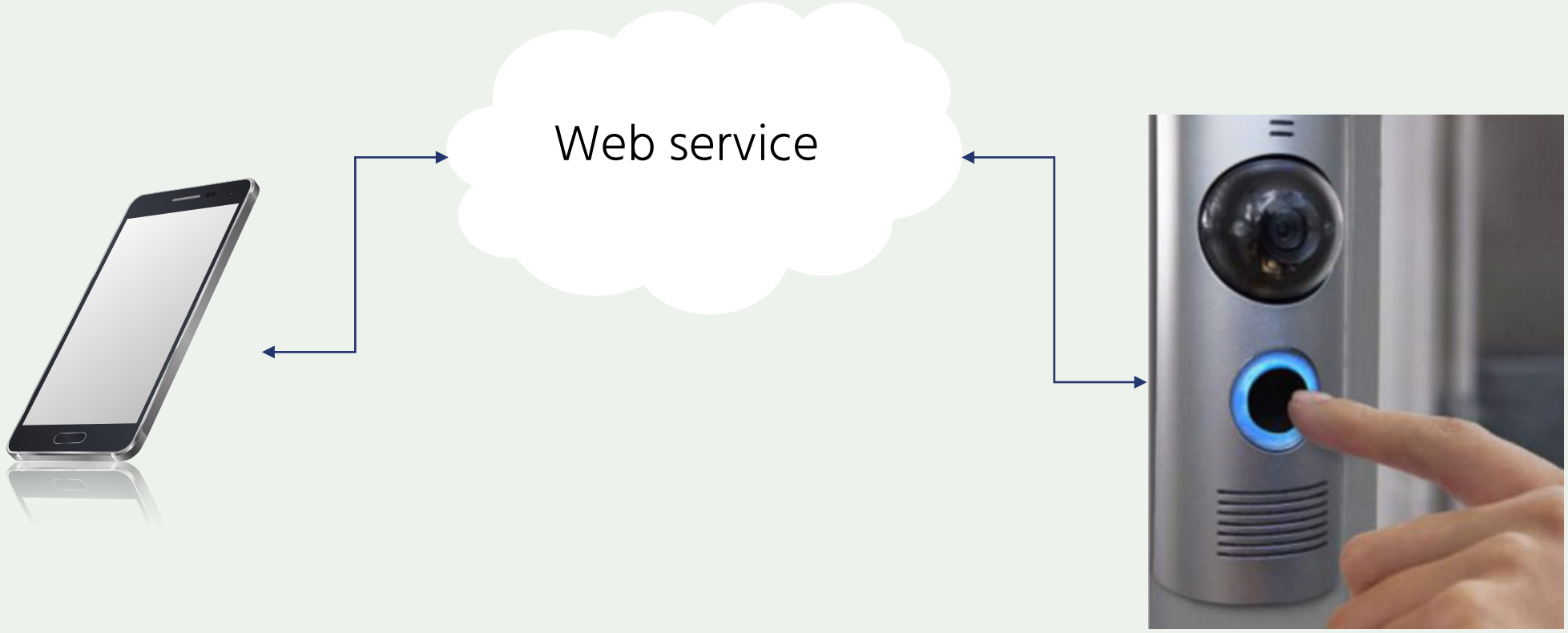
The intermediary – *even if it's the messaging server* - cannot see, alter or forge the message's contents.



- What is encryption *really* about?
- Why should we care?
- What can we do next?

