

Africa Chapters Workshop

# The Encryption Project And How You Can Use It



Robin Wilton - Director, Internet Trust

[wilton@isoc.org](mailto:wilton@isoc.org)

23rd September 2020

# Topics

- Project context
- Campaign approach
- Next steps



# Topics

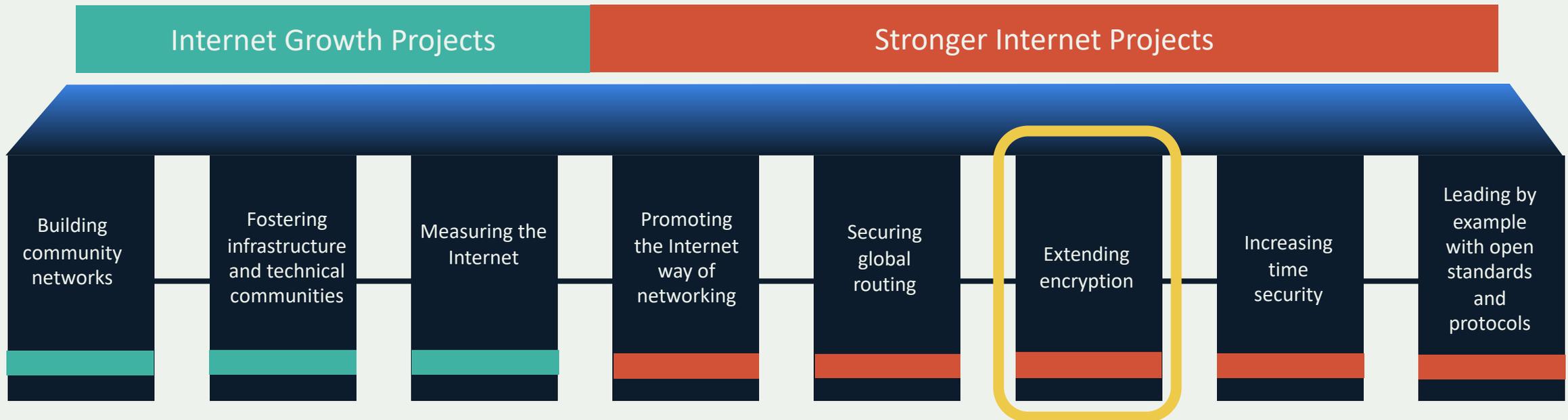
- Project context
- Campaign approach
- Next steps



# Where encryption fits

Internet Society mission statement:

*Working for an open, globally-connected, secure, and trustworthy Internet for everyone.*



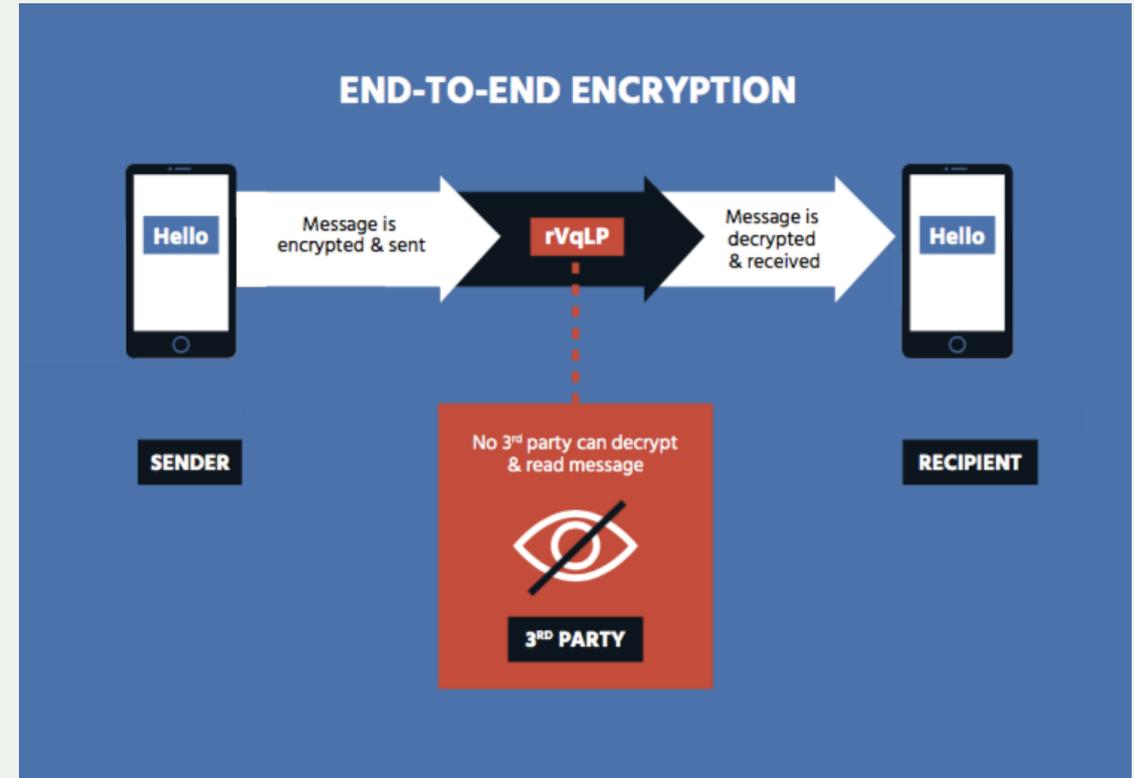
Encryption is a critical tool for the security of people, information and the Internet's infrastructure.

