THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 2

The costs of mandated access on the borderless digital economy

PROMPT

When laws require that companies change their way of doing business in order to facilitate surveillance, it often adds economic, reputation, and legal costs. These costs include the cost of building new or different infrastructure, or restructuring supply or service chains for different jurisdictions around the world; the costs of defending a company against questionable court orders or fighting gag orders and other restrictions on transparency; and the more amorphous costs of violating human rights, deteriorating user trust, and losing business as a result. Discussants in this track will attempt to explore these costs and discuss means and methods for measuring their impact on end users.

DISCUSSION LEADERS

Christian Dawson, i2Coalition

Holly Kilroy, Security First

WORKSHOP LEADERS

Nick Sullivan, CloudFlare

Nighat Dad, Digital Rights Foundation

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

Key Outcome: Track participants segmented industry into layers through which to define costs, and examined costs for each of those segments. The track further provided guidance for what additional information and research is necessary to quantify these costs across industry.

This track attempted to identify the costs, both direct and indirect, that would accompany a mandate for a company to provide exceptional access to law enforcement. We began by attempting to define how to identify a cost and who would pay these costs. Generally, we found that costs fell within three main themes, economic, political, and human.

To identify and define these costs we examined five different ecosystems: the telecom environment; the ISP level; the application and content layer; end user device layer; and the end users themselves:

Layer 1: The telecom environment

- Cost of doing business

Layer 2: The ISP level

- Technology costs
- Personnel to handle government requests
- Reputational costs
- Coding and developer costs
- "Brain drain"
- Velocity
- Global competitiveness
- Environmental costs
- Regulatory burden
- Legal costs
- Increased risk

Layer 3: Application and content layer

- Generally identical to the ISP level
- Data breaches and civil liability

Layer 4: End-user devices

- Security loss
- Remediation costs
- Security updates
- Security research costs
- The "slippery slope"
- Banalization
- Control

Layer 5: Users

- Trust
- Free speech and self-censorship
- Diplomatic costs
- Innovation
- Legal rights
- Privacy and other human rights
- Shrinking of civil society
- Shrinking economy and lack of choice

THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 2

The costs of mandated access on the borderless digital economy

PROMPT

When laws require that companies change their way of doing business in order to facilitate surveillance, it often adds economic, reputation, and legal costs. These costs include the cost of building new or different infrastructure, or restructuring supply or service chains for different jurisdictions around the world; the costs of defending a company against questionable court orders or fighting gag orders and other restrictions on transparency; and the more amorphous costs of violating human rights, deteriorating user trust, and losing business as a result. Discussants in this track will attempt to explore these costs and discuss means and methods for measuring their impact on end users.

DISCUSSION LEADERS

Christian Dawson, i2Coalition

Holly Kilroy, Security First

WORKSHOP LEADERS

Nick Sullivan, CloudFlare

Nighat Dad, Digital Rights Foundation

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

Some of these costs are amorphous. However, some are more measurable. For example, infrastructure/development costs associated with multiple supply chains and differing legal requirements and legal costs to comply with local restrictions. In order for us to measure these costs more fully, we need a functional competitive environment. Unfortunately, this healthy ecosystem does not exist at the telecom layer. It is therefore difficult to accurately gauge costs, especially without access to proprietary corporate information, which may not be standard across the industry. However, we are hopeful that there are competitive environments at the provider level, at the app and content level, and at the end user device level.

To try to work toward quantification of these costs, we examined what information exists and what research is necessary in order to measure these costs for companies, governments, and users. We focused on four specific types of costs: **Global Competitiveness**, **Risk**, **Consumer Trust**, and **Physical Harm**. We placed our focus on determining indicators; that is, information that is relevant and necessary to measuring the overall cost. The group recommends incorporating these questions into a poll that can be distributed to companies and organizations in order to get a functional sample size of data.

Global Competitiveness

Indicators: Trade statistics, network traffic data, when and where encryption is stripped, number of companies with customers in a transnational jurisdiction, how has jurisdiction changed due to mandates, domestic device market share, and market share as a percentage of device exports.

Risk

Indicators: Cost to companies resulting in breach and cost to companies of compliance and maintenance of mandated access. Financial impacts of international market segmentation based on legal requirements, and costs resulting from conflict of laws.

Consumer Trust

Indicators: Use of a lean data framework.

Physical Harm

Indicators: Number of cases where lives were lost because encrypted data were not able to be accessed. Number of cases where lives were lost because data were accessed by a third party.

This event is brought to you by accessnow

For more information, visit https://www.accessnow.org/crypto-summit-2-0/
or contact Nathan White (nathan@accessnow.org) & Amie Stepanovich (amie@accessnow.org)