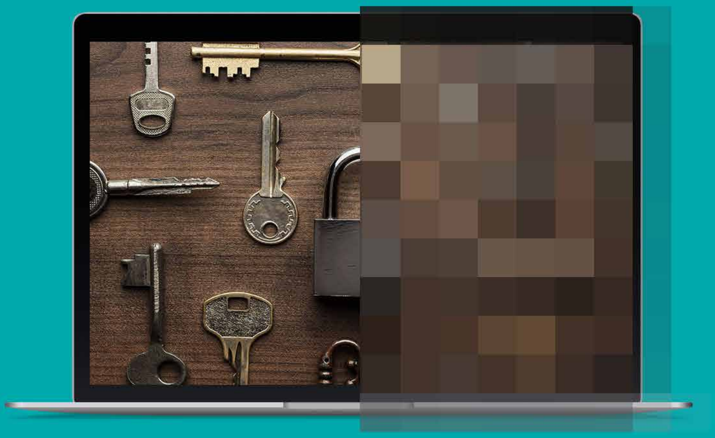
ORF SPECIAL REPORT 20

AUGUST 2016



NEW NORMS *for a* DIGITAL SOCIETY

SAMIR SARAN

New Norms for a Digital Society

SAMIR SARAN

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by by providing informed and productive inputs, in-depth research and stimulating discussions.

While the state continues to exercise its regulatory capacity over digital spaces — a task it will likely keep in the coming years — the internet has magnified the rights and responsibilities of the private sector and end users across the world.

The interaction between states, non-state actors and transnational corporations necessitates the creation of a regime complex that clearly outlines their respective roles. This paper is a first step in that direction, articulating norms that may serve as the baseline for legal and political agreements on cyberspace. Inter-governmental gatherings like the UN Group of Governmental Experts have largely focused their efforts on the security of networks and ICTs. Multistakeholder organisations and platforms like the Internet Governance Forum, the Internet Corporation for Assigned Names and Numbers, and the Internet Engineering Task Force, have begun to re-orient their mandate, with a view to make their governance more inclusive and accountable.

The set of seven norms and their corollaries identified in this paper may inform the functioning of both intergovernmental and multistakeholder processes. This document also attempts to chart the role of the private sector in digital governance. The end user today is valuable to internet companies, since the data collected from consumers directly contributes to the creation of revenues. If user data is the basis of wealth generation, internet giants have a responsibility to invest in the user by offering local content and innovative technologies that are contextual. This is particularly true in the case of emerging economies and developing countries, where internet businesses should tailor to the unique needs of the next billion users.

This paper argues that effective internet governance requires shifting the locus of digital debates from the Atlantic to the Asia-Pacific and bringing in new voices and views of a new constituency of stakeholders. Similarly, all stakeholders must work towards building the capacity of growing digital economies and first-generation internet users. Efforts to fragment digital spaces by creating alternative "internets" must be avoided. Just as regimes that curtail the freedoms of internet users are undesirable, actions that raise the cost of local innovation and increase barriers to the unrestricted flow of technology, and thereby quality of access, should also be discouraged. These norms are a work in progress, and the author reserves the right to refine them through continued consultations with stakeholders across the spectrum.

1

Online = offline + more

The protection of rights over the internet requires mechanisms that are unique, contextual and transformative. Rights on the internet should not be limited to those offline, and must build on the edifice of free speech and expression that already exists. Similarly, current regulatory frameworks must evolve in response to the digital medium. Just as traditional broadcasting regulations have become inadequate to regulate online speech, outmoded censorship laws often constrain free expression and impose a chilling effect. Contemporary conversations on privacy must reflect the need to protect sensitive data, while acknowledging its importance for technological innovations that benefit local communities.