We are working with partners globally to support the use of strong encryption, and prevent dangerous attempts to prevent its implementation or weaken its effectiveness.



# Encryption basics

- **Encryption** is the process of scrambling or enciphering data so it can be read only by someone with the means to return it (decrypt) to its original state. It makes data secure.
- **End-to-end (E2E)** encryption is any form of encryption for data-in-transit in which only the sender and intended recipient (so not even the provider) can read the message.
- Encryption is a data security mechanism which provides data **confidentiality**, and underpins other data security services such as data **integrity**, digital **signatures** and **authentication**.



# Everyone relies on encryption

**Nearly everyone and every sector relies on encryption, and many on end-to-end encryption, whether they know it or not**

- Companies – financial and intellectual property
- Critical infrastructure – energy, water, and transportation
- Financial systems – including online banking
- Healthcare – private health information
- Law enforcement/military – activity and communications

**Undermining encryption puts personal and national security at risk**



We rely on encryption every day



**Web browsing:** Browsers and websites use HTTPS, an encrypted protocol, to provide secure communications, keeping our data from being read by criminals while in transit.



**E-commerce:** We trust companies to protect our financial information when we buy things online or use online banking. Encryption is an important method of doing that.



**Secure messaging:** When we use a messaging app, we expect the messages to be private. Some messaging apps use encryption to maintain the privacy and security of their users' communications while it is in transit. Others even use end-to-end encryption, so only the sender and receiver can read the messages, e.g. iMessage, WhatsApp, and Signal.

