Africa Chapters Workshop

The Encryption Project And How You Can Use It

Robin Wilton - Director, Internet Trust
wilton@isoc.org
23rd September 2020

Topics

- Project context
- Campaign approach
- Next steps

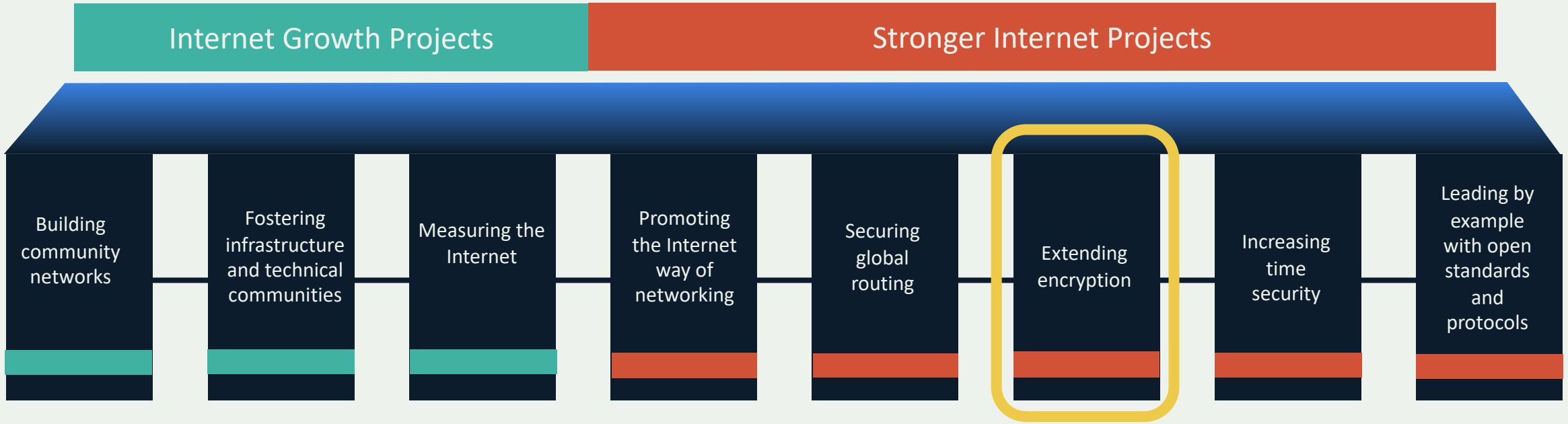
Topics

- Project context
- Campaign approach
- Next steps

Where encryption fits

Internet Society mission statement:

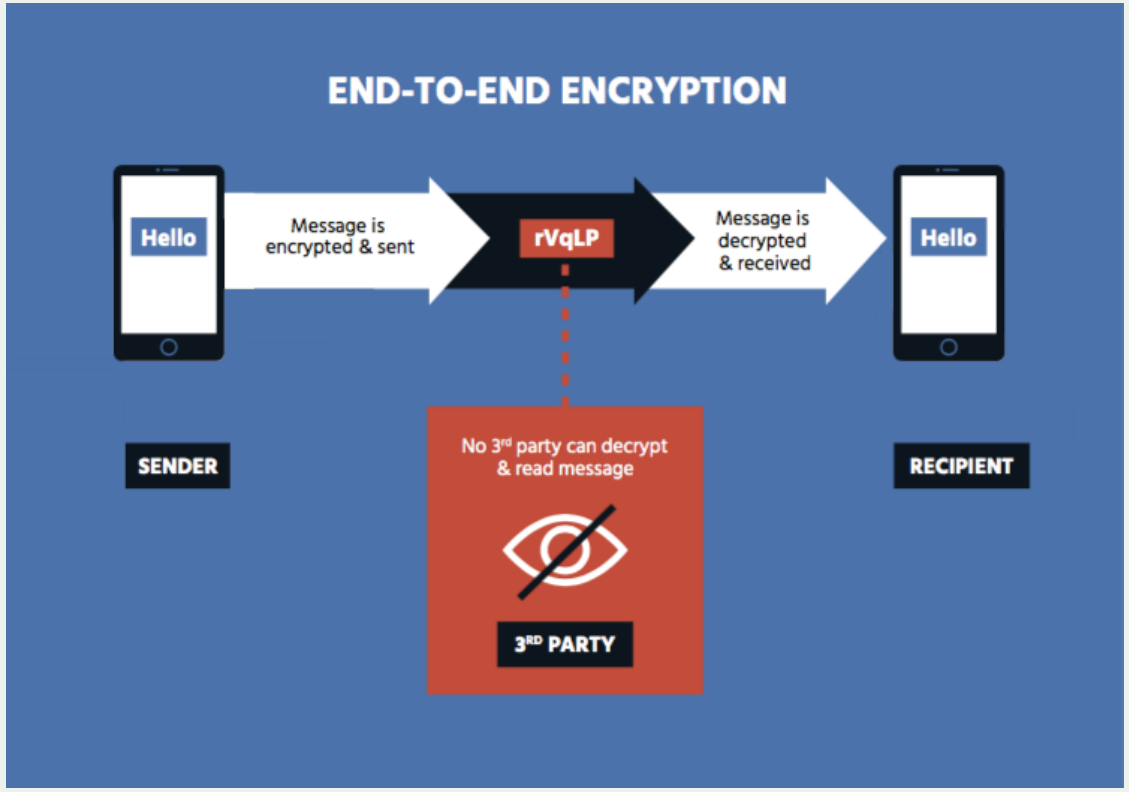
Working for an open, globally-connected, secure, and trustworthy Internet for everyone.



