The Internet and human rights: access, censorship, shutdowns, and surveillance

Ewan Sutherland†
LINK Centre, University of the Witwatersrand

Abstract
A C21st bill of rights needs to address Internet-related issues such as censorship, collection and dissemination of personal data, lawful interception, provision of access, and government-enforced shutdowns. However, the uncertain nature of Internet access means firstly that it ought not to be a right, and secondly that institutions and practices need to be designed to benefit from the Internet, to be secure from any threats and to be able to be transformed as technologies change. These complex and evolving challenges call for institutional reforms to support enforcement of existing rights of freedom of expression, privacy and safety, combined with good governance and the rule of law in a digital age. In particular, it requires independent data protection agencies that can share challenges and experiences with their counterparts and which can publicise data breaches and emerging issues. It requires openness, with disclosure of governmental and regulatory activities (e.g., impact and threat assessments), with judicial appeals against decisions and parliamentary oversight of ministers and agencies. Transparency will not be enough to stop autocratic states from shutting down parts of the Internet, when faced with opponents, governments seem able to ignore international protests. Much greater transparency is necessary on national security and its relationship to the rights for privacy and safety, and the need for intrusive surveillance. Good governance at national level can be improved and supported by international cooperation (e.g., peer review, threat assessment, and training).

Keywords: Governance, Human rights, Internet, Security, Telecommunications.

Introduction
A number of concerns have been raised about the relationship between human rights and the Internet, about the provision of access, the censorship or removal of content, the collection and processing of data, the shutting down of networks, the surveillance of citizens, and, more generally, about the digitalisation of economies and society. These complex issues are both international and national, for example, with Internet services

† http://twitter.com/#!/sutherla http://ssrn.com/author=927092 http://orcid.org/0000-0001-5220-9605
delivered on markets that are subject to treaties,¹ regulated by quasi-independent national agencies, with governments directing lawful interception and network coverage.² Where there is good governance the courts enforce constitutional rights and hear appeals on individual administrative decisions,³ while the ‘regulatory state’ is overseen by parliaments. Governments, regulators, intelligence services and police forces, to differing extents and with differing degrees of accountability and transparency, coordinate their activities at national, continental and global levels, both through international organisations and regulatory networks, conducting peer reviews, developing best practice and preparing and monitoring treaties. All of this is subject to lobbying by businesses, plus some engagement with citizens. Global markets supply the underlying technologies, devices, infrastructure, and network management services, whereas network provision is invariably national in scope, with extensive obligations set out in licences and general authorisations. The content accessed over networks is sometimes national, but is often provided by or through multinational corporations (MNCs).⁴ The questions addressed in this paper concern how the continuing technological advances achieved with the Internet can be related to the formulation and implementation of human rights.

The Internet began as a simple network of local networks, linking a few research institutions in the USA, growing by adding more networks and gateways to other networks, which later switched to use Internet protocols (Hafner & Lyon, 1998; Leiner, et al., 2009). Massive expansion came with the commercialisation of access, using pre-existing telephone networks. The supposedly technical protocols contained a strong political bias against regulation, trying to confine that to the underlying telecommunication layers, even when services began to erode the telephony revenues of operators. A political imperative was stated in the ‘right to innovate’ (Lessig, 2001; Torrance & von Hippel, 2015), to create novel end-to-end services, without reference to commercial operators or governments. In parallel, firms and governments developed standards for mobile networks that added ever increasing capacity for Internet access, which, when combined with smartphones, allowed third parties to create apps. Advances were driven by strong capitalist forces, in particular the race to produce ever more powerful microprocessors, enabling greater functionality that was used by a stream of new apps and services that generated user data that could be sold to advertisers. In hearings before Senate Committees on the Judiciary and on Commerce, Science, and Transportation (2018) and the House Energy & Commerce Committee (2018), Mark Zuckerberg evaded explaining how Facebook disregards the privacy of its customers and their friends when collecting, processing and profiling their data.

Globalisation have been analysed in economics, politics and sociology, despite disagreement over its definition (Stiglitz, 2002; Holton, 2011; Christensen & Kowalczyk, 2017; Caselli & Gilardoni, 2018), while the rise of identity politics, nationalism and populism are receiving attention (Post, 2017; Saramo, 2017; Galbraith, 2017; Stockemer & Barisone, 2017). Opposition has become commonplace, even global, with condemnations of multilateral trade agreements and of regional economic groupings. By contrast, China supports its own version of globalisation, notably its Belt and Road Initiative, while remaining protectionist and authoritarian at home (Rolland, 2017; Ferdinand, 2016).