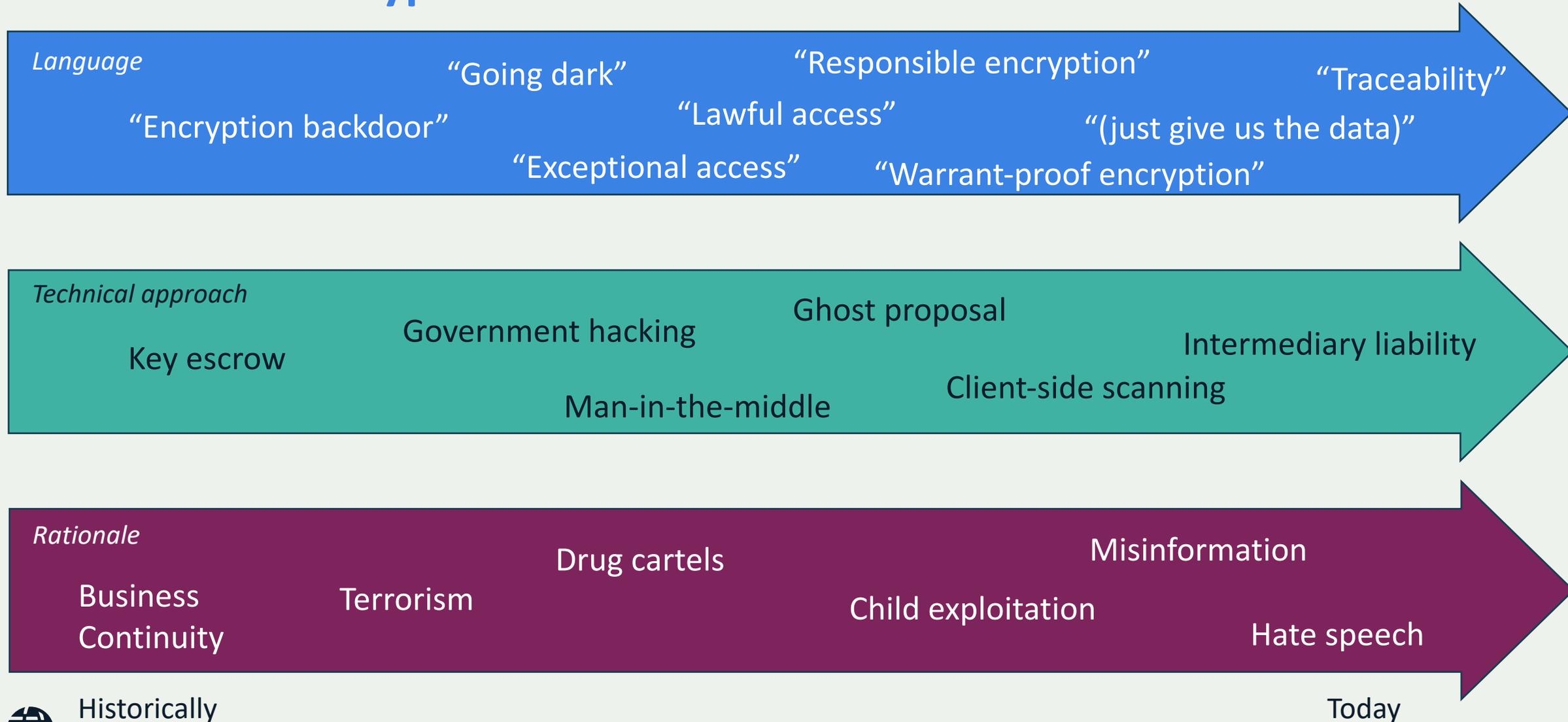
# Encryption secures your daily routine

- Remotely locking/unlocking your car
- Paying the right amount for petrol
- Making a card payment
- Entering the PIN for your phone or tablet
- Connecting your cellphone to the network
- Authenticating to your home wi-fi
- Making a video call to your family, friends or colleagues
- Browsing securely for online shopping
- Using a password or token to log in

*These daily tasks, and many more, depend on reliable encryption.*



# Evolution of encryption threats



# The danger with backdoors

- No matter the method, there is no such thing as secure “exceptional” access. **Criminals can and will discover and use the same way to get in. And the bad guys will just use another encrypted service to communicate!**
- It is effectively a vulnerability designed into the system, which undermines the security and trust of the affected systems.
  - Includes critical systems used by law enforcement and military
  - Though focused largely on messaging platforms, other services (banking, telehealth, e-commerce) are now integrated as well, so undermines critical communications
  - Can have negative economic impact on industry because of mistrust