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.

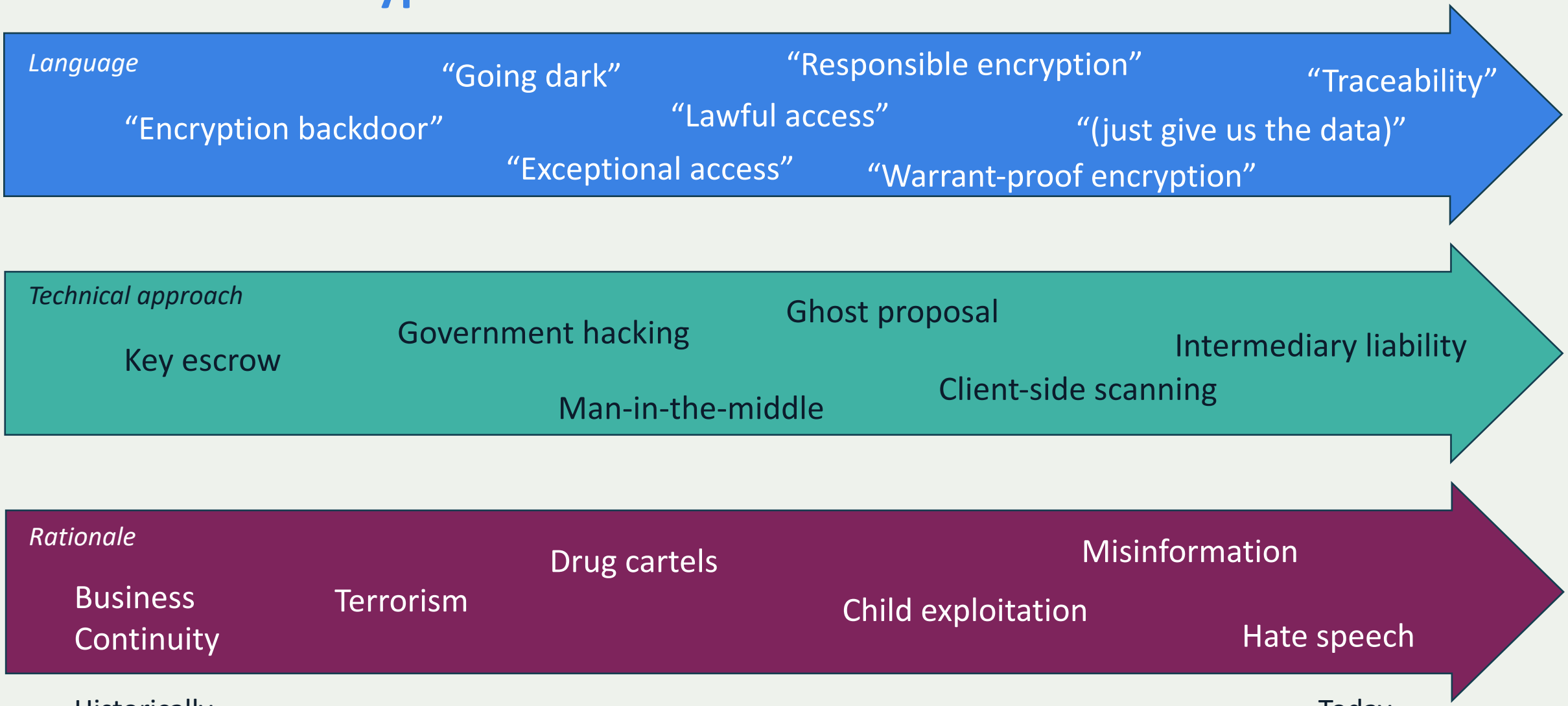
Secure messaging: When we use a messaging app, we expect the messages to be private. Some messaging apps use encryption to maintain the privacy and security of their users' communications while it is in transit. Others even use end-to-end encryption, so only the sender and receiver can read the messages,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



