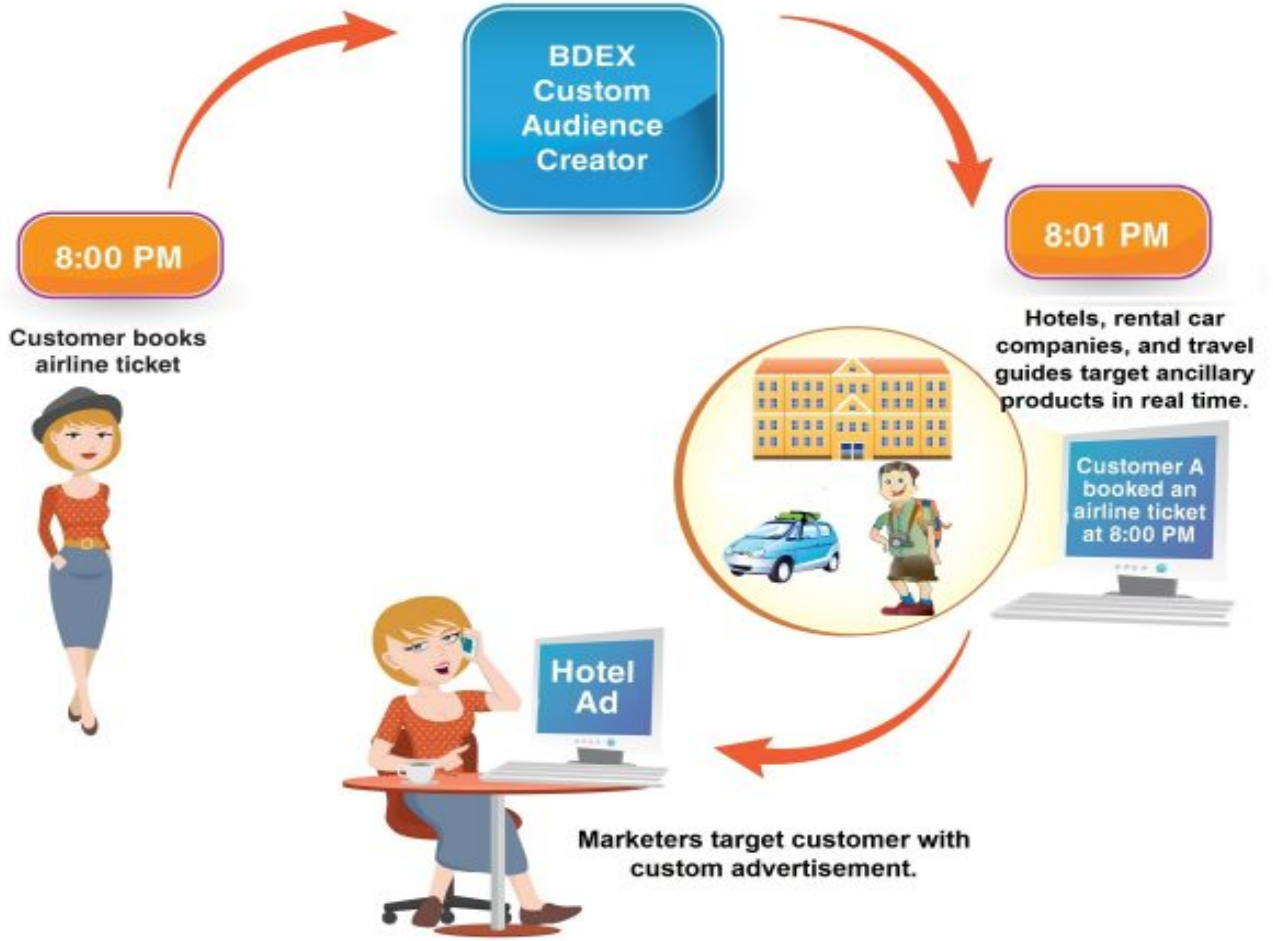
Consumer Privacy, Trust and Digital Trade

Burcu Kilic
December 2020

PUBLICCITIZEN

Data Hoarding

Personal data is routinely sent, every time a page loads, to hundreds/thousands of companies, and consumers have no control over what happens to it.