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



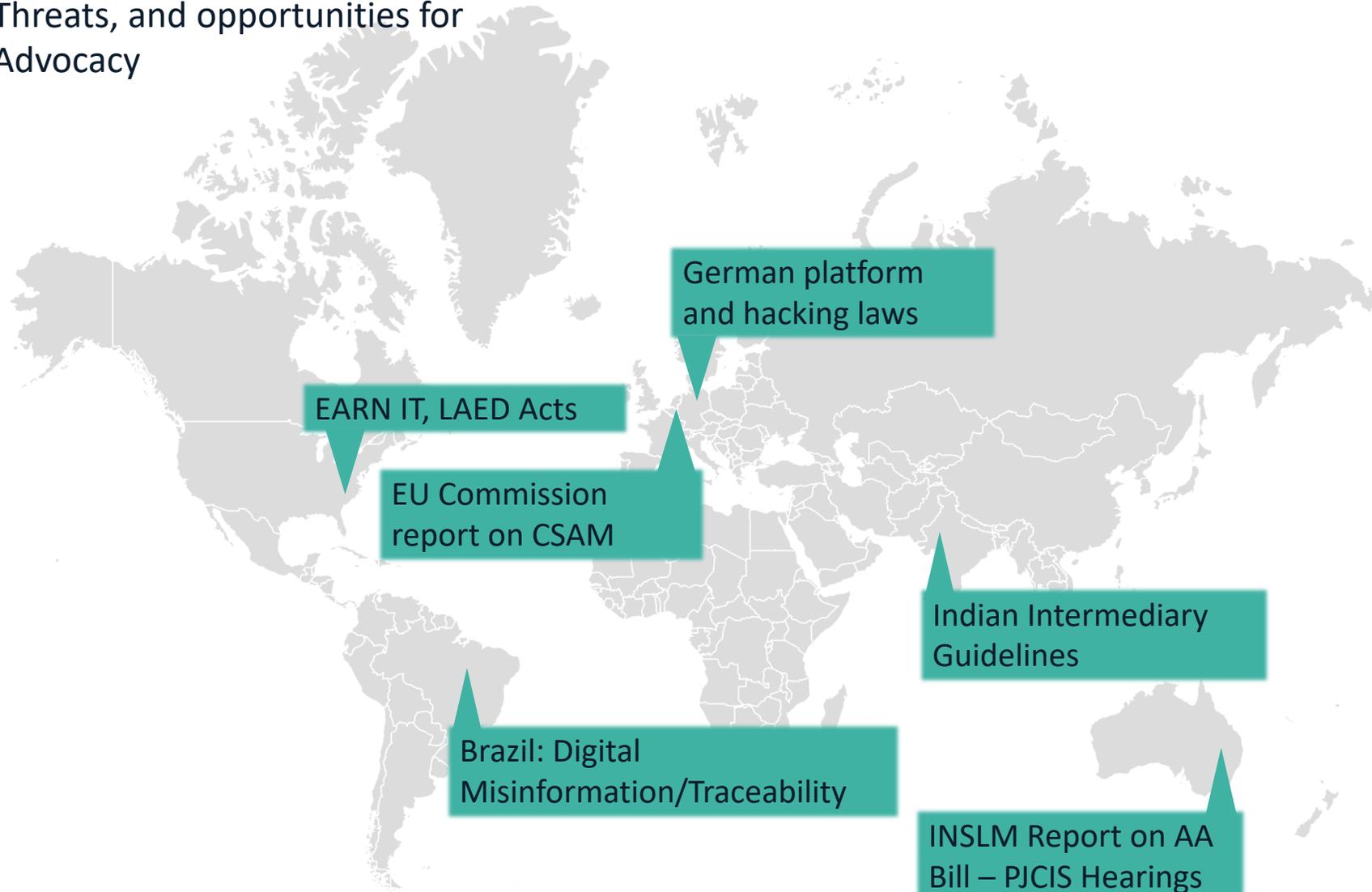
Investigatory Powers  
Act 2016



# Encryption “hotspots” – our weekly snapshot

For more information see: <https://www.internetsociety.org/issues/encryption/>

Threats, and opportunities for  
Advocacy



2020 target  
countries/regions:

- Australia
- Brazil
- Canada
- EU
- France
- Germany
- India
- UK
- US

# Topics

- Project context
- Campaign approach
- Next steps



# Campaign approach

## Thought Leadership

- Position ISOC as credible, unbiased and expert, with resources and content for target audiences

## Building a Movement

- Recruit supporters – ISOC community, partners, civil society, partners, coalitions
- Link to ISOC engagement goals

## Raising New Heroes

- Identify and equip champions to carry our message

## Mobilization & Advocacy

- Collaborating with and empowering community (chapters, partners, coalitions) to create change

*The common theme:*

- *Multiply our voices*
- *Amplify our influence.*



# Thought leadership – supporting content

The collage features several key documents:

- Man-in-the-Middle Attacks:** What are they, and how can we prevent them?
- Intermediaries and Encryption:** Pressuring intermediaries to weaken security is not the answer to prevent harmful content online.
- Ghost Proposals:** What are they, what is their impact, and can they achieve their goals?
- Government Hacking:** What is it and when should it be used?
- Encryption:** How It Can Protect Journalists and the Free Press.
- Encryption:** Essential for the LGBTQ+ Community.
- 3 Ways to ACT:** so your life won't be hacked.
- Virtual schooling:** 11 ways to keep your child safe online.
- Factsheet For Policymakers:** 6 Ways “Lawful Access” Puts Everyone’s Security At Risk.
- Client-Side Scanning:** What it is and why it threatens trustworthiness, private communication.

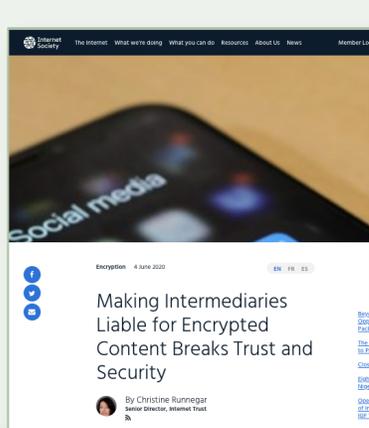
- Fact sheets to explain/counter various backdoor access approaches
- Partner-generated content highlighting importance of encryption
- Simple “explainers” in development



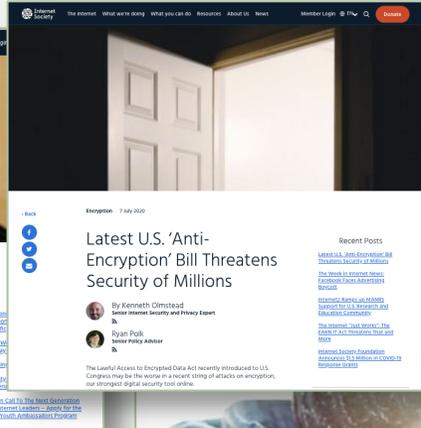
# Thought leadership – blogs, op-eds, webinars