For many, the Internet epitomises hyper-globalisation, with a single global market transcending national borders. The manufacturers of equipment have non-market strategies

¹ Notably the International Telecommunication Union (ITU) Radio Regulations (RRs) and WTO General Agreement on Trade in Services (GATS) and Information Technology Agreement (ITA).
² These may take the form of both obligations to cover certain percentages of the population and state aid to cover part of the capital costs of extending networks into areas that are not commercially viable.
³ In some countries regulatory authorities will reconsider decisions, while in others initial appeals are heard by specialist tribunals.
⁴ A rare instance of cross-border content regulation is provided by the EU Audio-Visual Media Services Directive 2010/13/EU.
(NMSs) to deliver borderless global markets, subject to the least possible regulation, in order to maximise their economies of scale and profits. These include extensive lobbying at multiple levels (e.g., United Nations, continental, national and municipal), sometimes supported by national or municipal litigation, but only token efforts at corporate social responsibility (CSR) and the observance of human rights (Sutherland, 2014; 2016). Activists support a unitary global Internet, superseding national political and regulatory processes, envisaging the obsolescence of Westphalian nation states (Fraser, 2007; Eriksson & Giacomello, 2009; Liaropoulos, 2017). At the other extreme is China, which maintains a separate national Internet, behind its Great Firewall (Ensafi, Winter, Mueen, & Crandall, 2015; Ensafi, et al., 2015; Roberts, 2018). This blocks incoming content, as part of its censorship and is also a trade barrier keeping out foreign providers, while their protected Chinese counterparts are required to engage proactively in its sophisticated censorship system (Lee, 2016; King, Pan, & Roberts, 2017). Many other governments wish to have such national controls, with some seeking an extraterritorial reach to monitor dissidents and émigrés using advanced surveillance technologies (PI, 2017).

Human rights are codified and recognised at multiple levels, in international treaties, such as:

- United Nations Universal Declaration of Human Rights (UN, 1948);
- European Convention on Human Rights (CoE, 1950); and

These have been expanded in a range of specialist conventions. The rights are also recognised at the national level, for example:

- US Bill of Rights 1789;
- Constitution of South Africa Act of 1996; and
- United Kingdom Human Rights Act 1998.5

Enforcement of these treaties and laws varies enormously, often being ignored by authoritarian governments. There are intergovernmental discussions, for example at the United Nations Commission on Human Rights and the Council of Europe, reviewing implementation. International enforcement is generally limited and ineffective, with the exception of the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU). Businesses are supposed to observe human rights, but many avoid difficult countries and controversial problems (e.g., UN Global Compact (2018)). There are a number of projects that seek to measure the state of human rights, the rule of law and the fragility of states, albeit incompletely and controversially (Freedom House, 2017; WJP, 2017).

In the 1970s, the growing use of computer systems gave rise to concerns that data might be misused by corporations and governments, infringing the right of citizens to a private life, resulting in legislation in the USA and a number of European countries (González Fuster, 2014). This was codified in the OECD (1980) Guidelines and Council of Europe (1981) Convention, and the Data Protection Directive 95/46/EC, now replaced by the General Data Protection Regulation (EU) 2016/679 (GDPR). While these rules have diffused far beyond Europe, their implementation is often pro forma, there being few effective data protection authorities, only rarely the option of civil litigation and almost no effective network governance (Guadamuz, 2000; Greenleaf, 2014; Makulilo, 2016; Wolfson, 2017). One important addition to the original principles has been the ‘right to be forgotten’, to have some set of data about an individual expunged, generating extraterritorial issues, with service providers reluctant to ensure global deletion (Rosen, 2012; Neville, 2017).

While it was never planned, the Internet now allows individuals to exercise other rights, to associate, to communicate, to participate in political processes, even to pursue a family life.