PUBLICCITIZEN

Digital Protectionism

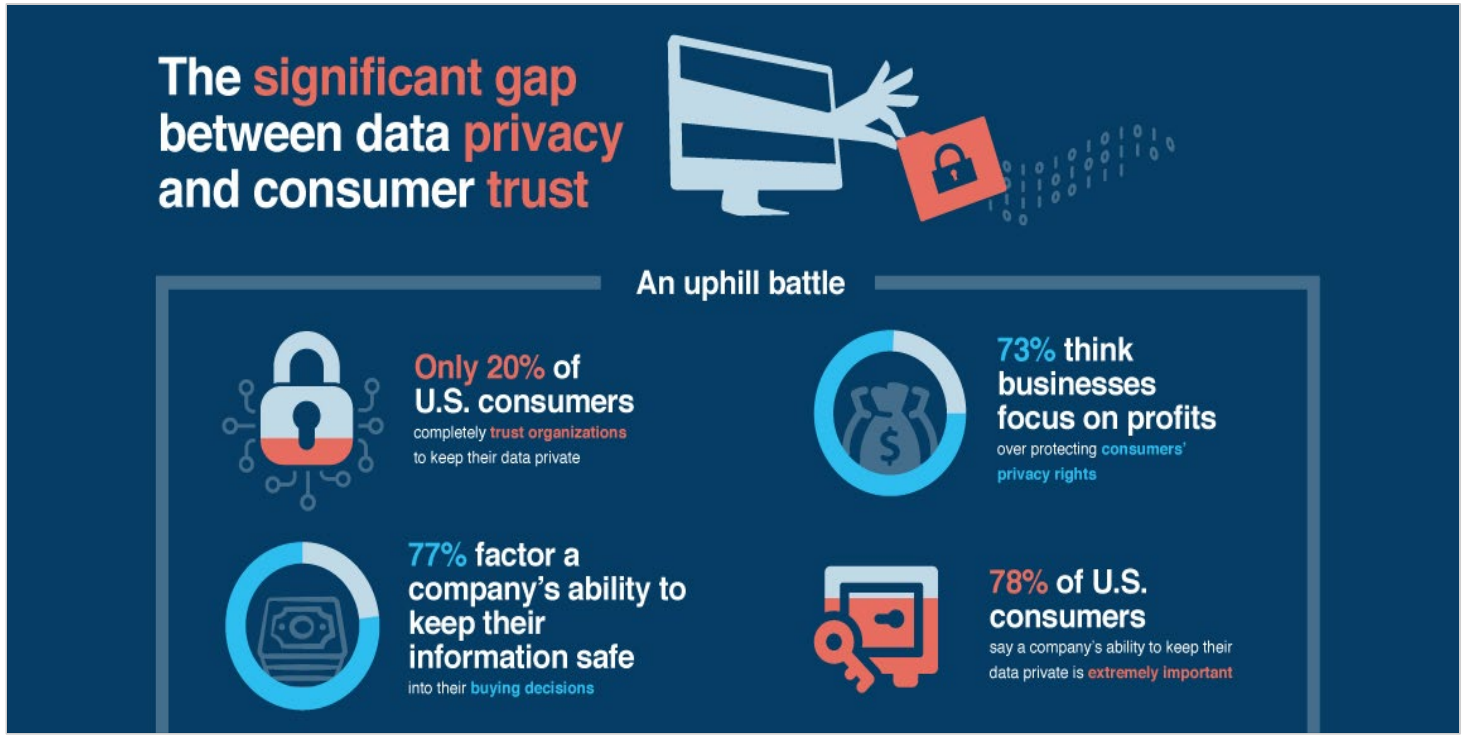
- Easy to assert
- Hard to define
- Deeply polarized