**THE HILL**  
**Encryption helps America work safely — and that goes for Congress, too**  
BY RYAN POLK, OPINION CONTRIBUTOR — 03/31/20 06:00 AM EDT  
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL  
0 COMMENTS  
Just In...  
SHARE TWEET



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
Social media  
Encryption 4 June 2020  
**Making Intermediaries Liable for Encrypted Content Breaks Trust and Security**  
By Christine Runnegar  
Senior Director, Internet Trust



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
Latest U.S. 'Anti-Encryption' Bill Threatens Security of Millions  
By Kenneth Olmstead  
Senior Internet Security and Privacy Expert  
By Ryan Polk  
Senior Policy Advisor  
The Lawful Access to Encrypted Data Act recently introduced to U.S. Congress may be the newest in a recent string of attacks on encryption, our strongest digital security tool online.



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
**VPNs in the Age of COVID-19**



PowerPost  
PowerPost • Analysis  
**The Cybersecurity 202: Cybersecurity pros are uniting in a battle to save encryption**  
By Joseph Marks  
July 7 at 7:53 AM  
Cybersecurity and privacy advocates are rallying to defend strong encryption, which is facing its harshest assault in decades from the Trump administration and Congress.



Kids, the Internet & COVID-19: How to keep our ch...  
Watch later Share  
**Kids, the Internet & COVID-19: How to keep our children safe online**



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
**Kids Need Encryption Too**  
By Najielle Frai  
Senior Advisor, Public Policy



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
**There's No Duty of Care without Strong Encryption**  
By Kenneth Olmstead  
Senior Internet Security and Privacy Expert



SC MEDIA  
The Cyber-Security source  
HOME | NEWS & FEATURES | BUYER'S GUIDE | OPINION  
SCUK | SCUS  
TRENDING SC AWARDS EUROPE 2020  
**Now is not the time to put everyone's security on the line**  
Apr 30, 2020  
OPINION by Jeff Wilbur



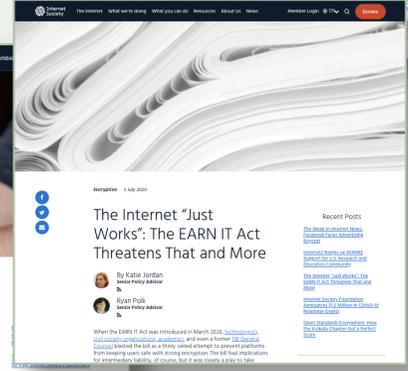
**Cybersecurity Experts Take Aim at Senators Over Encryption**  
GOP bill would open companies to more cyberattacks, they say  
Sen. Tom Cotton (R, Ark.) is one of three senators sponsoring The Encrypted Data Act, which is intended to help authorities track or communications.



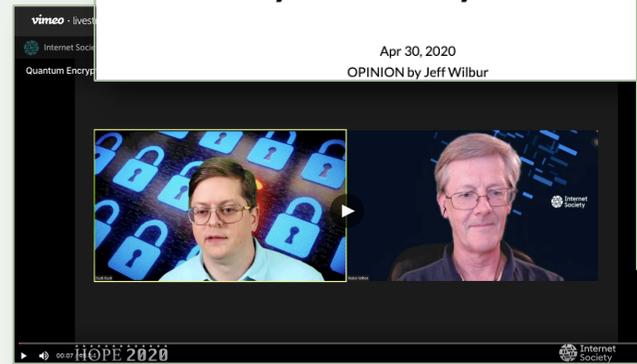
**O que o STF decidirá sobre a criptografia que nos protege online?**  
Supremo julga no dia 20/05 dos casos que tratam de legalidade dos bloqueios de WhatsApp ocorridos há alguns anos no Brasil



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
**Encryption: The Digital PPE We All Need**  
By Natalie Campbell  
Director, Community Organizing and Public Advocacy



Internet Society  
The Internet What we're doing What you can do Resources About Us News Member Login  
**The Internet "Just Works": The EARN IT Act Threatens That and More**  
By Kristie Jordan  
Senior Policy Advisor  
By Ryan Polk  
Senior Policy Advisor  
When the EARN IT Act was introduced in March 2020, it promised to protect children from online predators, and even a former U.S. Attorney General called it a "winning strategy to prevent child sexual exploitation." But it's a strategy that would strip away the very protections that have kept children safe from predators for decades.



