



Government-Mandated Front Doors?

A Global Assessment of Legalized Government Access to Data

Andrea Little Limbago, PhD
@limbagoa

#BHUSA @BlackHatEvents

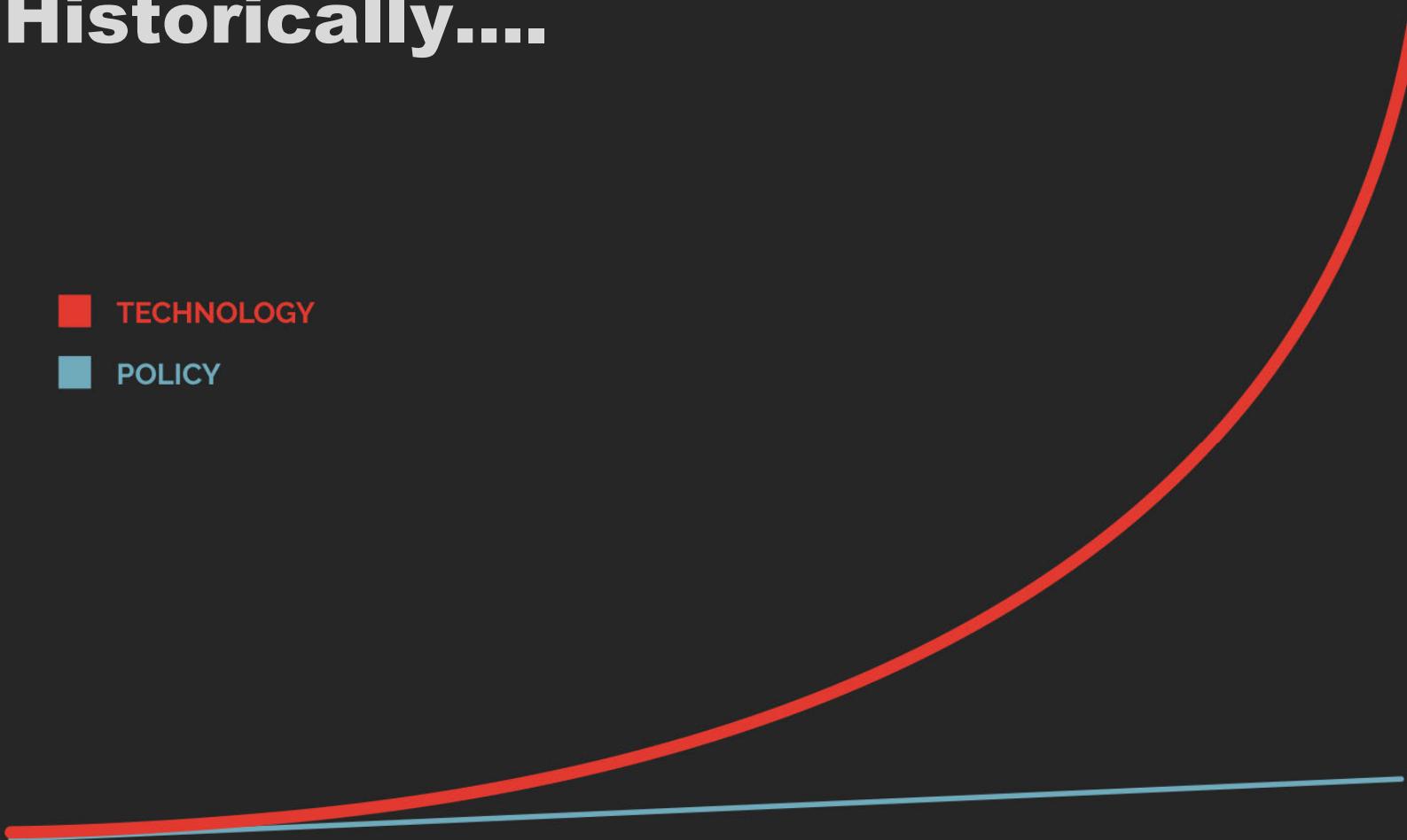


More than half the world's population live under governments who have mandated, or are considering mandating, government access to data

Historically....