---

5 There have been proposal that the UK withdraw from the ECHR in favour of domestic rights legislation.
However, it is a double-edge sword, being also used for bullying, fraud, and a range of domestic and international crimes, and for warfare, requiring the courts, the police, the intelligence services, the military and governments to protect citizens. In many respects it requires a digital transformation of government and governance, just as it does for businesses, for example, a restructuring, retraining, and rethinking of police forces and of their work (HMIC, 2015). The archetypal use of social networks is captured in the phrase: “The President is up and tweeting”, providing a means to connect with large number of past and potential voters. Social networks provide immediacy, openness and transparency that would be very difficult by other means.

The following section addresses the question of Internet access as a potential right. The following sections examine in turn security, censorship and network shutdowns. Finally, conclusions are drawn and issues identified for further research.

Internet access

Vint Cerf (2012), sometimes termed a founding father of the Internet, argued access was not a human right. The nature of access has been constantly and intentionally changing, a feature not a bug, with massive corporate and governmental investments in research and development, changing business models, making it very difficult to formulate the text. Moreover, it would entail picking technologies, deciding on the pace of network deployment, shaping market competition and defining interventions, against the background of, seemingly unending, change. Accelerating development is often part of industrial policies to create some future Internet, with nations currently aspiring to lead the deployment of the Internet of Things (IoT) and fifth generation mobile (5G).

Internet access is being extended to ‘things’, including coffee machines, fridges and electronic tattoos. A person might conceivably have a right to Internet access, but not their chattels and effects, even ‘smart’ underwear cannot have rights, though its owner might have a right to connect (Mashable, 2018). A yet more complex issue concerns the data from the smart underwear that might be transmitted to a home server, a fitness service provider or the manufacturer, data that is personal and potentially sensitive, that should be protected.

The smartness of buildings and cities brings significant challenges for privacy and data protection, for example, with CCTV cameras linked to face and gait recognition.

The problem of setting rates for services first arose for railroads in the USA in the 19th century, resolved in the USA by creating an independent regulator (MacAvoy, 1965; Stone, 1991). Subsequently, policy was made by the administration, laws were scrutinised and adopted by the legislature, decisions were taken by the regulator, subject to appeals to the judiciary, creating what came to be termed the regulatory state (Anderson, 1962). The global diffusion of this model for telecommunications occurred late in the twentieth century (Guislain, 1997), with the liberalisation of markets and the privatisation of state providers, though often flawed by the lack of accountability and oversight, and sometimes corruption.

Assuming Internet access remains with regulated markets, then an expert agency is considered the best option, subject to government policy, appeals to the courts and all scrutinised by parliaments (WTO, 1996; Laffont & Tirole, 2001). Its roles being to:

- Analyse prices;
- Examine qualities of experience and of service;
- Adjust for technological changes; and
- Oversee any subsidies and cross-subsidies.7

---

6 Parts of this were later codified in the Administrative Procedure Act 1946, Pub.L. 79–404, 60 Stat. 237.
7 Cross-subsidies arise under universal service obligations, where flat, non-geographic tariffs allow an operator to take money from cheaply supplied customers to pay for those in more expensive locations.
The principal alternative is a monopoly, long out of favour, whether direct state provision or a concession to a commercial operator. They are seen as inefficient and wasteful, responding poorly to rapid changes in equipment and services.

Since the 1990s, access to the Internet has been addressed by the European Union as part of its universal service obligation (USO) (EC, 1997; 1998). The EC (2000) dropped access to older technologies in favour of an obligation of:

\[\ldots\] data rates that are sufficient to permit functional Internet access (EC, 2002).

Subsequent reviews excluded broadband, since the majority of consumers relied on narrowband (EC, 2006; 2008). Member states could mandate universal broadband, provided they did so from general taxation, rather than a levy on the operators, though even by 2011 only Finland, Malta and Spain had done so (EC, 2011).

The legislative proposal, presently before the European Parliament and the EU Council,\(^9\) adds broadband to the USO. A minimum speed is defined by a list of basic digital services that should be enabled, which will be amended to keep pace with developments, but presently includes banking, education and government (EC, 2016).\(^10\) Whereas, expanding geographic coverage is expected to be addressed by means of coverage obligations in spectrum licences and public investment in conformity with state aid rules.\(^11\) Additionally, there should be financial support from governments, to allow operators to provide social tariffs for those with low incomes or special social needs (i.e., various disabilities).