Internet Society  
Quantum Encryption  
HOPE 2020



MORNING CONSULT  
**Encryption Is the Digital PPE the Health Care Industry Needs Now**  
BY KENNETH OLMSTEAD, GREG NOJEIM & CHARLES BRADLEY  
June 5, 2020 at 5:00 am ET  
A lack of personal protective equipment and ventilators are top of mind for doctors, nurses and hospital administrators on the front lines of the COVID-19 pandemic, and for good reason — lives hang in the balance each minute of each day. But that's not the only challenge straining health care providers still grappling with the outbreak of COVID-19 across the country.



# Building a movement – the Global Encryption Coalition

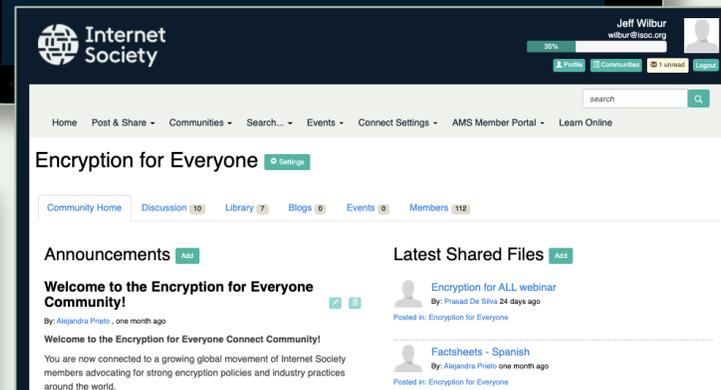
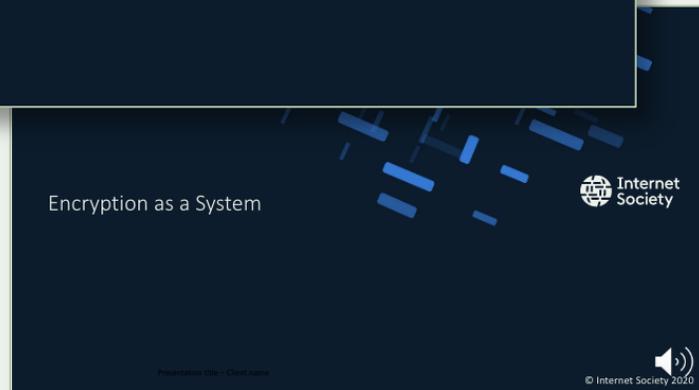


The mission of the Global Encryption Coalition is to promote and defend encryption in key countries and multilateral gatherings where it is under threat. It also supports efforts by companies to offer encrypted services to their users.

- Steering committee is Internet Society, Center for Democracy and Technology (CDT) and Global Partners Digital (GPD)
- Launched 14 May 2020 with series of five global webinars
- Started with 35 civil society members, now at 75 members and invitations in process to industry and technologists
- Actively supporting advocacy in UK, Brazil, Australia, India



# Raising new heroes – equipping



- Conducted chapter training in May
- Reached 120 people from 80 chapters, 83 did a follow up “initiative”
- Developing an eLearning encryption course for later this year



# Advocacy – mobilizing the community

**TC**  
Join Extra  
Crunch  
Login  
Search Q  
Disrupt SF 2020  
Startups  
Videos  
Audio  
Newsletters  
Extra Crunch  
The TC List **NEW**  
Advertise  
Events  
—  
More

## Over two dozen encryption experts call on India to rethink changes to its intermediary liability rules

Manish Singh @refsrc / 3:24 pm CST • January 9, 2020 Comment



**Image Credits:** PRAKASH SINGH / AFP / Getty Images

Security and encryption experts from around the world are joining a number of Indian experts to call on India to reconsider its proposed amendments to local intermediary liability laws. In an open letter to India's IT Minister Ravi Shankar Prasad on Thursday, cryptography experts warned the Indian government that if it goes ahead with the proposed changes to the law, it could weaken security and limit the use of the internet.

The Indian government proposed (PDF) a series of changes to its intermediary liability laws in late December 2018 that, if enforced, would require millions of service providers to trace the originator of questionable content to avoid assuming full liability for their users' actions.

The originally proposed rules say that intermediaries — which the government defines as those services that facilitate communication between two or more users or more users in India — will have to proactively monitor and filter their content. They will also be able to trace the originator of questionable content to avoid assuming full liability for their users' actions.