PACE OF CHANGE

- TECHNOLOGY
- POLICY

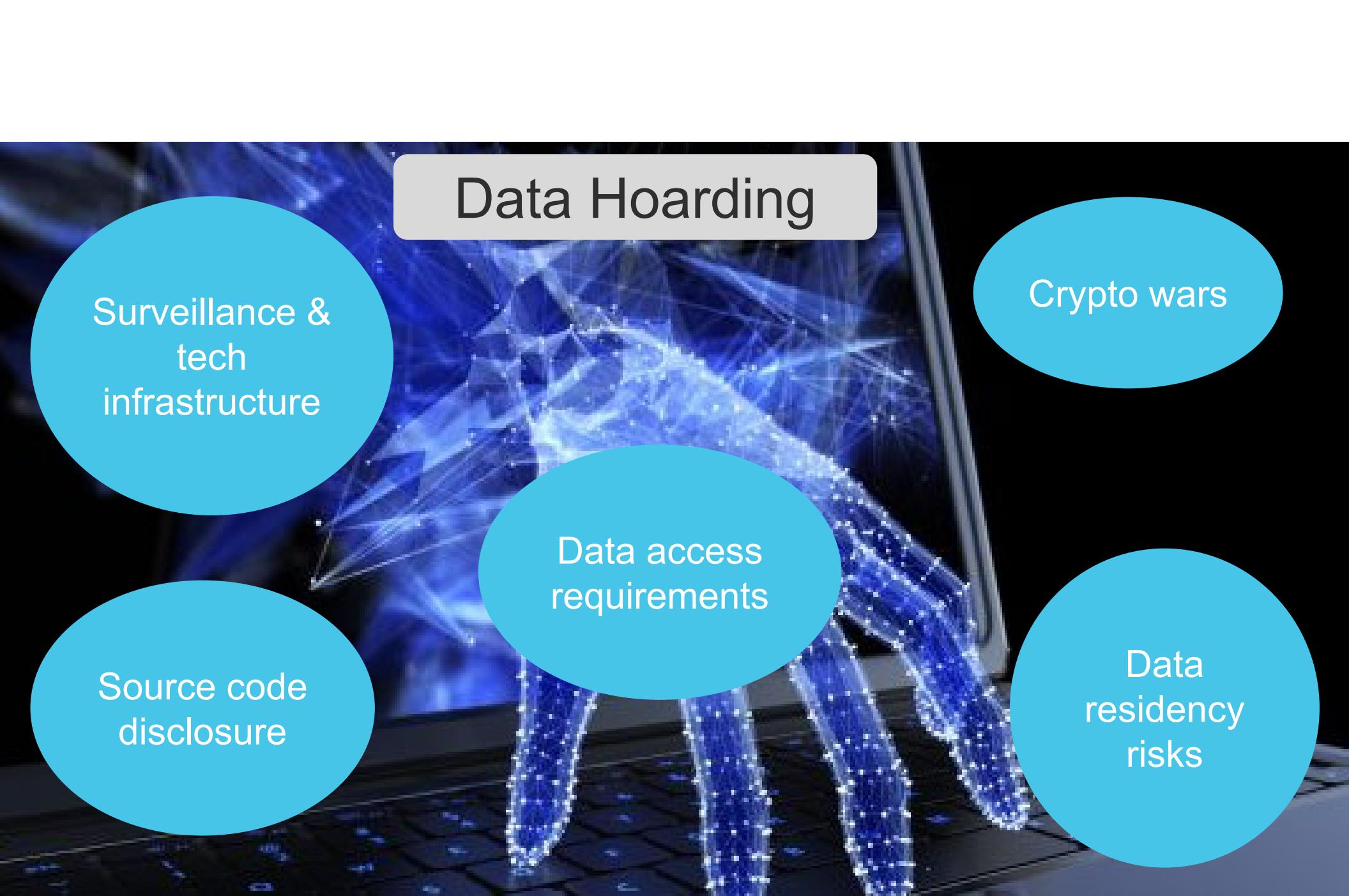


The New Normal

PACE OF CHANGE

- TECHNOLOGY
- POLICY





Data Hoarding

Surveillance &
tech
infrastructure

Source code
disclosure

Data access
requirements

Crypto wars

Data
residency
risks

Data Protection

Lei Geral de
Proteção de
Dados (LGDP)