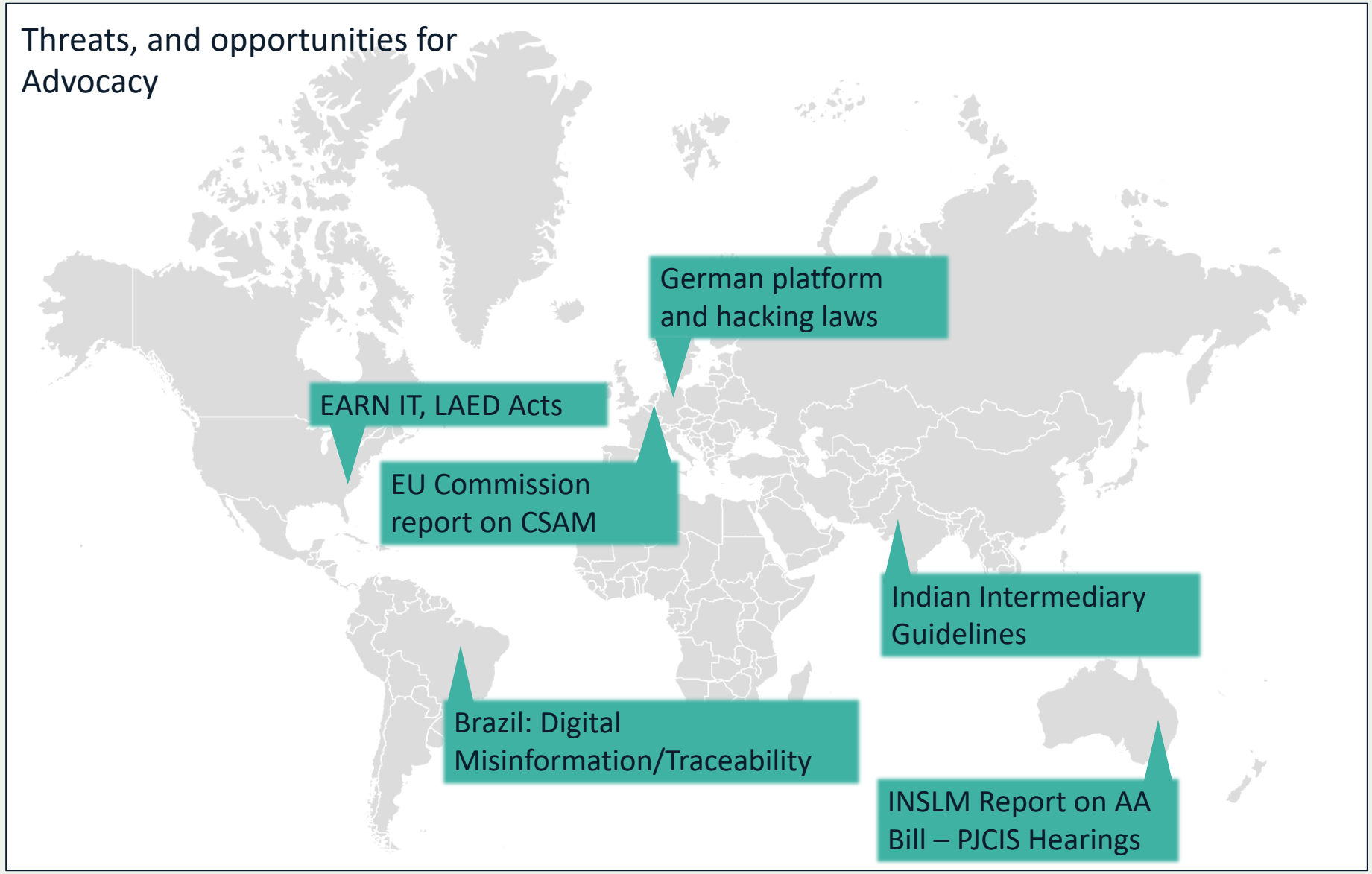
The danger with backdoors

- **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.