## Internet Society Open Letter Against Lawful Access to Encrypted Data Act

July 7, 2020

The Honorable Lindsey Graham  
Chairman, Senate Committee on the Judiciary

The Honorable Marsha Blackburn  
Senate Committee on the Judiciary

The Honorable Tom Cotton  
Senate Committee on the Judiciary

Dear Senators Graham, Blackburn, and Cotton:

The undersigned organizations and security experts from civil society, industry and academia express our strong opposition to the Lawful Access to Encrypted Data Act, S. 4051. The bill's language as drafted is seriously flawed and could endanger public and national security.

Tip Off Advertise Support Us My Account

**MEDIANAMA** Audit-ready cybersecurity compliance. A single source for your cyber liability, documentation needs. **COMPLIANCE FORGE** PURCHASE ONLINE

HOME EXPERT VIEWS POLICY EVENTS VIDEOS BUY OUR REPORTS

### Encryption and issues related to Terrorism and Communications

Aditi Agrawal

Tip Off Advertise Support Us My Account

**MEDIANAMA** **Shark Rocket Zero-MV** Pet Hair? No Problem Powerful Cleaning

HOME EXPERT VIEWS POLICY EVENTS VIDEOS BUY OUR REPORTS

HOME / NEWS

Home terror

By Nikhil Patil

### Encryption and issues related to Child Protection online

Nikhil Patil

"Trace but try to speak the tech the pre-technic The text from the dis attribb

Tip Off Advertise Support Us My Account

**MEDIANAMA** **Square Online Store** Launch a free online store

HOME EXPERT VIEWS POLICY EVENTS VIDEOS BUY OUR REPORTS

Home • June 2020 • June 15, 2020

By Soumyarendra Barik

"When I WhatsApp web, inc the mat identity the mail upload I problem it at a D This wo was und

### Encryption and issues related to Misinformation

Soumyarendra Barik

Home • Encryption, Intermediary Liability, Misinformation, NAMA Encryption June 2020

By Soumyarendra Barik ( @imsoumyarendra soumyarendra@medianama.com ) June 15, 2020

Share This: f t in Share via Email

**DAILY NEWSLETTER**  
Enter your email address

**HEADLINES**

- COVID-19: Swiggy lays off another 350 employees
- Parliamentary Committee focusses on exemptions for govt agency under Data Protection Bill
- Emails reveal how the government finalised exemptions for deploying drones for COVID-19
- Bombay Flying Club becomes India's first DCA approved drone training

"In discussions on misinformation, we generally focus on what the government and platforms should do, when in fact it is a people problem, as much as it is a tech problem. People generally don't have the agency to act on some of these problems. So how do you empower everyday people to actually respond to misinformation is the bigger question," a speaker said during MediaNama's workshop on identifying challenges to Encryption in India. Traceability emerged as perhaps the biggest challenge to encryption, but several speakers questioned its effectiveness in curbing misinformation.

This workshop was held with support from the Internet Society (Asia Pacific Office), and was under the Chatham House rule; the quotes have thus not been attributed.



# Topics

- Project context
- Campaign approach
- Next steps – audience participation ;^)



Je peux prendre votre température, svp?  
Le chiffrement: sujet incendiaire chez vous?

Can I take your temperature, please?  
How "hot" is encryption as a policy topic?

Incendiaire – gardez votre distance!

5

Inflammatory – keep away!

Fébrile – vaut mieux éviter le sujet

4

Feverish – it's best to avoid the subject

Quelques ennuis, mais abordable

3

Of concern, but we can still discuss it

Normale – on peut le discuter sans mal

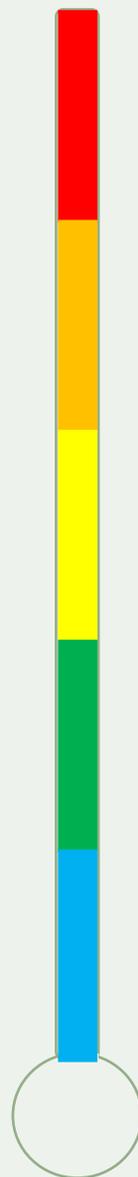
2

Normal – we can have a healthy discussion

Froid – on s'en fiche

1

Cold – no-one really cares



## Quel traitement vous faudrait-il?

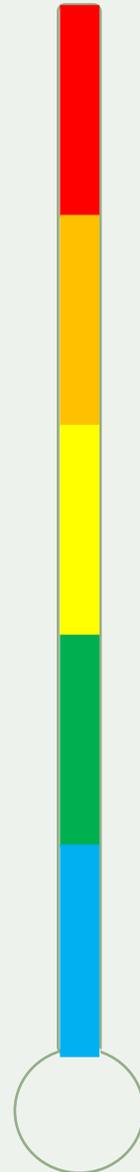
Mobilisation: amener les décideurs au débat