California
Consumer
Privacy Act
(CCPA)

General Data
Protection
Regulation
(GDPR)

Almost half of Africa's
54 countries have
adopted some form of
data protection laws

The geography of data protection and access risk

- Borders do exist on the Internet....
 - The impact of the Splinternet on supply chain risk: Data protection and cyber risk vary by location
 - Which movement is gaining traction and where?
- Let's quantify it!





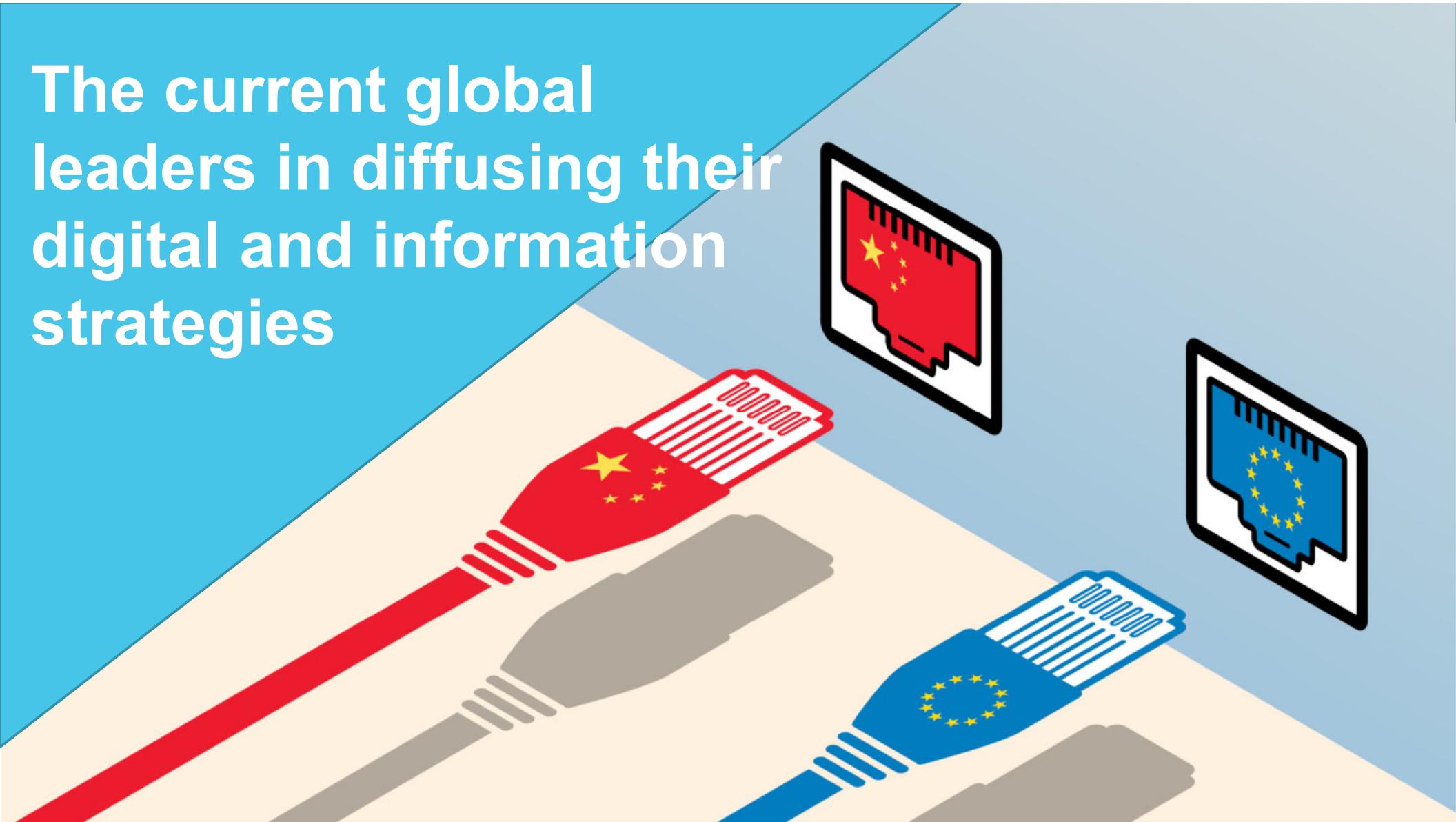
Informing the Research Design: A Shifting Regulatory Landscape