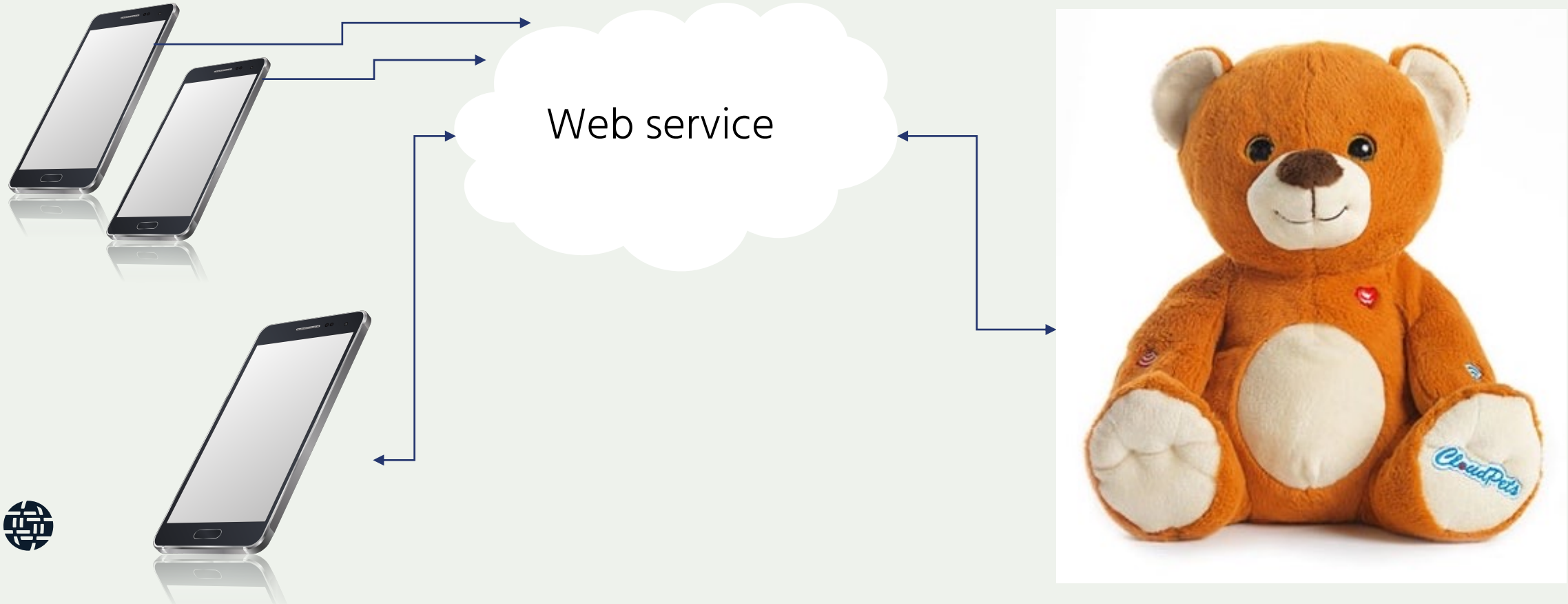
Encryption is not just about data, it's now about physical safety.

- Monitoring your smart doorbell remotely via the manufacturer's web service
- It's your home, your family, your mobile device… and someone else's cloud.