A further regulatory approach has been suggested by the EC, the use of the essential facility doctrine in competition law, which could include platforms such as Facebook and Google (White, 2018). Dating from the case of a railway bridge over the Mississippi River (United States v. Terminal R.R. Association, 1912), that would have been costly and difficult to replicate (Werden, 1987; Areeda, 1989). While doubtless opposed by providers, it has a solid basis in economics and law, allowing the courts to settle any appeals.

The principal-agent problem describes circumstances in which a person or entity as the ‘agent’ make decisions or take actions on behalf of another person or entity as the ‘principal’ (Eisenhardt, 1989). Agents are motivated to act in their own best interests, which may be contrary to those of their principal. The problem arises with the electorate and MPs, MPs and ministers, ministers and regulators, regulators and regulated firms, and investors and managers of those firms. A major challenge for regulators and policymakers is to have a sufficient understanding of technological developments and the likelihood and strength of their adoption by consumers and business users.

These issues become more complex in the regulatory state, since there is lobbying by regulated firms, the manufacturers supplying them and their trade associations. In some countries there are measures to provide transparency, such as, the publication of lists of meetings with ministers and regulators, and of gifts and political donations. In most countries lobbying goes unreported and may be supplemented by gifts and travel, or replaced by bribes and cronyism. This raises the risk of capture by operators, or there can be capture by government, when the regulator can be reduced to a façade, with only the appearance of independence (Dal Bó, 2006).

One reason for liberalisation and privatisation of state providers of telecommunications was to shift the risks of the massive investments needed to upgrade networks from government and taxpayers to private investors. This has been substantially reversed by lobbying, with

---

8 This provided two 60 kbps channels on each telephone line.
10 It will also remove the provision of legacy services: public payphones, comprehensive telephone directories and directory enquiry services.
11 Subject to Article 117(1) TFEU.
operators and manufacturers arguing that new technologies should be part of national industrial strategies, because they contribute to economic growth and improve productivity. Later, when networks have been deployed in more populated areas, operators have argued for state aid to extend them into areas considered uneconomic. They even persuaded the EC to modify its definition of state aid to allow the funding of the ‘next generation’ of network technologies in areas where networks already existed (EC, 2013).

It is very difficult to define and implement USOs other than by national mechanisms. The EC tried for decades to create a pan-EU ‘single’ regulator and faced bitter resistance from national governments, while receiving little support for industry (Sutherland, 2010). Nonetheless, the EU has transferred considerable funds for network construction in poorly provided areas. Developing countries already have access to funding from the World Bank and its Chinese counterpart, but declining demand in the face of operators borrowing on commercial markets.

In the United Kingdom a court faced with a challenge on the right to Internet access would have to identify a remedy that it might compel one of the following to execute:

- Secretary of State for Digital, Culture, Media & Sport (DCMS);
- Office of Communications (OFCOM);
- Openreach; or
- One or more of the operators.

As in the Clientearth case it might require HMG to adopt a policy that would deliver a programme, or it might strike down an existing policy (Clientearth v Secretary of State for Environment, Food & Rural Affairs, 2017). It would not be able to write a new policy and very unlikely to force HM Treasury to spend specific sums. In picking a technology it would create a path dependency, just like Openreach, potentially constraining access policies for years into the future.

Two cases have been brought against monopoly telecommunication providers, arguing that the insufficiency of provision infringed the right of freedom of expression, resulting in the licensing of alternative providers in Dominica and Zimbabwe (Retrofit (Pvt) Ltd v. Posts & Telecommunications Corp, 1995; Butler, 1997; Cable and Wireless v. Marpin Telecoms & Broadcasting, 2000).

Internet access has increasingly become necessary to exercise other rights, such as freedom of expression and is deeply entangled with the right to privacy, perhaps even with the right to a family life, but access per se is too changeable and ephemeral to be a right itself. Today, there can only be limited understandings of the future markets for Internet of Things or 5G mobile, with even vaguer visions of 6G. It is essential to recognise the drivers and pace of change and to have governance, institutions, laws, policies and practices that are able to keep up. It is important to ensure good governance, with transparency in processes, in access, in meetings, in payments, in data and statistics, and so on.