Increasingly an overlap and more so a spectrum of policies, tactics, and norms



The current global leaders in diffusing their digital and information strategies



The Rule Setters



China

- Cybersecurity Law
 - Since 2015, series of laws focused on cyber sovereignty, internet controls, state access to data or technical support to authorities, security standards
- Latest Five-Year Plan emphasizes tech self-reliance, data localization and government influence over data
- Data Security Law (Sept '21) seeks to limit extent of private data collection, while classifying private-sector data by importance to state interests



European Union

- General Data Protection Regulation
 - Focused on transparency, security, minimalization, purpose limitation, accountability, strict standards for data transfer outside of EU
- Recent discussions of banning facial recognition in public spaces

Global Diffusion



Turkey

- Unrestricted access to communications data without a warrant under emergency surveillance decrees
- Forced appointment of local representatives, which must be an incorporated company under Turkish law or Turkish citizen
- Forced localization: companies have less ability to control data access, local reps may facilitate additional access requests, encryption apps blocked



Ecuador

- Service providers may be compelled to hand over data or technical information required to decrypt encrypted data
- Interception of communications also permitted with a warrant
- Following '19 breach of 20M citizens, movement toward data protection, approved law in May '21

Global Diffusion



Thailand

- '19 law allows government official to seize, search, infiltrate computers without a warrant if deemed high-security threat
- Officials empowered to decrypt or order data decryption



Kazakhstan

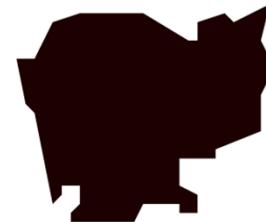
- Service providers must assist authorities with data access
- Several attempts since 2015 to require every internet user in the country to install a digital cert, but faces pushback

Global Diffusion



Mauritius

- Historically supported freedoms, but has been growing emphasis on censoring social media
- Considering a law to intercept and decrypt internet traffic, routing all traffic through government servers
 - No judicial oversight



Cambodia

- '21 decree requires all external traffic to pass through a government-controlled hub
 - Oversight by the regulatory body who also monitors online activity
- QR code contact tracing app -> data requested by China in exchange for telecom upgrade from Huawei

Global Diffusion

Indonesia

- Pending legislation focused on censorship also requires companies to provide access to systems and data, potentially bypassing data privacy protections

Australia

- '19 anti-encryption law requires companies to hand over data to the government and/or create tools to bypass encryption
- '20 proposed Surveillance Legislation Amendment Bill

United Kingdom

- Snooper's Charter– bulk interception of online communications, found in violation of right to privacy by European court of human rights
 - End-to-end safeguards required
- 2016 Investigatory Powers Act replaced the previous regime

Building a model

Assessing Data Access Risk

Data residency

Joint ventures

Federal data
privacy
protections

Encryption &
surveillance

Source code
requirements

Transparency and
judicial oversight
(DPAs)



Data in a Haystack Problem:

While some information is available from security and privacy sources, needed to expand to sources focused on ‘ease of doing business’



Data Triangulation

U.S. DEPARTMENT of STATE

POLICY ISSUES ▾ COUNTRIES & AREAS ▾

Home > Reports > Bureau of Economic and Business Affairs > 2020 Investment Climate Statements > Mauritius

★★★

2020 Investment Climate Statements: Mauritius

FREEDOM IN THE WORLD 2020

Mauritius

FREE

D4 0-4 pts

Are individuals free to express their personal views on political or other sensitive topics without fear of surveillance or retribution?