Encryption “hotspots” – our weekly snapshot

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



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

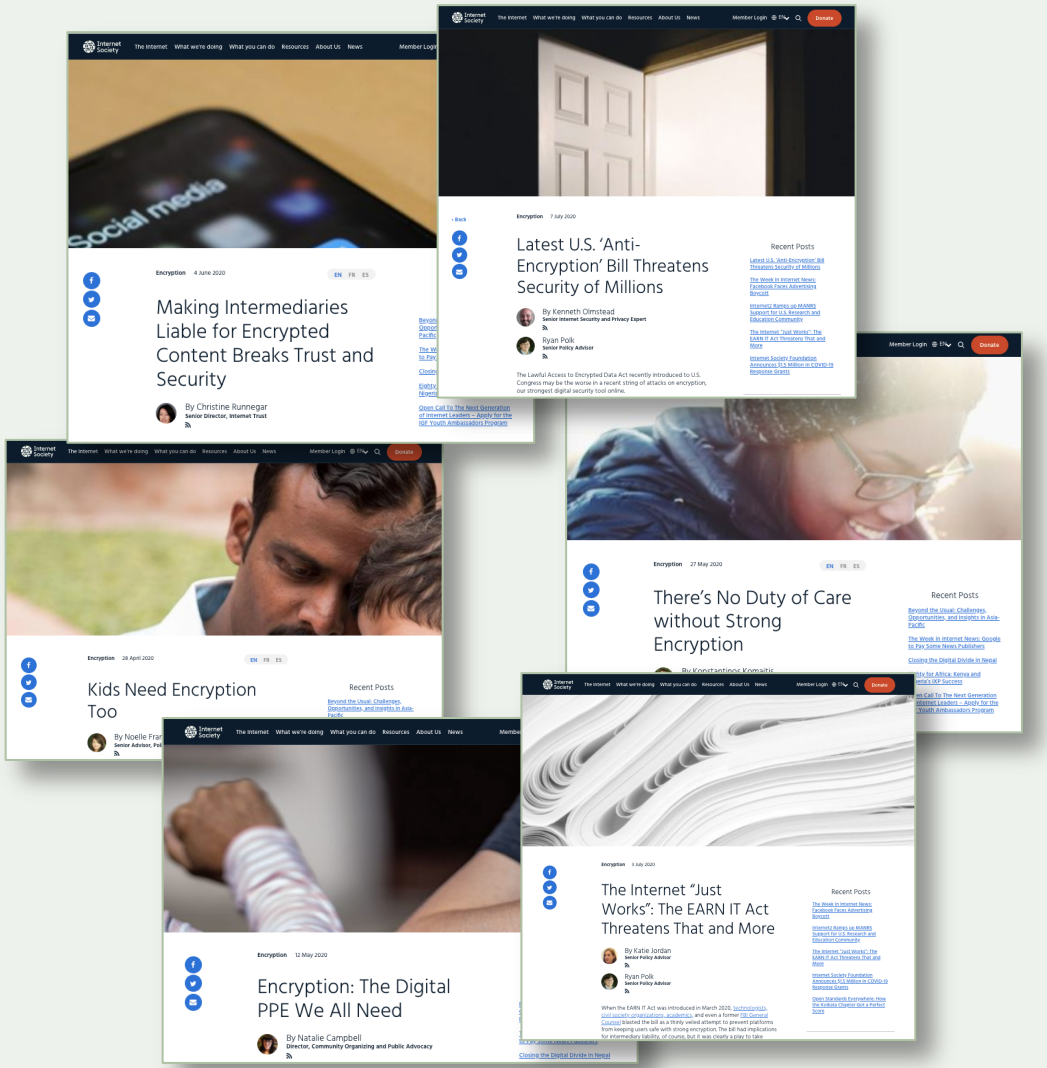
The common theme:

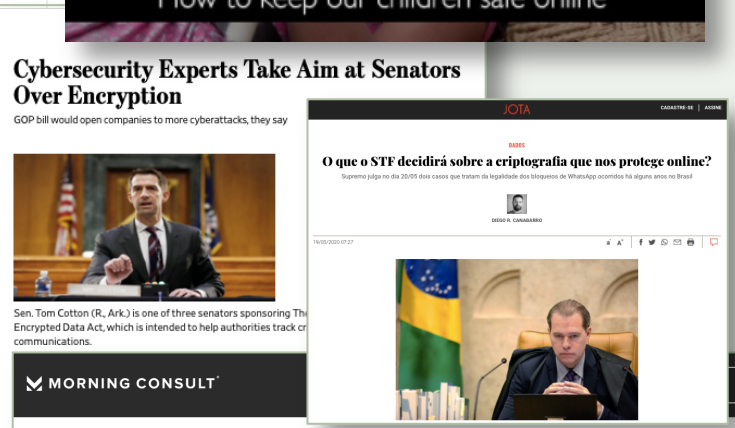
- ***Multiply our voices***
- ***Amplify our influence.***

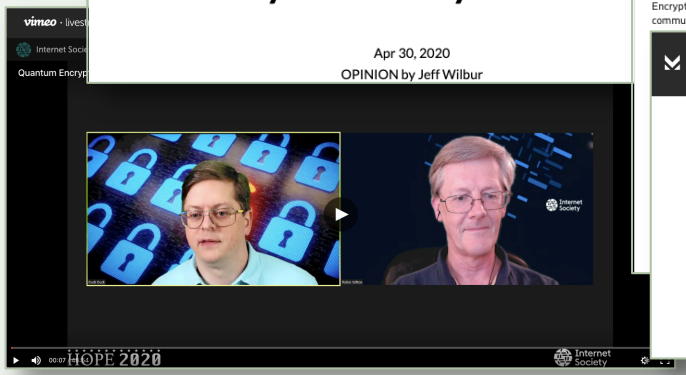
Thought leadership – supporting content

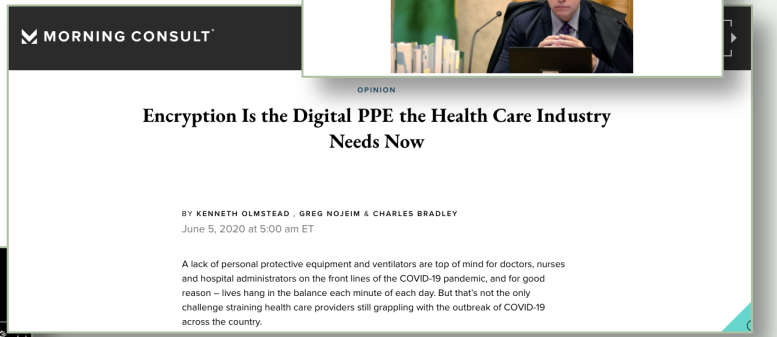
- Fact sheets to explain/counter various backdoor access approaches
- Partner-generated content highlighting importance of encryption
- Simple "explainers" in development