NORM ***Realising the transformative potential of the internet requires progressive online freedoms that move beyond rights granted offline.***

COROLLARY ***Real-world regulations must not constrain the advancement of technology; rather, they must evolve in response.***

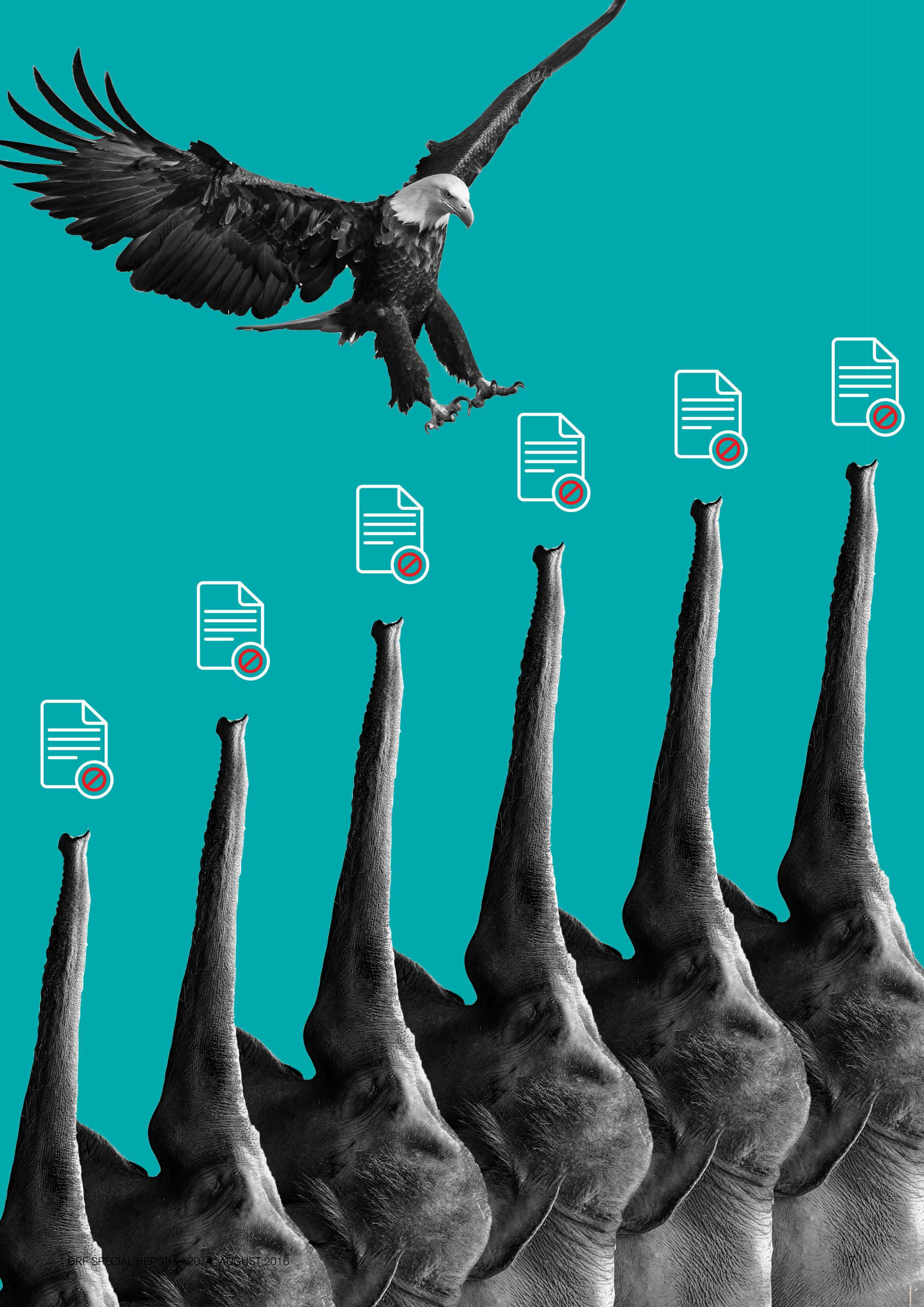
2

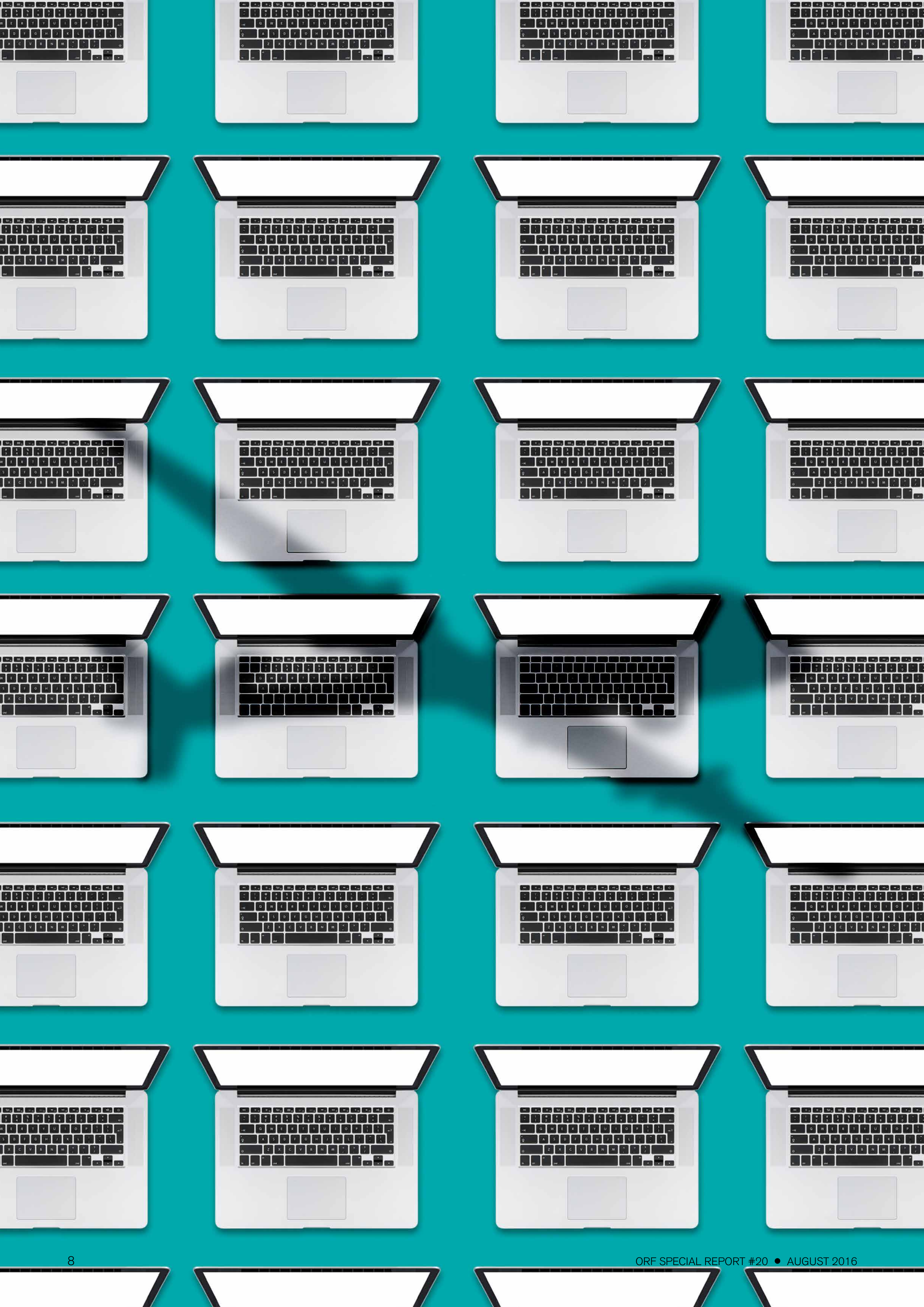
Let data flow

Affordable, universal and high-quality access to the internet is among the top policy prerogatives of governments today. Access will require substantial investments in the form of local data centres, internet exchanges and last-mile connectivity. As net exporters of data, developing countries represent a robust market for internet companies. Indeed, data flows seem to be thriving globally, even as financial and trade flows dwindle (McKinsey: 2016)[1]. For their digital economies to expand, the free flow of trans-boundary data must be coupled with the unrestricted flow of technology. Emerging markets should not be left behind the curve, and the end user must have affordable access to the latest technologies, rather than having to wait years for products and services that have been rendered obsolete in advanced economies. Custodians of data should orient their research and development towards local solutions, and foster domestic entrepreneurship. Data flows, however, should respect the sovereign imperative of law enforcement and security.