MARKETS IN FOCUS		
AFRICA	Kenya	Kenya's Data Protection Act requires data controllers to provide "proof" that personal data will be secure as a condition for transferring data outside Kenya but does not describe what would constitute proof. The Act requires consent of data subject as a condition for cross-border transfer of any "sensitive personal data," a broad category of information.
	Nigeria	NITDA guidelines require all insurers to store data of Nigerian citizens in Nigeria.
AMERICAS	Brazil	Brazil's Marco Civil, an Internet law that determines user rights and company responsibilities, states that data collected or processed in Brazil must respect Brazilian law, even if data is subsequently stored outside country. Brazil is considering draft legislation that could regulate cross-border data flows and storage requirements.
EAST ASIA/PACIFIC	China	China's Cybersecurity Law and related draft and final implementing measures include mandates to purchase domestic ICT products and services, restrictions on cross-border data flows and requirements to store and process data locally.
	South Korea	Through KORUS, Korea undertook commitments to allow financial institutions to transfer data to foreign affiliates and allow certain data processing and other functions to be performed outside Korea. Implementation of this commitment has been slow. As of 2018, difficulties remain due to Korea's consent requirement. Korea imposes constraints on ability of banks and insurance cos to utilize cloud computing services.
EUROPE/CENTRAL ASIA	EU	General Data Protection Regime (GDPR) restricts the movement of the data of EU citizens, not matter where the data is processed.
	Russia	Federal Law No. 242-FZ requires local storage and processing of data.
	Switzerland	The Swiss-US Privacy Shield Framework provides a mechanism to comply with Swiss requirements when transferring personal data from Switzerland to US. Switzerland issued a partial adequacy decision for US, limited to companies in Privacy Shield Framework.
	Turkey	Data localization is required. Turkey also imposes restrictions on transfers of personal data out of Turkey. Information systems used by financial firms for keeping documents and records must be located within Turkey.
SOUTH ASIA	India	On July 27, 2018, India announced a proposed Data Privacy Bill. The draft is based on EU's General Data Protection Regulation (GDPR). However, it seems to extend beyond reach of GDPR as it looks to require data localization, limits processing, and allows government-wide access to data. It would apply to any company that handles data of Indian citizens in almost any manner.
	Indonesia	OJK's Regulation 69/POJK.05/2016 mandates insurers/reinsurers to establish data centers and disaster recovery centers in Indonesia. Indonesia is considering national legislation and additional regulations on personal data protection, which could expand requirements for data localization.
	Malaysia	Bank Negara Malaysia has amended its recent Outsourcing Guidelines to remove original data localization requirement and shared that it will similarly remove data localization elements in its upcoming Risk Management in Technology framework.[20]
	Thailand	Thai government in February 2019 passed new laws and regulations on cybersecurity and personal data protection that raise concerns over Thai authorities' broad power to demand confidential and sensitive information without sufficient legal protections or a company's ability to appeal or limit such access.[20]

PUBLICCITIZEN

Consumer Trust

- Data privacy is key to consumer trust
- To boost consumer trust, privacy must be a top priority