Thought leadership – blogs, op-eds, webinars







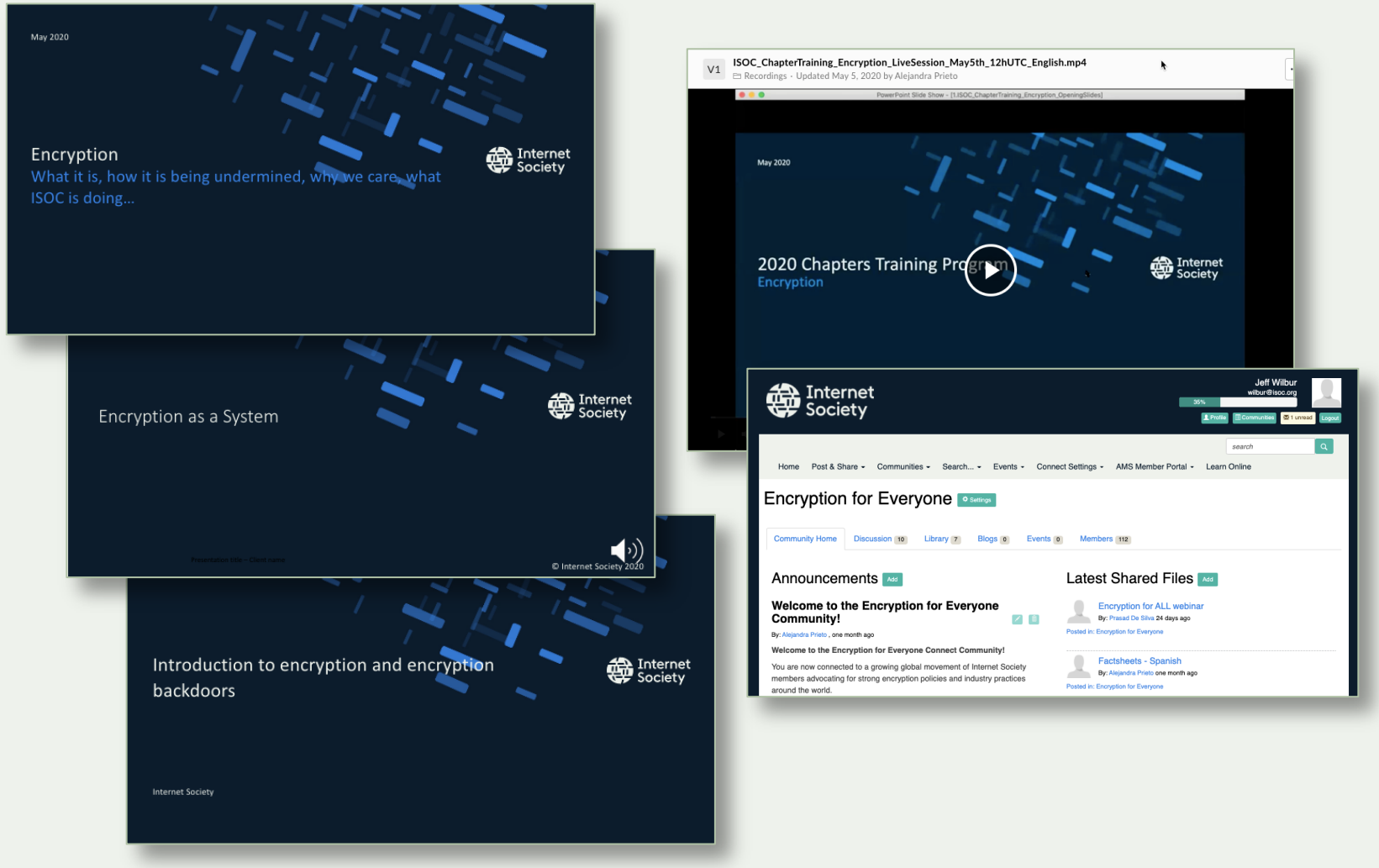


Building a movement – the Global Encryption Coalition

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.