NORM ***The global free flow of information must necessarily lead to universal access to the internet in emerging economies that is affordable and qualitatively rich.***

COROLLARY ***Free flow of data must be complemented by free flow of technology that is tailored for local innovative solutions.***





3

Living in an encrypted world

Governments around the world are locked in debate with industry bodies and civil society for the right to access encrypted communications. Backdoors and forced localisation of data, however, can decrease the overall standard of security in the market, curtail free speech, and violate the integrity of data. Governments should welcome technological developments that incorporate security by design, with a view to preserve the integrity and stability of digital networks.

NORM *Encryption must be the norm.*

COROLLARY *Decryption of data must be subject to rigorous standards of judicial review.*

4

The responsibility to inspect?

States are faced with increasingly dangerous and sophisticated threats from state and non-state actors in cyberspace. The technological and legal capacity for dealing with these threats is often disparate, caused in part by lack of access to proper forensic, investigative and prosecutorial tools. It is the sovereign function of a state to protect its own citizens and infrastructure from such threats, without undue interference or intervention in its affairs. The interconnected nature of the internet demands that governments and businesses across geographies cooperate towards norms of cooperation that mitigate the risk of conflict.

NORM *The responsibility of states to protect cyberspace is a sovereign function, commensurate to their capacity.*

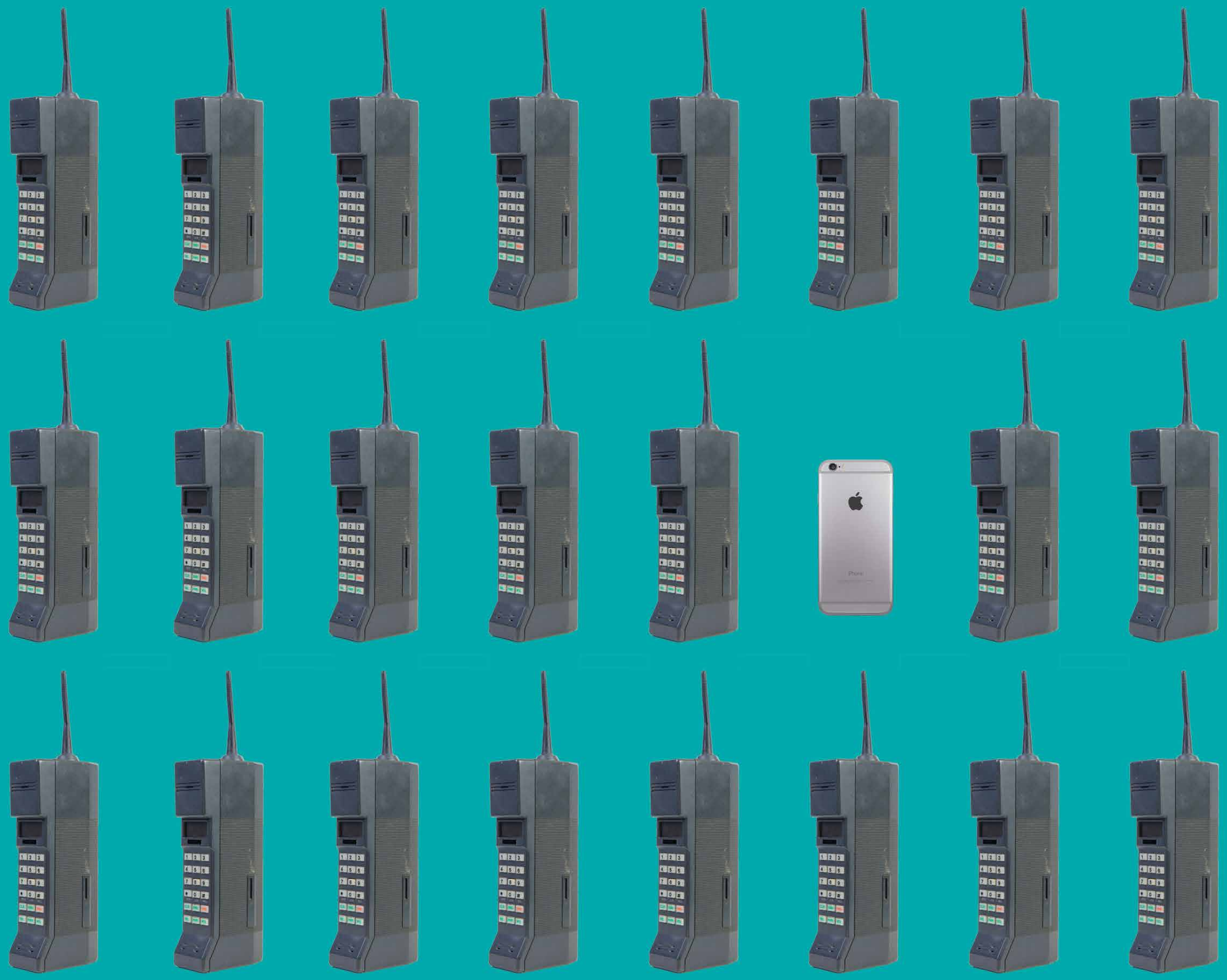
COROLLARY *The collective responsibility for protecting cyberspace requires global investments for building capacity in developing countries.*