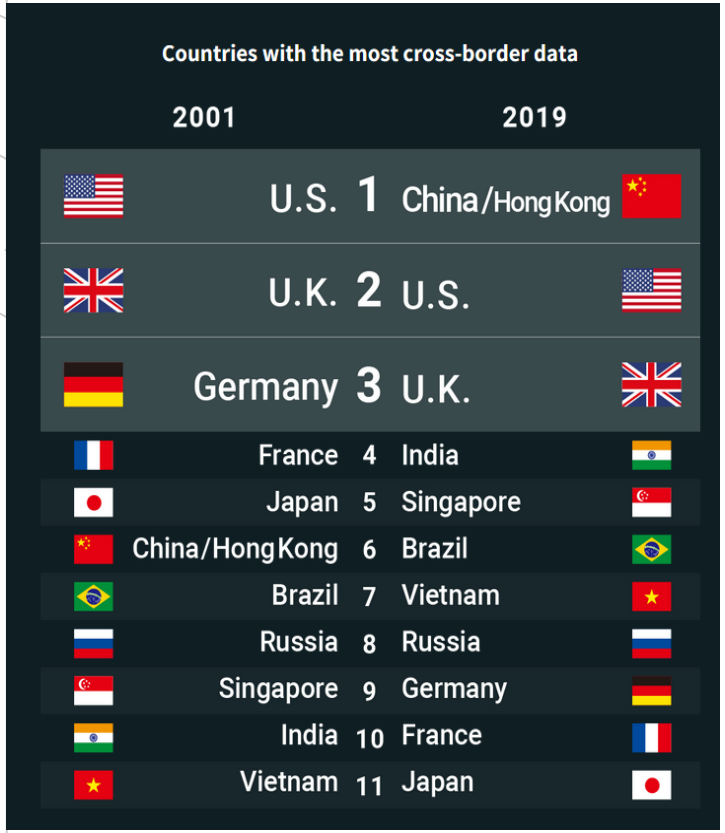


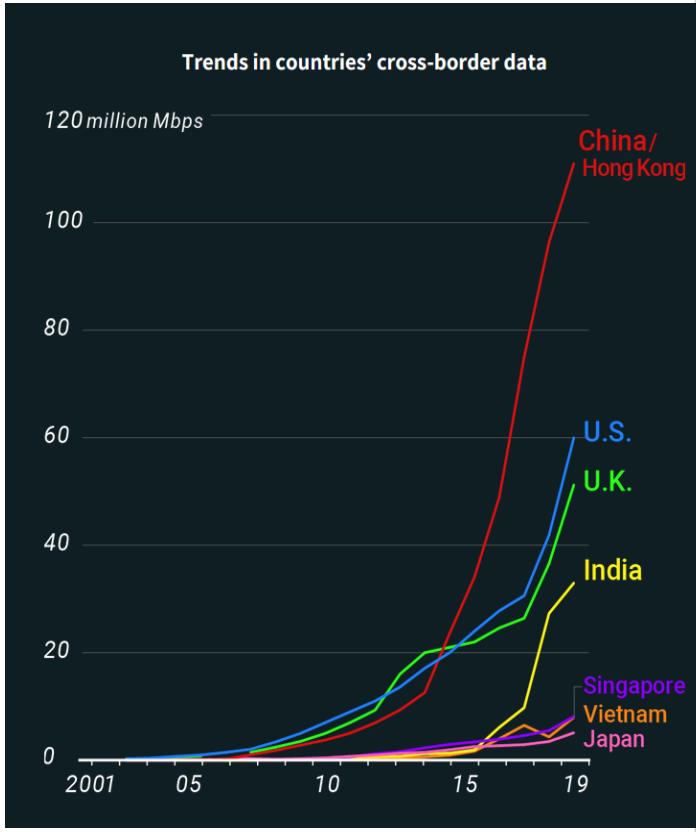
PUBLICCITIZEN

Cross –Border Data Flows

"Whoever controls the data will control the future"

- The Chinese mainland and Hong Kong together account for 23% of all of the world's data flows (about 485.66 million Mbps).
- That is about twice the size of the data in the U.S.



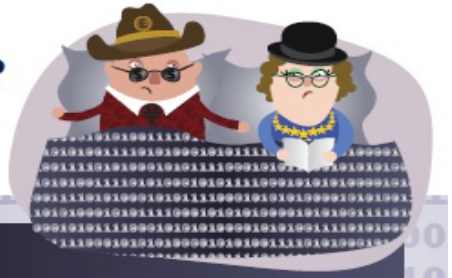


PUBLICCITIZEN

Trade & Privacy: Complicated Bedfellows?

TRADE AND PRIVACY: COMPLICATED BEDFELLOWS?

How to achieve data protection-proof free trade agreements



WHY DOES IT MATTER FOR CITIZENS?

Modern digital markets are fuelled by personal data. In e-commerce, for example, a consumer's personal data needs to be processed to conclude an online sale. Citizens shouldn't need to care about territorial borders, although regulations on how to protect these data differ widely around the world. Modern trade agreements increasingly try to tackle these differences, in order to make trade easier. For European Union (EU) citizens, it is crucial that trade deals do not undermine fundamental rights to privacy and personal data protection, and ultimately, trust in the online economy.

WHAT IS THIS STUDY ABOUT?