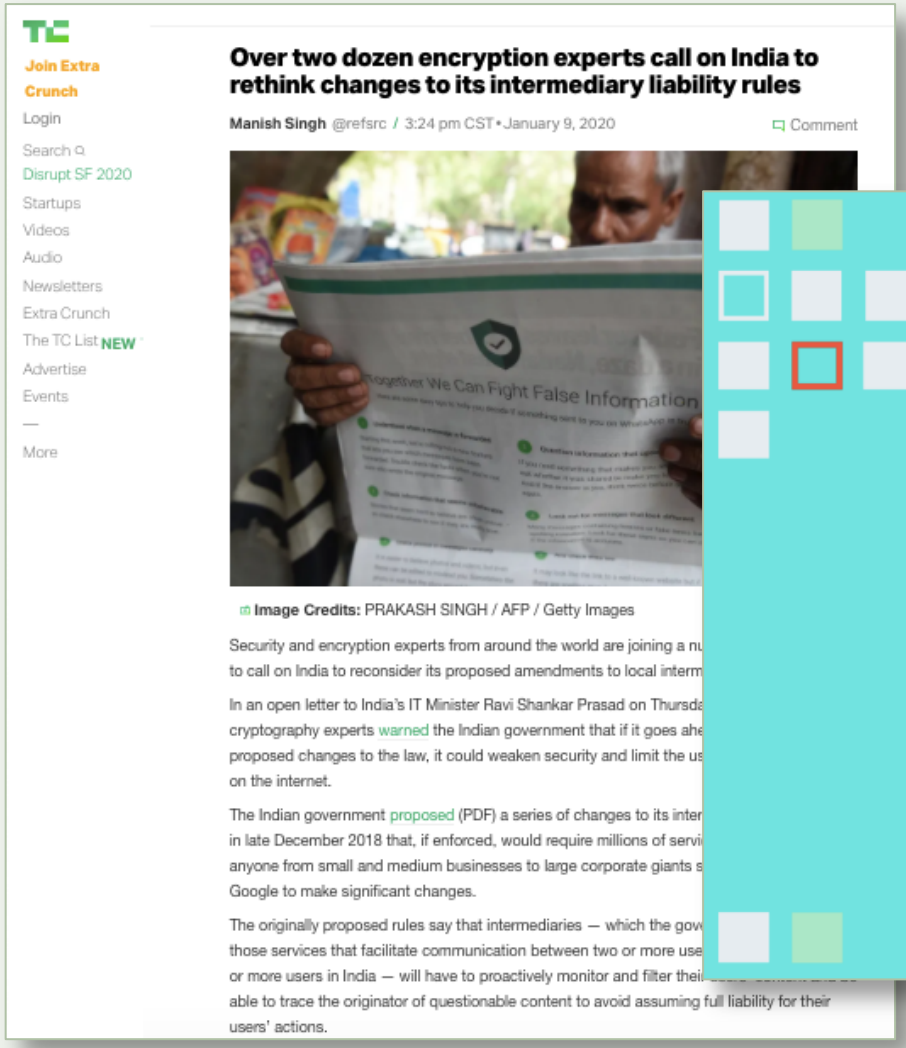
- Steering committee is Internet Society, Center for Democracy and Technology (CDT) and Global Partners Digital (GPD)
- Launched 14 May 2020 with series of five global webinars
- Started with 35 civil society members, now at 75 members and invitations in process to industry and technologists
- Actively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

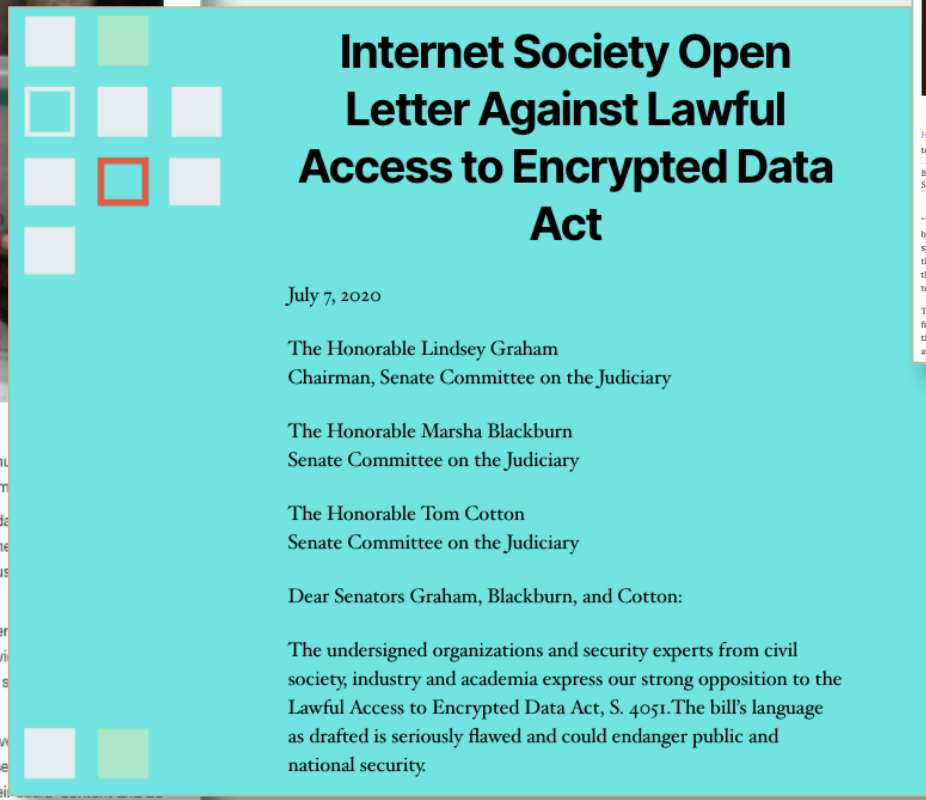
Image Credits: PRAKASH SINGH / AFP / Getty Images

Security and encryption experts from around the world are joining a nu
to call on India to reconsider its proposed amendments to local interm

In an open letter to India's IT Minister Ravi Shankar Prasad on Thursda
cryptography experts warned the Indian government that if it goes ahe
proposed changes to the law, it could weaken security and limit the us
on the internet.