4 / 4



Proposed New Internet Law in Mauritius Raises Serious Human Rights Concerns

BY JILLIAN C. YORK AND DAVID GREENE | APRIL 30, 2021

About Issues Our Work Take Action Tools

Mauritius

Home / Mauritius

Download the Factsheet

+ Fast Facts

- Law

Mauritius was among the first movers in the data privacy space in Africa, and as such, its regulations are robust, and in line with international standards. When the country enacted the [Data Protection Act 2004](#) (DPA 2004), it became the first African country to establish the [Office of the Data Protection Commissioner](#) and make it operational.

As of January 2018, Mauritius regulates data protection under the [Data Protection Act 2017](#) (DPA 2017), which repealed and replaced the former act, so as to align with the European Union [General Data Protection Regulation 2016/679 \(GDPR\)](#). The updates to the law include the implementation of data protection impact assessments, notification of personal data breaches, stricter security requirements attached to data processing, and clearer standards around the details of lawful processing.

Among other things, data subjects have the right to:

- have their personal data corrected;
- access their personal data;
- object in writing to the processing of their personal data, at any time;
- prevent processing of personal data for purposes of direct marketing;
- object to a decision based solely on automatic processing that would significantly affect them or adverse legal repercussions.

+ Personal Data

+ Collection and Processing

+ Registration and Enforcement

+ Cross-border Transfer

+ Security and Breach Protocol

+ Complaint Portal

✓ Data protection law enforced

>Last updated: 31 March 2020

Data Protection Africa
<https://dataprotection.africa/>
#BHUSA @BlackHatEvents

Unstructured to Structured Text

- Each question aligned and coded such that low scores reflected less data protection/more invasive government intervention while higher scores reflected more data protection/less invasive government intervention
- Core areas:
 - Data storage
 - Restrictions on government access to data
 - Data protection law and independent oversight
 - Source code disclosure requirements
 - Joint venture requirements
- Global Coverage: 189 countries or territories

Results/Findings

Opposite Ends of the Spectrum

Government Intervention

- 1) North Korea
- 2) China, Russian Federation
- 3) Vietnam, Eritrea
- 4) Iran, Cuba, Equatorial Guinea, Pakistan, Syria, UAE
- 5) Azerbaijan, Bangladesh, DRC, Egypt, Myanmar, Rwanda, Saudi Arabia, Uzbekistan, Venezuela

Data Protection

- 1) Iceland, Antigua & Barbuda, Bahamas, Costa Rica, Denmark, Estonia, Taiwan
- 2) Austria, Bahrain, Belgium, Bulgaria, Croatia, Czech Republic, Japan, Latvia, Liechtenstein, Lithuania, Macedonia, Netherlands, New Zealand, Norway, Panama, Portugal, Romania, Slovenia, Sweden, Uruguay