**Security**

In the Weberian state, governments have the exclusive right to the legitimate use of force (Weber, 1919). The state thus has to protect citizens against cyberattacks, whether from domestic or foreign criminals, terrorists or foreign powers. At the extreme, this means protecting the life and the exercise of rights of its citizens, where attackers try to disable the French TV5, the Ukrainian electricity grid or the UK National Health Service. It should also assist businesses and citizens in protecting themselves, for example, by encouraging the use of more secure passwords, antimalware software and keeping offline backups of data.
Interception by the state dates back to opening of letters in ancient times, belatedly given a legal basis as part of postal monopolies in early modern times.\(^{12}\) Lawful interception was extended as new technologies came into use, first telegrams and telephone calls, then Internet communications. It was embedded in telecommunication standards and technologies, but not in Internet equipment and software, with some providers emphasising their systems were above interception. Democratic governments maintained a degree of secrecy about their capabilities for interception and decryption, to discourage criminals and terrorists from adopting more secure communications. More authoritarian regimes sometimes emphasise they are listening and watching.

There is little, if any, dispute over the need for lawful interception in the investigation of crimes. Whereas, there is considerable disagreement over the level and nature of the necessary approval, whether by a senior police officer, a government official or a judge, and the level of justification required for that approval.\(^{13}\) Similarly, there is disagreement about the nature of oversight by independent tribunals, the transparency of mandatory reporting and the effectiveness of parliamentary oversight. In addition to the right to privacy there are issues of good governance.

While the right to privacy is well established, in the Universal Declaration of Human Rights and the African, European and Inter-American conventions, procedures and observance vary enormously between countries, reflecting administrative, cultural, legal and political differences. Governance has been slow to keep pace with technological advances in interception, and in having to develop or to adapt rules for drones, IMSI-catchers, and intrusive malware.

From the 1960s, the rise of administrative and commercial data processing, especially for censuses, caused concerns about the collection of data, the combination of databases and transborder data flows. This prompted work in a number of countries, including the US, and in international organisations, leading to the adoption of:

- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980; Gassmann, 2010); and

Like the OECD, there was concern that divergent data protection laws would inhibit economic growth, with the EC (1981) proposing that member states (MSs) sign and ratify the Council of Europe Convention. Most MSs set out what were to become data protection principles and institutions in the Schengen Convention (1985), in respect of the Schengen Information System (SIS). It was only much later that the EC (1990; 1992) produced a legislative proposal,\(^{14}\) that became the Data Protection Directive 95/46/EC, with its dual objectives:

- Ensuring that Member States protect the fundamental rights and freedoms of natural persons, especially privacy; and
- Forbidding any restrictions of the free flow of personal data between Member States.

It was to create a single European market for personal data with a high level of protection for individuals, with transfer to third countries permissible only where there was an adequate level of protection. MSs had to create supervisory authorities represented in the Article 29 Working Party, a European regulatory network (ERN) that produced formal opinions, improved harmonisation and facilitated informal discussions. There were also

\(^{12}\) In the UK the Post Office (Revenues) Act 1710.

\(^{13}\) For example, the 'Nunes Memo' alleges that the US Department of Justice failed to disclose to the FISA Judge the nature of the material presented as the basis for surveillance warrants.

\(^{14}\) Encouraged by the Bangemann Report (Bangemann, 1994)
standard EU governance procedures of regular reporting on progress, including periodic privacy Eurobarometers (Poullet, 2006).

The Comité des Sages (1996) proposed rights be incorporated into the *acquis communitaire*, including addressing threats from technological advances. The EC appointed a further Expert Group on Fundamental Rights (1999), which proposed adopting all the ECHR rights and adding the right to determine the use of personal data. The inclusion of a data protection right was supported by the Article 29 Working Party (1999) and by the European Group on Ethics in Science and New Technologies (2000), and taken up by the Convention in preparing a European Constitution. With the assent of the European Parliament the Charter of Fundamental Rights was proclaimed in 2000, but only had legal force from the Lisbon Treaty in 2009.

The Charter (EU, 2016) restates in Article 7, the right to a private life, and in Article 8 the right to protection of personal data: ¹⁵

i) Everyone has the right to the protection of personal data concerning him or her.

ii) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

iii) Compliance with these rules shall be subject to control by an independent authority.