Modern trade agreements increasingly include provisions which allow unrestricted transfers of data between countries, including personal data. The EU's trade negotiators claim that present and future trade deals will not undermine data protection and privacy rights. As organisations defending consumer interests and fundamental rights and freedoms in the digital environment, we want to be sure that personal data and privacy are not weakened by EU trade agreements. This study analyses how the WTO agreement on trade in services (GATS), the EU-Canada agreement (CETA), the future EU-US agreement (TTIP) and the planned Trade in Services Agreement (TiSA) deal with personal data and privacy.

MAIN CONCLUSIONS OF THE STUDY

- The current measures used by the EU to safeguard its data protection laws in trade agreements are not sufficient.
- It cannot be excluded that a trade partner will bring legal actions against the EU because of its rules on data protection. For example, the way the EU grants trade partners 'adequacy' status for personal data transfers could be accused of being obscure and inconsistent, and this would make them vulnerable to a legal challenge.

WHAT THE EU SHOULD DO TO BETTER PROTECT ITS CITIZENS' PERSONAL DATA AND PRIVACY IN TRADE AGREEMENTS

- Keep rules on privacy and data protection out of trade agreements, by means of a legally-binding exclusion clause. This is also recommended by the European Parliament[i].
- Include an exception that allows any signatories to regulate cross-border data transfers. This should apply to any sector that deals with the processing and transfer of personal data, such as financial services, within a trade agreement.
- Insert a clause into trade agreements that prevents an EU measure from becoming automatically invalid or inapplicable.
- Prevent clauses in trade agreements which would oblige the EU to submit forthcoming rules on privacy and data protection to trade 'tests' in order to see if they are more burdensome than necessary.
- Treat all trade partners the same way when granting 'adequacy status' for data transfer purposes to prevent the EU from being vulnerable to potential challenge under trade rules.
- Require the European Data Protection Supervisor (EDPS) to issue an opinion on the texts of free trade agreements.

PUBLICCITIZEN

Financial Services: The Challenge of Cross-Border Data Flows

- **E-commerce chapter**: Art 14.1: definition of '**covered person**' 'does not include a "**financial institution**" or a "**cross-border financial service supplier of a Party**" as defined in Article 11.1 (Definitions);'
- Art 14.11.2: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of **a covered person.**"
- Art 14.13.2: "No Party shall require **a covered person** to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.'
- **Financial Services Chapter:** Chapter 11 (financial services): Art 11.18: Annex 11-B sets out specific commitments: Section B: "Each Party shall allow a financial institution of another Party to **transfer** information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business."