5 Strengthening the base

The ubiquity of low-end smartphones, the growth of affordable data networks in emerging economies, and the relative lack of awareness of cyber vulnerabilities among users leave networks and individuals vulnerable to exploitative practices. Enhancing cyber hygiene among internet users in emerging economies can help substantially decrease the vulnerability of the global digital space as a whole.

NORM *Cyber security must account for, and address technology limitations of the end user at the bottom of the pyramid.*

COROLLARY *Local communities must be at the forefront of articulating policy solutions for cyber security.*



6

Three rules for internet governance

Despite attempts to decentralise and diffuse the management of global internet governance institutions, there are inadequacies in revised accountability mechanisms. The locus of internet governance must shift from big transnational corporations to start-ups, medium and small local enterprises, from governments to multistakeholder communities, and from trans-Atlantic conversations to Asia-centric debates.

NORM ***Multistakeholderism should be institutionalised by accounting for diversity in gender, geography and sectors.***

COROLLARY ***International internet governance must undertake three transitions and accommodate new stakeholders:***

a) ***States » Communities.***

b) ***Trans-national corporations » Small & Medium Enterprises and Startups.***

c) ***Atlantic » Asia and Africa***

7

Against the Splinternet

The Domain Name System (DNS) represents a stable and contiguous platform of unique identifiers, comprising numbers and names. Attempts to fragment the internet by creating an “alternative” system or through interference in the functioning of the “root” should weigh its potential impact on internet users, businesses and governments. Just as technical efforts to create a parallel DNS should be discouraged, trade regimes around the digital economy should consider the effect of fragmenting the internet into differential pricing regimes. Affordable and universal internet access can be realised by removing policy barriers to the creation and strengthening of ICT infrastructure.

NORM ***The internet should remain unfragmented.***

COROLLARY ***Differential trade regimes should not raise the cost of doing business in the digital economy nor impede low-cost connectivity to users in Asia and Africa.***

ENDNOTES

1. “Digital globalization: The new era of global flows” McKinsey Global Institute, February 2016, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

Observer Research Foundation **(ORF)** is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academics and business leaders.

Observer Research Foundation
20, Rouse Avenue Institutional Area,
New Delhi — 110002
INDIA

Phone: +91 011 43520020
Fax: +91 011 43520003
Email: contactus@orfonline.org

DESIGNED BY **SHANTANU SALGAONKAR**