These have to be read with Article 52, explaining that any limitation of the rights must be by means of law, and respect the “essence of those rights and freedoms” and the principle of proportionality. This right was novel in international law, but was based on a range of previous legal instruments. (González Fuster, 2014)

An area of contention was the trans-Atlantic transfer of data, with MEPs protesting against inadequate safeguards that allowed the US government to access sensitive data about EU citizens. The EU-US Safe Harbour Agreement was struck down by the CJEU, to be replaced by the disliked Privacy Shield. This will become more contentious with the adoption of the US Cloud Act, purportedly requiring providers to transfer data from foreign servers to the US authorities.

Yet more controversial is the use of mass surveillance from the ePrivacy Directive 2002/58/EC, which replaced Directive 97/66/EC, empowering MSs to direct operators to retain communications data that could subsequently be used to investigate serious crimes and terrorism (Breyer, 2005; Ripoll Servent, 2013). The limitations of retention have been addressed extensively by the CJEU and ECHR, with ongoing litigation (Burke, 1981; Tele2 v PTS, 2016; Home Secretary v Watson & Ors, 2018). Arguments concern the lack of transparency in the process and the disproportionate collection of data, which government argue is essential to contain the growth of terrorism.

Some of these issues were taken up at the UN Human Rights Council,¹⁶ which appointed a Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.¹⁷ The overwhelming majority of countries lack effective checks and balances on mass surveillance powers (Korff, Wagner, Powles, Avila, & Buermeyer, 2017, p. 8), even those with constitutional provisions or that have incorporated human rights into their laws. Protection is sometimes limited to citizens within the boundaries of the state, not being extended to foreign visitors or residents, let alone data about foreign citizens, which may be

---

¹⁵ The exclusion of the Charter from the EU Withdrawal Bill is one of many contentious aspects of Brexit.


extended by the sharing between intelligence agencies, itself not always subject to oversight. Many authoritarian states systematically ignore constitutional protections.

There is somewhat limited reporting of lawful interception by operators and service providers, often with a prohibition against describing the arrangements or the scale of activity. This is complicated in some countries by senior politicians and their families owning operators, which greatly eases interception and surveillance. There have been efforts by the Telecommunications Industry Dialogue (2018) and Global Network Initiative (2017) to increase transparency, but most operators and providers decline to participate. It is difficult to see how effective pressure can be brought on such governments to become more transparent.

National security is, generally, defined in very wide terms and its use to collect data or exclude processing from data protection rules, that are rarely tested in constitutional courts. Intelligence services are not pursuing individuals who have performed specific criminal acts, but foreign agents, spies and terrorists, where the issues have rarely been set out in terms of human rights.

**Censorship**

Censorship has long been used by governments to block the access of some or all citizens to a range of materials, generally concerning moral or political issues, often based on the idiosyncratic positions of particular religious cults. The Internet opened access to a much wider range of material for those with access, but lacked the traditional controls that governments had used to block access to content. The capacity and speed of the Internet meant it was unlike intercepting books and magazines in the post, or classifying and prohibiting the distribution of films.

Demand from governments led to the development of a wide variety of software and hardware that could be used to enforce bans on specific sites or topics. For example, the Ethiopian government used software intended to filter out unsolicited commercial messages (i.e., spam) to block the sending of text messages about demonstrations and protests. The Egyptian government has had its telecommunications regulator operate a facility for deep packet inspection (DPI), allowing it to block the use of services such as voice over Internet protocol (VoIP), which would have evaded its more conventional surveillance systems. These technological advances were made independently from or beyond the sight of those protecting human rights.

The operation and fairly high level of encryption in the Telegram messaging system was designed to avoid and evade lawful interception. It has caused driven a number of governments to suppress the service or to require users to register with them, for example, Iran, Philippines, and Zimbabwe. Ironically, although a Russian company, the service has been banned there by court order, because it would not allow the government to intercept messages, but is proving difficult to block because of ‘domain fronting’ through Google.

There has long been special concern over the protection of children, to stop them being exposed some of the material readily available to adults on the Internet. This ranges from banning materials and efforts to impose age restrictions. The effectiveness of age controls is presently being tested by Facebook, which is trying to raise the age limit on its messenger service from 13 to 16 in order to comply with the GDPR.