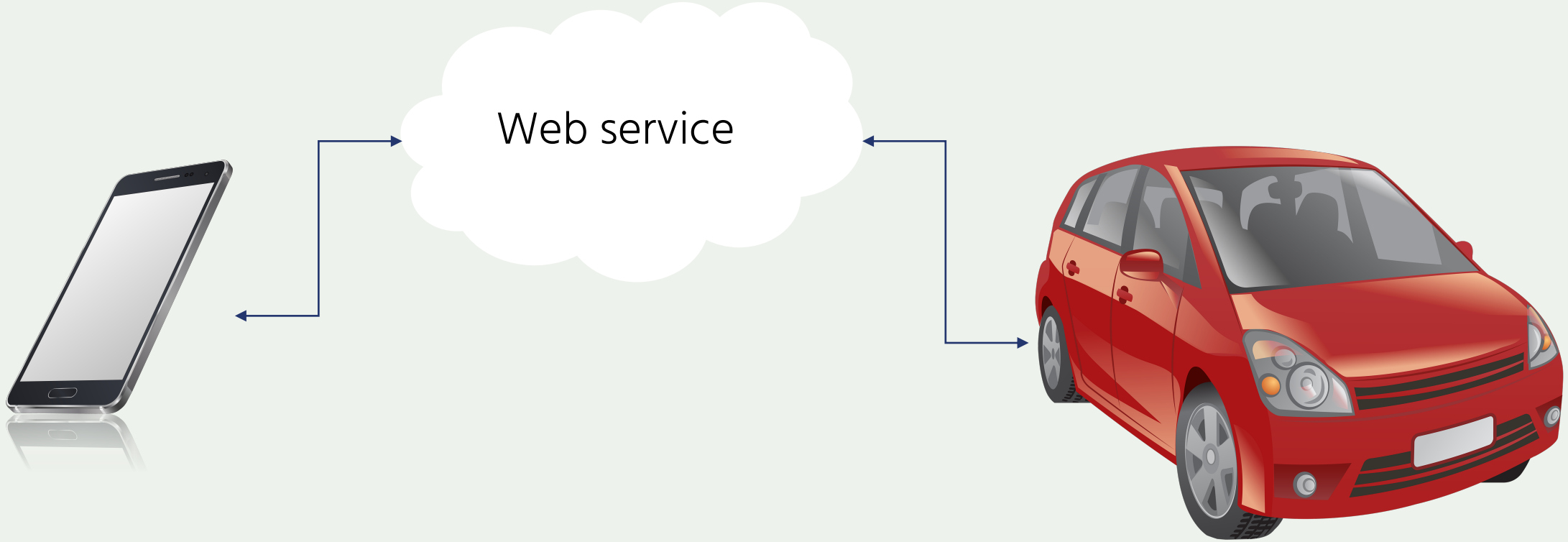
… and it's about the safety of your children …

- Did you really expect that this connected toy would let strangers access personal messages to your child?



… and it's not just about safety at home…

- Monitoring your car's location/security remotely via the manufacturer's web service
- It's your car, your mobile device, your safety… and someone else's cloud.



… and it’s not just about security of people.

- Any control system that operates via a third party ”cloud” illustrates the same point.
- Infrastructure services running on “elastic computing”…
- Drones
- Autonomous vehicles
- Charging stations for electronic cars

- In any such setup, it’s not only none of the intermediary’s business what’s in the traffic they handle, it’s actively unsafe if they can read, alter or fake messages.

The “No-one But Us” Mentality

Weakening mass market products and services does not prevent malicious actors from finding secure ways to communicate.

⇒ It compromises our security without delivering the intended result.

Exceptional access “will be hacked, it will be utilized, and there’s no way to make it secure” – US legislator

”Encryption is an overwhelmingly good thing – it keeps us all safe and secure. Building in backdoors is a threat to everybody and it’s not a good idea to weaken security for everybody to tackle a minority.”

- Robert Hannigan, former director of GCHQ

“The EU has fallen for the myth that it’s possible to keep us safer by weakening the very thing that protects us.”

- Markéta Gregorová, MEP

We should fundamentally oppose policies that weaken cryptographic technology, because they make everyone less safe.

Is encryption still under threat?

Yes!

- Australia, Bangladesh, Canada, India, Turkey, UK and US, among others, are all legislating for more Government access to data, even if it's encrypted.

- Proposals with labels like "traceability", "content moderation", "child safety", "age verification" all represent steps towards undermining, bypassing or even banning encryption.

You can check a country's status here, and submit updates too!
https://www.gp-digital.org/world-map-of-encryption/

Topics

- What is encryption really about?
- Why should we care?
- What can we do next?

Join The Movement - October 21st *is* Global Encryption Day

Companies, civil society, Chapters, individuals... even policymakers have joined in. A rights activist and a journalist told us how encryption protects them.

- Do you depend on encryption?
- Has encryption kept you safe?