The Indian government proposed (PDF) a series of changes to its inter
in late December 2018 that, if enforced, would require millions of servi
anyone from small and medium businesses to large corporate giants s
Google to make significant changes.

The originally proposed rules say that intermediaries — which the gov
those services that facilitate communication between two or more use
or more users in India — will have to proactively monitor and filter thei
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

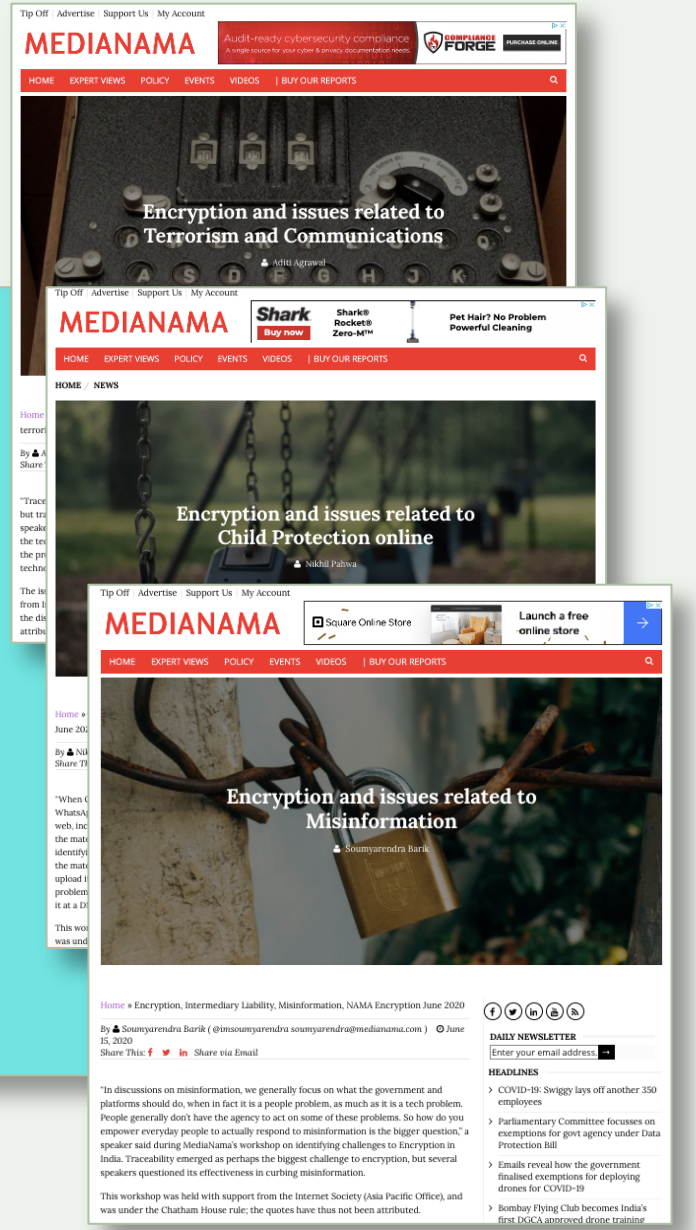
The Honorable Lindsey Graham
Chairman, Senate Committee on the Judiciary

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

HOME | EXPERT VIEWS | POLICY | EVENTS | VIDEOS | BUY OUR REPORTS

Encryption and issues related to Terrorism and Communications

Aditi Agrawal

Encryption and issues related to Child Protection online

Nikhil Pahwa

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

"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.

DAILY NEWSLETTER

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 DGCA approved drone training

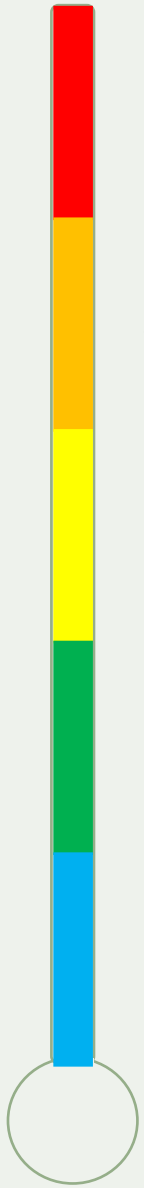
Topics

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

Je peux prendre votre temperature, 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?