There is a very active debate between owners of platforms such Facebook, Instagram, Twitter and YouTube about the removal of content posted by terrorists. Inevitably, there are arguments over what is classed as terrorist and the removal of material used by human rights activists in documents crimes against humanity. There are disputes over the speed of removal and the scale of the effort required of the platforms, and the potential efficacy of artificial intelligence. Such discussions and the various technical measures will continue, not
THE INTERNET AND HUMAN RIGHTS: ACCESS, CENSORSHIP, SHUTDOWNS, AND SURVEILLANCE

least in efforts to keep pace with technological advances and in improving accuracy and in reducing false positives and false negatives.

**Shutdowns**

In 2008, the then Mubarak regime in Egypt began planning for the shutdown of Internet access in the event of political unrest. Its implementation in 2011 was to be a watershed, with other authoritarian governments following its example (see Table 1). Cameroon is one of the most extreme, where the Biya regime has closed Internet access in its Anglophone region, sometimes for several months. The approach has also been used extensively in South Asian countries, often in particular provinces (Internet Shudowns, 2018).

Some short outages, for minutes or hours, are seen as technical measures, when governments are installing the latest hardware and software to improve their interception and surveillance. Indeed, this may signal to citizens that they are using the latest interception technologies. Other outages are caused by cable faults, notably affecting North Africa, since the continent is slowing moving northwards as a result of plate tectonics.

Some organisations have calculated the costs, arguing that governments should not damage their economies (OECD, 2011; West, 2016; Kathuria, Kedia, Varma, Bagchi, & Sekhani, 2018). In Egypt a legal case for damages was brought for the 2011 shutdown, with the Supreme Administrative Court fining as follows:

- Hosni Mubarak (President) EGP 200 million
- Ahmad Nazif (Prime Minister) EGP 300 million
- Habib al-Adly (Interior Minister) EGP 40 million

However, the decision and the fines were later set aside (Alaraby, 2018).

### Table 1  Recent network closures in Africa

<table>
<thead>
<tr>
<th>Country</th>
<th>Dates</th>
<th>Reasons given</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algeria</td>
<td>June 2016</td>
<td>To stop students cheating in examinations.</td>
</tr>
<tr>
<td>Cameroon</td>
<td>January-April 2017</td>
<td>None, but believed to be during suppression of protests in English speaking regions.</td>
</tr>
<tr>
<td>Chad</td>
<td>April 2016</td>
<td>For elections.</td>
</tr>
<tr>
<td>Congo</td>
<td>March 2016</td>
<td>For reasons of national security and to stop the publication of illegal results of the elections.</td>
</tr>
<tr>
<td>DRC</td>
<td>Early 2015, late 2016 &amp; early 2018</td>
<td>To help in stop and prevent protests in Kivu provinces and in the capital. To limit protests when the President’s term of office expired, and subsequent protests.</td>
</tr>
<tr>
<td>Gabon</td>
<td>2016</td>
<td>Evening for two weeks prior to the election</td>
</tr>
<tr>
<td>Gambia</td>
<td>Late 2016</td>
<td>Closed during immediate election period.</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>2016</td>
<td>To stop protests against the government, especially in Oromia region</td>
</tr>
<tr>
<td>Gabon</td>
<td>September 2016</td>
<td>Four day shutdown, then 12-hour-a-day internet curfew due to political tensions</td>
</tr>
<tr>
<td>Uganda</td>
<td>February &amp; May 2016</td>
<td>For the election period and again prior to his re-inauguration.</td>
</tr>
<tr>
<td>Zambia</td>
<td>August 2016</td>
<td>During protests at re-election of president.</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>July 2016</td>
<td>To stop the ‘Shut down Zimbabwe’ protests.</td>
</tr>
</tbody>
</table>

Internet shutdowns are easily detected, often within minutes, opening governments to early criticism (IODA, 2018). However, the administrations concerned have shown themselves inured to protests, willing to persist, either in silence or by offering justifications in terms of the threats to public order and the risk to citizens from riots and communal violence. International pressure has made no discernible difference. The economic argument has been wasted on regimes more concerned with survival than with economic damage or hardship.

---

18 For subsequent outages see Access Now, CIPESA, and Paradigm Initiative.
for citizens. The absence of administrations, courts and parliaments that will uphold rights of communication and free speech are the central problem, with the Internet merely highlighting deep-seated problems of authoritarianism.