What's your story? Tell us, and we'll help you tell the world.

https://www.globalencryption.org/events/ged/encryption-kept-me-safe/

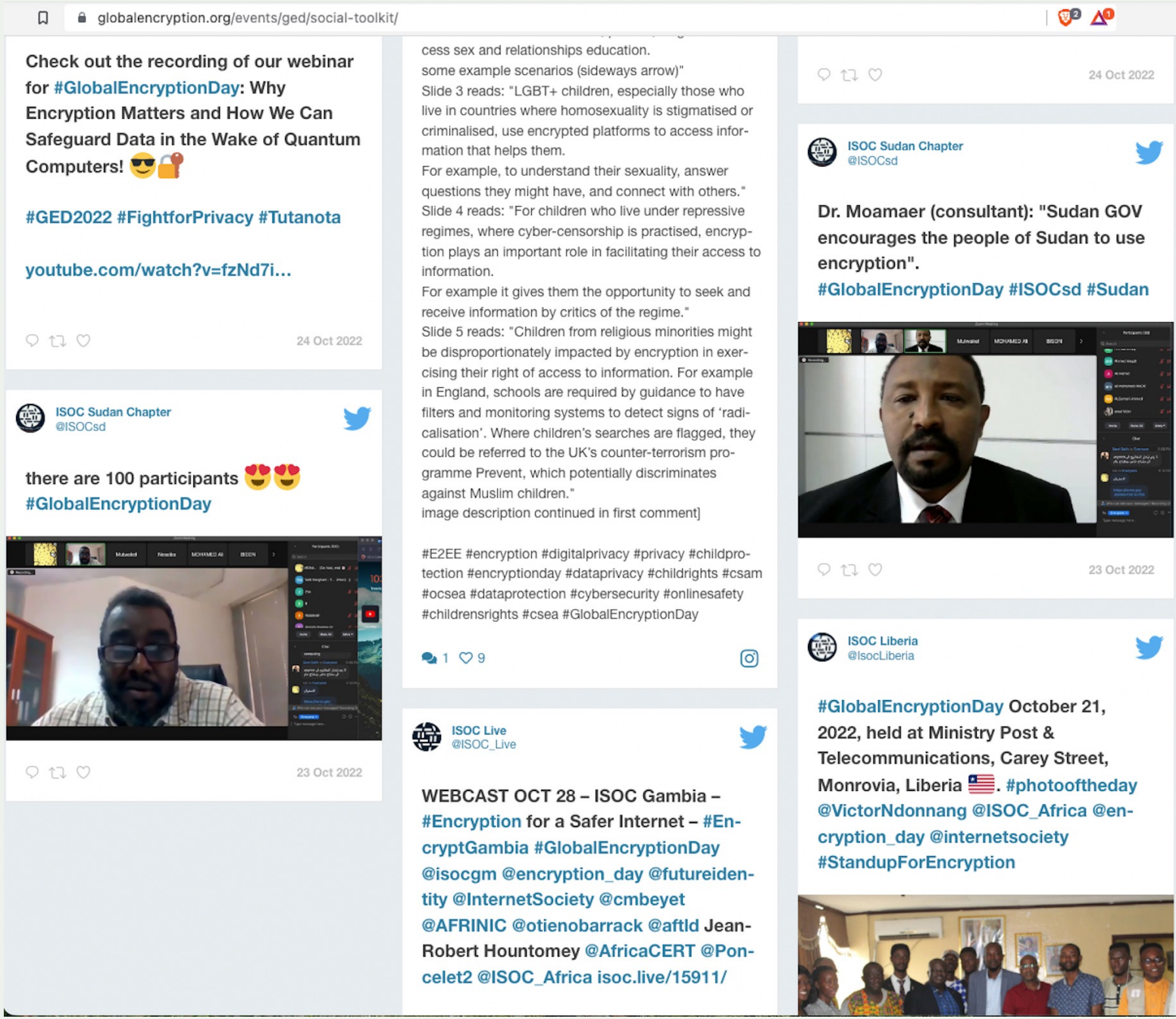
Resources and Next steps

The GEC Social Toolkit page contains user stories, video clips, updates, this year's game, but also

... it shows that if you join the effort to defend encryption, you are joining a world-wide movement on a huge scale.

https://www.globalencryption.org/events/ged/social-toolkit/

Encryption protects us:
we have to protect encryption.



ISOC Gambia Chapter Workshop
28th October 2022

Thank you

Robin Wilton - Director, Internet Trust
wilton@isoc.org