November 8, 2023

Cybersecurity Workshop: Panel on Encryption

Jon Camfield
Meta

Ruth Babette Ngene
Electronic Frontier Foundation

Greg Nojeim
Center for Democracy & Technology

Brianne Powers *(Moderator)*
Paul Hastings, LLP

Privacy+ Security Forum

Speakers

Brianne Powers

Senior Privacy Director & Chief Privacy Officer
Paul Hastings, LLP

Ruth Babette Ngene

Director, Public Interest Technology
Electronic Frontier Foundation
Organization

Jon Camfield

Product Policy, Threat Ideation
Meta

Greg Nojeim

Senior Counsel & Director of Security and Surveillance Project
Center for Democracy & Technology

Encryption in the U.S.

Historical Context

Privacy+ Security Forum

The good

- It’s a basic human right to have a private conversation. To have those rights realized in the digital world, the best technology we have is end-to-end encryption.
- We are more encrypted than ever. Let’s Encrypt , Signal, our devices, phones, means a much higher percentage and internet traffic are encrypted and difficult to surveil.
- There is greater public understanding around encryption issues.

Historical Context

The not so good

It is déjà vu all over again

- **The Clipper Chip Plan (1993):** The Clinton White House introduced the Clipper Chip, a plan for building in hardware backdoors to communications technologies. The chip would be used in American secure voice equipment, giving law enforcement agencies the explicit ability to decrypt its traffic using a key stored by the government. The White House promised that only law enforcement with proper "legal authorization" could access that key—and thus, the contents of the communications.

- **Bernstein vs Department of Justice (1999):** In the 1999 decision throwing out the government's export regulations on encryption in EFF's case *Bernstein v. Department of Justice*, the Ninth Circuit Court of Appeals noted: "The availability and use of secure encryption may…reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights…but also the constitutional rights of each of us as potential recipients of encryption's bounty."

- **SaveCrypto (2015)**: On September 30, along with Access Now , we launched SaveCrypto.org as a way to let the public have its voice heard. Over 104,000 people signed on to a statement rejecting "any law, policy, or mandate that would undermine our security" and demanding "privacy, security, and integrity for our communications and systems."

What's Happening Now?

- **The EARN IT ACT (2020-2022):** The EARN IT Act is intended to eliminate CSAM on internet platforms by creating a government commission tasked with creating "best practices" for running an internet website or app. The act then removes nearly 30-year-old legal protections for users and website owners, allowing state legislatures to encourage civil lawsuits and prosecutions against those who don't follow the government's "best practices," including scanning everyone's private conversations for illegal material.

- **STOP CSAM ACT (2023):** Similar to the EARN IT in it goal to remove from the internet CSAM materials, The STOP CSAM Act creates criminal and civil liability for platforms that "recklessly" allow sharing of illegal material, and the fact they offer encryption can be used as evidence of recklessness. As with EARN IT, the bill will discourage the use of end-to-end encryption.

- **Cooper Davis (2023):** Requires providers to report their users to the Drug Enforcement Administration (DEA) if they find out about certain illegal drug sales and allows for penalties if providers "deliberately blind" themselves to this content. Given the possibility that encryption could be used as evidence of such blindness, it discourages providers from allow users to have private conversations even about entirely legal subjects related to drugs.

Issues with Proposed Legislation

Privacy+ Security Forum

- These bills target intermediaries and allow private plaintiffs, law enforcement, and attorneys general to sue for CSAM on platforms, even if the platform encrypts content.

- It's an indirect attack on end-to-end encryption, since compliance will push companies towards using Client-Side Scanning (CSS) to become compliant.

EFF Proposals

Privacy+ Security Forum

- Get a warrant: Law enforcement and the government should respect due process and the 4th Amendment.
- While a search warrant may not give police access to an encrypted devices, getting informed consent from users to access that data is often effective.
- Technology companies need robust reporting tools that flag illegal content and activities.
- Proactively educate users on detecting and reporting digital crimes.

Protecting Encryption

Privacy+ Security Forum

- Take action: https://act.eff.org/
- Use encryption and encourage others to do so: use Signal and other privacy protecting technologies in your communications.
- Keep yourself Informed:
  - Follow the Electronic Frontier Foundation (EFF), the Center for Democracy and Technology (CDT), AccessNow, and the Global Encryption Coalition.

Global Challenges To Encryption

Privacy+ Security Forum

End-to-End Encryption

Privacy+ Security Forum

- A service is fully encrypted end-to-end if:
  - only the sender
  - and the intended recipient(s)
  - can understand information communicated.

- The intermediary who provides the service is neither sender nor recipient.

Duties of Intermediaries

- Governments increasingly task intermediaries with duties to moderate content (they cannot understand) to advance important societal goals:
    - Stop the spread of Child Sexual Abuse Material
    - Thwart on-line terrorist recruiting
    - Prevent trade in fentanyl and other illicit drugs
    - Address other illegal or harmful on-line conduct

UK: Online Safety Act

- Providers of user-to-user services have “duty of care”
- Must monitor for Child Sexual Exploitation and Abuse (CSEA)
  - Images
  - Grooming
- They can use technology they develop, but if it is not effective
- UK regulator, Ofcom, can require use of “accredited technology”.
- In an E2EE system, monitoring not possible with current technology.

Proposed EU CSAM Regulation

Privacy+ Security Forum

- Regulation proposed by European Commission going through legislative process.
- Once adopted, has legal force w/o further Member State action.
- Imposes duties on online hosting and interpersonal comms. services
- Detect, report, remove
- Known CSAM, new CSAM, grooming
- Inconsistent with end-to-end encrypted services

Advocacy Response

Privacy+ Security Forum

Global Encryption Coalition

- Promote pro-encryption policies at governmental level, and encryption adoption at the corporate level
- 3 years old
- 330+ members
- Engaging in EU, UK, Australia, India, Brazil, Turkey
- Steering Comm: CDT, GPD (UK), Mozilla, IFF (India), ISOC
- www.globalencryption.org

Advocacy Response

Privacy+ Security Forum

Global Encryption Day

- Annually, on October 21
- Over 50 encryption-related events around the world
- ”Summit” drew participants from 79 countries

Ongoing Advocacy Efforts

Encryption in Action

Questions & Contacts

Brianne Powers

Senior Privacy Director & Chief Privacy Officer
Paul Hastings, LLP

Ruth Babette Ngene

Director, Public Interest Technology
Electronic Frontier Foundation
Organization

Jon Camfield

Product Policy, Threat Ideation
Meta

Greg Nojeim

Senior Counsel & Director of Security and Surveillance Project
Center for Democracy & Technology