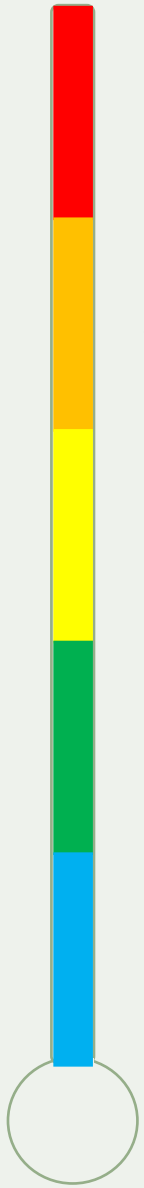
Mobilisation: amener les décideurs au débat

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

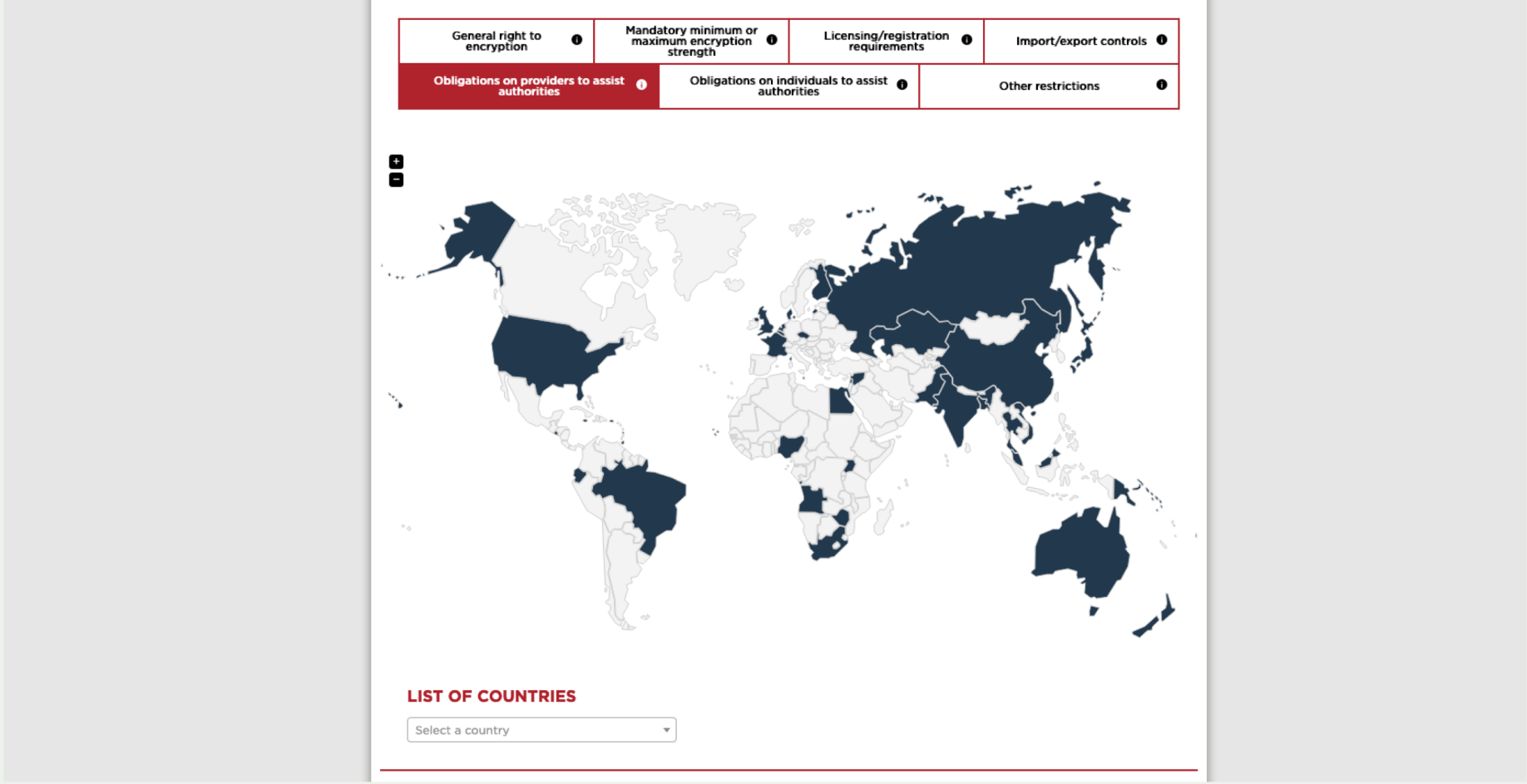
Ensuring reliable encryption is available

Practicality: how to stay safe and secure online

Examples – where encryption helps my life

Awareness-raising: that encryption is important

(non exclusive poll?)



- 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/1FAIpQLScQJlEFE76JKB2l3SF53x8U2Rr6r1cghC5_fZ1kXG9hl8gTfw/viewform
2. Everyone: please recruit organizations to join the Global Coalition on Encryption
   - https://docs.google.com/forms/d/1Hk_xGJUp7RMuRyTpoCgEEL1gQ5656JQ8ibeHr2p1pMQ/viewform?ts=5f15e2be&edit_requested=true
3. Take advantage of the Encryption training materials on Connect
   - https://connect.internetsociety.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

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