**Conclusion**

A bill of rights for the 21st century needs to remain workable for decades, thus it should avoid issues that are already or will soon become obsolete or archaic. While the Internet may be inextricably linked to other rights (e.g., expression and privacy), it is difficult to conceive of access as a right in itself, being changeable and inconstant. For reasons of economic growth, geographical cohesion, social equity and to support the achievement of other rights governments, regulators, parliaments and the courts have pressed and supported operators to extend their services geographically to remote areas and socially to poorer citizens and to the disabled. To boost economic growth and improve productivity a range of legislative, policy and regulatory tools have been devised to facilitate the introduction and adoption of new technologies. Central questions for electorates and governments concern how quickly they want such technologies to be deployed, how extensively, and how much of their tax revenues they will pay towards such networks. It is not obvious that the processes of rights help to answer such questions.

Misuse of the Internet presents growing cybersecurity problems for businesses, citizens and governments, with threats originating from criminals, hacktivists, foreign states, terrorists, the sociopathic and the insane. At the abstraction of rights the primary issue has been privacy, from which flowed legislation for data protection to minimise data breaches and to avoid the abuse of personal data, together with laws to criminalise attacks on computer systems. The European Union created data protection as a separate right. Perhaps, the creation is more important than the right, a system of governance that identified a problem requiring changes to institutions, legislation and rights, an area where the EU has had considerable success in the work of the EC, EP and the Article 29 Working Party. Outside the EU, few countries have the governance needed to constrain the collection of data by firms, or its sale and transfer to other firms or to political parties, let alone acquisition by the secret police. Given their weaknesses in governance and rule of law, it may be easier to define a more technical right to data protection, than to try to enforce privacy. Ideally, they should be working in international networks to address complex and emerging problems, echoing the Article 29 Working Party. A major step advance would be an international treaty-based organisation for data protection, with the UN General Assembly already unanimously adopting a resolution recognizing the right to personal data protection on the Internet.19

Claims by service providers that self-regulation is sufficient are self-serving and false, firms have written incomprehensible terms and conditions, permitted but not reported data breaches, transferred data to other jurisdictions and supplied data to secret police. Their efforts at multistakeholderism, just lobbying by another name, have proved entirely insufficient to contain spam, trans-border data flows or to provide a culture of cybersecurity. This is unsurprising, since commercial drivers are not aligned with the rights of citizens, only the serving of their wants where it is sufficiently profitable. In particular, the business model of hoovering up data in the hope of future monetisation, through sale of the data, supported by multistakeholderism, has created a Facebook monster that is proving so difficult to tame. Multistakeholderism is grossly inadequate as a substitute for domestic rights, antitrust and sectoral regulation.

There are severe challenges concerning the exemption for reasons of national security from rules concerning privacy. Often the practice of surveillance and wire-tapping is not specified.

in law, while the supposed constitutional constraints are frequently ineffective. The challenge is not the bill of rights, but to devise and implement practical measures for what is permitted, what must be reported and how this can be brought under the oversight of the courts and parliaments, and to make these effective. It is equally important that the threat assessments are carefully evaluated and subject to scrutiny and oversight, for example, the threat of terrorism to public safety and the consequently need for censorship and surveillance.

The institutions dealing with constitutions and bills of rights must recognise the continuing digitalisation of society, initially in the means to devise the bill of rights and then in the ways in which it is implemented. It is necessary to engage with Internet-based technologies, requiring the transformation of government, police, regulation, parliamentary oversight and systems of appeals. Digitalisation and the use of the Internet requires considerable work in governance and in metagovernance, in the creation and periodic reform of institutions, including the training of officials, parliamentarians, police, prosecutors and judges. It requires mechanisms for the digital transformation of the police, the courts, public administration and parliaments, to ensure that they are fit for purpose. These processes will never end, there will need to be constant rounds of reviews and transformations.

Further research into the availability and use of surveillance technologies is necessary, to establish patterns of its development and diffusion. The adoption of artificial intelligence is raising new issues about the use of data and requires careful consideration.

**Bibliography**


THE INTERNET AND HUMAN RIGHTS: ACCESS, CENSORSHIP, SHUTDOWNS, AND SURVEILLANCE


González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer International. doi:10.1007/978-3-319-05023-2

González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer International. doi:10.1007/978-3-319-05023-2


OECD. (2011, February 4). *The economic impact of shutting down Internet and mobile phone services in Egypt*. Retrieved from Organisation for Economic Cooperation and Development: The economic impact of shutting down Internet and mobile phone services in Egypt