Trends: The Good

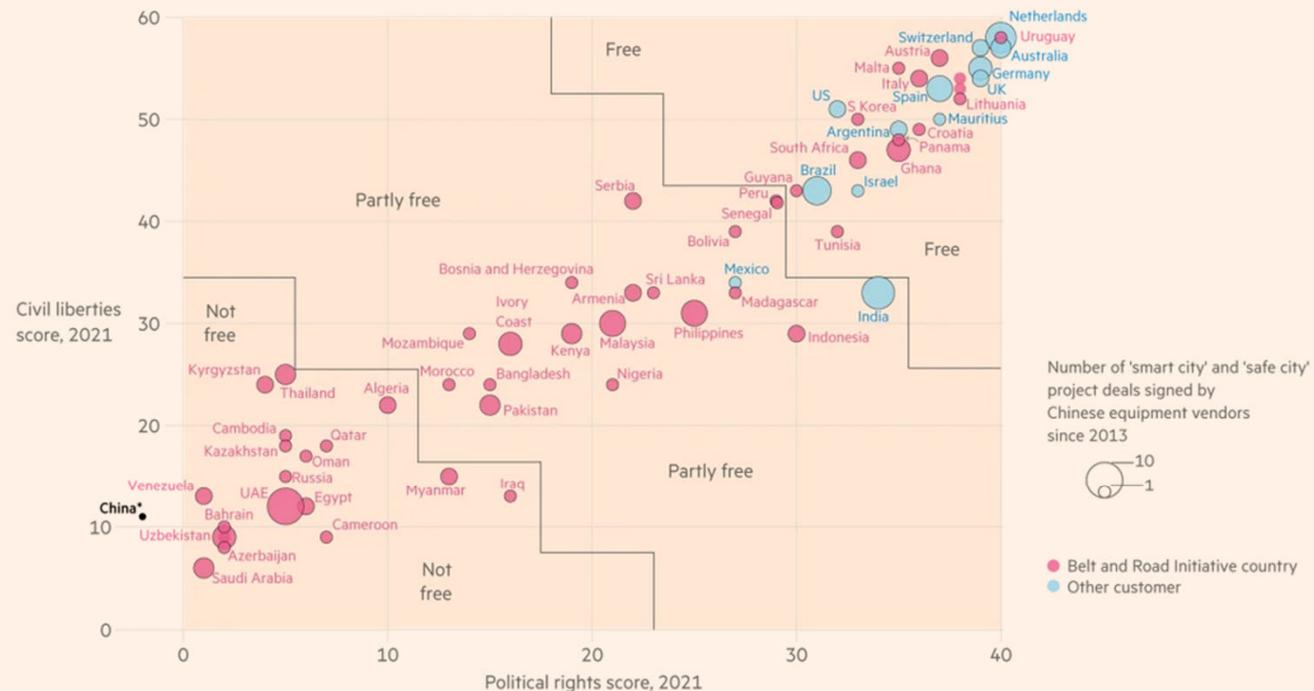
- Almost 100 countries with data protection laws
 - Many more have passed but are not yet enacted
- Accountability on the rise
 - Data protection laws in one country/region are changing behavior elsewhere
 - Fines and regulatory action may be at tipping point to prioritize data protection
- Growing global societal interest and movement for data protection

Trends: The Bad

- If you can't block them....
 - Censorship as a precursor to data access requirements
- Gaps between law and reality
 - Identifying scandals that demonstrate lack of adherence to data protection laws
- The rise of the rest
 - Copycat laws and policies across all regions
- Greater interference around elections

Trends: The Hybrid

Authoritarian regimes are keen on China's surveillance technology — but they are not the only customers



*It is possible for a country's political rights score to be less than zero
Graphic: Alan Smith Sources: RWR Advisory, Freedom House
© FT

<https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab>

Next Steps

Change is coming fast

**Zambian CSOs challenge constitutionality
of newly passed cybercrime law**

**US government pushed tech firms to hand
over source code**

**Germany's New Surveillance Laws Raise Privacy
Concerns**

Police Handed Enhanced Powers to Infiltrate Phones and Computers

Ecuador Approves Data Protection Law

**Expanding state surveillance: Organised crime and
the PM's push for more police powers**

Colorado Passes Data Privacy Law

**Indian government launches
trusted telecom portal**

**Facebook received 40,300 requests for user
data from Indian government, restricted
access to 878 items in India**

**Russian lawmakers vote to force
U.S. tech giants to open local
offices**

**Lisbon gave protesters' data to
foreign embassies**

**Hungarian government
susends some aspects of
GDPR**

**New Data Security Law in China Makes
Government Power Over Tech Giants
Absolute**

Future Considerations

Data Updates!

- Stay apace changes and begin versioning and time stamps to track temporal shifts

Community Input

- Validating and based on input
- Integrate regional/country-specific experts

Other Considerations

- Government/private sector autonomy
- Other tech dependencies? (smart cities, underseas cables, other tech risks?)

White Paper

- Overview of the research design, methodology, and rankings



Tracking Which Way the Balance Tips



#BHUSA @BlackHatEvents



Thanks!

Andrea Little Limbago, PhD
@limbagoa

#BHUSA @BlackHatEvents