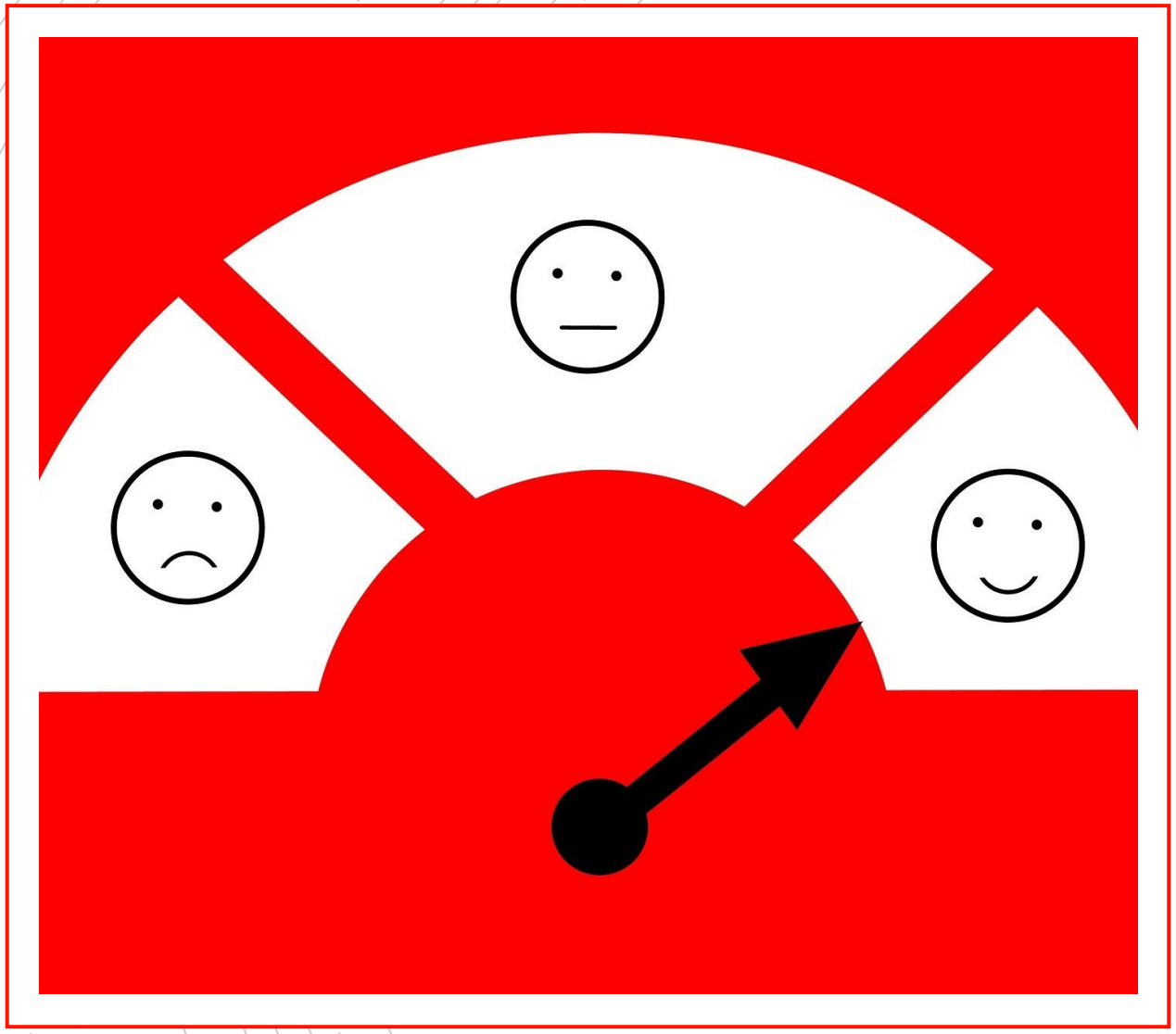
> "In the case of financial services and prudential regulation, there is a very difficult issue, and it is one that I think there is a reason to be cautious on. That is, that prudential regulators need **access to information in a timely way**, and our experience has been that there have been moments, particularly in moments of crisis, when prudential regulators could not get the information they needed from international sources."
>
> *Jack Lew, Secretary of the Treasury, 2016*

PUBLICCITIZEN

Financial Services: The Challenge of Cross-Border Data Flows

- **Digital Trade Chapter**: Art. 19.1: definition of '**covered person**' does not include a covered person as defined in Article 17.1 (Financial Services Chapter, Definitions);
- Art. 19.11: "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of **a covered person**."
- Art. 19.12: "No Party shall require **a covered person** to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."
- **Financial Services Chapter:** Art. 17.17: "No Party shall prevent a covered person from transferring information, including personal information, into and out of the Party's territory by electronic or other means when this activity is for the conduct of business within the scope of the license, authorization, or registration of that covered person. Nothing in this Article restricts the right of a Party to adopt or maintain measures to protect personal data, personal privacy and the confidentiality of individual records and accounts, **provided that such measures are not used to circumvent this Article.**"
- Art. 17.18: "No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, **so long as** the Party's financial regulatory authorities, for regulatory and supervisory purposes, **have immediate, direct, complete and ongoing access** to information processed or stored on computing facilities th at the covered person uses or locates outside the Party's territory."

PUBLICCITIZEN



DATA COLLECTION, PROCESSING & ANALYSIS

STATUS QUO (NO REGULATIONS, RIGHTS/PROTECTIONS)

INSURERS MAY BE AT THE CENTRE OF THE NEXT BIG CRISIS

A GROWING CONSUMER AWARENESS

CREATIVE THINKING — ECONOMICALLY, LEGALLY AND POLITICALLY

PUBLICCITIZEN

Burcu Kilic
Digital Rights Program
bkilic@citizen.org
@burcuno

PUBLICCITIZEN