Assurer la disponibilité de chiffrement fiable

Pratique: comment sauvegarder ma vie en ligne

Exemples – où le chiffrement soutient ma vie

Sensibilisation à l'importance du chiffrement



## What treatment do you need?

Advocacy: bringing policymakers to dialogue

Ensuring reliable encryption is available

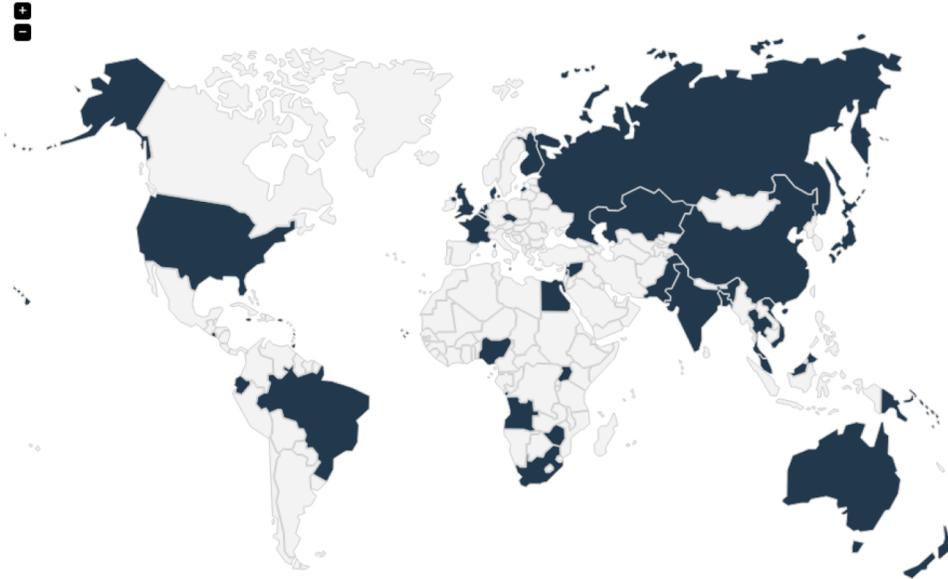
Practicality: how to stay safe and secure online

Examples – where encryption helps my life

Awareness-raising: that encryption is important

(non exclusive poll?)

|  |  |                                       |                          |
|--|--|---------------------------------------|--------------------------|
| General right to encryption ⓘ                    | Mandatory minimum or maximum encryption strength ⓘ | Licensing/registration requirements ⓘ | Import/export controls ⓘ |
| Obligations on providers to assist authorities ⓘ | Obligations on individuals to assist authorities ⓘ | Other restrictions ⓘ                  |                          |



**LIST OF COUNTRIES**

Select a country

- Maps are a great way to communicate and understand
- Help populate the global encryption “status map” hosted by Global Partners Digital:
  - <https://www.gp-digital.org/world-map-of-encryption/>
  - (Email updates to richard{at}gp-digital.org )



# Join us

## 1. Chapters: please join the Global Coalition on Encryption

- [https://docs.google.com/forms/d/e/1FAIpQLScQJIEFE76JKB2l3SF53x8U2Rr6r1cghC5\\_fZ1kXG9hl8gTfw/viewform](https://docs.google.com/forms/d/e/1FAIpQLScQJIEFE76JKB2l3SF53x8U2Rr6r1cghC5_fZ1kXG9hl8gTfw/viewform)

## 2. Everyone: please recruit organizations to join the Global Coalition on Encryption

- [https://docs.google.com/forms/d/1Hk\\_xGJU7RMuRyTpoCgEEL1gQ5656JQ8ibeHr2p1pMQ/viewform?ts=5f15e2be&edit\\_requested=true](https://docs.google.com/forms/d/1Hk_xGJU7RMuRyTpoCgEEL1gQ5656JQ8ibeHr2p1pMQ/viewform?ts=5f15e2be&edit_requested=true)

## 3. Take advantage of the Encryption training materials on Connect

- <https://connect.internetociety.org/communities/community-home?communitykey=3d65736e-0336-43f0-a6c2-9642132601b7>

Watch the Chapter Delegates' list for details of our next Encryption webinar.



# Thank you.

For more information, email [encryption@isoc.org](mailto:encryption@isoc.org)

Encryption home page:

<https://www.internetsociety.org/issues/encryption/>

Connect Community page

<https://connect.internetsociety.org/communities/community-home?communitykey=3d65736e-0336-43f0-a6c2-9642132601b7>

