access

TO REGULATE OR NOT TO REGULATE, IS THAT THE QUESTION?: A ROADMAP TO SMART REGULATION OF THE INTERNET

October 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The question whether to regulate or not to regulate the internet is a complex and nuanced one, and does not yield a binary answer. Just like the "offline" world, internet usage is governed by laws and regulations. Yet, online protections of user rights often lag behind those incorporated in offline; indeed, the internet's decentralized infrastructure does not lend itself well to clear rules of governance or regulation. Technological change outpaces the speed at which policy and regulations can be made, and the consequences of technological policy decisions are often difficult to predict.

Nevertheless, the novelty of the internet, its force, as well as the considerable challenges it poses on governments trying to control it, has given voice to calls to "regulate the internet." What that means exactly, if regulation is indeed necessary, and what it should look like, is the subject of serious debate. This discussion paper aims to contribute to that debate during a timely moment of introspection about what the internet has brought us and what it can bring in the future.

While all actors have an important role to play in the realization of human rights, national governments are primarily responsible for defending these rights, protecting against violations of them (by States and other actors), and taking appropriate steps to investigate and redress abuses. These international obligations apply online as they do offline, but governments, politicians, corporations, judiciaries, and civil society are increasingly uncertain about what their roles are in the digital arena.

Given that the success of today's internet has been achieved with a comparatively limited level of regulation, Access believes it important that policy makers tread carefully and err on the side of not regulating the internet. But the question is not really to regulate or not to regulate, but rather: what does a roadmap to light-handed, user-centric regulation look like?

While government efforts to regulate the internet have certainly become more frequent in recent years, these policies tend to focus on addressing "the problems" with the internet, an approach that relies on criminalizing activities. Given the many difficulties with enforcing laws on the internet, which will be discussed below, such frameworks precipitate the inclusion of increasingly draconian means to "ensure" compliance. However, critically missing in this approach is a focus on the fundamental freedoms of the users of the internet, and the important role that the internet plays in facilitating the realization of human rights. The notable exception to this trend in internet governance, is the Civil Rights Framework currently making its way through the Brazilian Congress. This proposed law takes a rights-based approach to internet policy, and is an example of the importance and the great potential of multistakeholder involvement on policy-making.[1]

In order to facilitate an understanding of regulation on the internet, this paper draws on five themes that often permeate policy discussions on regulation: privacy, national security and cybercrime, filtering and censorship, copyright enforcement, and the right to access the internet. There is necessarily much overlap between these topics. At the same time, the interaction between the various topics underlines the interwoven makeup of the internet, and the inevitable consequences of a policy in one area on other areas.

At this critical juncture, it is vital that governments, corporations, and intergovernmental bodies, in conjunction with users, make the appropriate decisions about where regulation should take place (if at all), what that regulation should look like, and how to ensure that regulation works to the benefits of all and maintains the integrity of the internet. To that end, a series of guiding principles is set out below to help policy makers navigate the crafting of regulation in this nuanced and complex policy area.

GUIDING PRINCIPLES

Access believes that the driving force of, and indeed litmus test for, internet policy should be whether regulation will enable or protect users' ability to freely, fully, and safely participate in society, and whether it will ensure the ongoing openness, quality, and integrity of the internet. Furthermore, any regulation of the internet must be targeted, necessary,

1 http://infojustice.org/archives/5684

proportionate to these goals, and achieved through the least restrictive means possible. With these maxims in mind, the questions of when and how to regulate the internet (if at all) should be informed by the following guidelines:

Maximizing Openness: Regulation cannot be wholesale. It must only be applied in the specific areas where it is deemed essential to further or maintain the openness, equality, and the integrity of the internet, and the greater realization of human rights. Access believes that the starting point of policy makers should be an unregulated internet, and when in doubt, they should err on the side of openness and the protection of the rights of users.

Managing Jurisdiction: As regulators seek to craft internet regulation based on offline legal frameworks — grounded in enforcing laws within physical geographic borders — they necessarily must confront the hyper mobility and globalization of online data. Thus, whenever States impose regulation on the internet, they need to be mindful of the effects on those outside of their borders and understand the practical limitations that national regulation can have in achieving a specific policy outcome.

Avoiding Copycat Legislation: States take inspiration from each other for regulatory frameworks, especially in new policy arenas, a tendency that is exacerbated by international treaties and trade agreements that oblige many States to enforce regulation on a wide segment of the economy. The adoption of flawed regulation that does not include relevant protections and safeguards or is insensitive to local context easily leads to dangerous copycat legislation.

Preventing Mission, Technology, and Geography Creep: The introduction of regulation to address one policy area may lead to its use in other areas, even when such measures would be disproportionate, or create significant risks for abuse. For example, monitoring frameworks (both legally and technologically) put in place to protect national security may easily fall victim to mission creep, and eventually be used to silence certain voices or track down copyright infringers. Similarly, filtering mechanisms imposed under the banner of countering child exploitation may also be used for weeding out undesired speech. Yet, once the door is opened to filtering and surveillance, there is a risk of "technology creep" as well, where increasingly invasive technologies will be developed or implemented to achieve the same "mission," which may have serious consequences for the human rights of internet users. Moreover, given the incredibly interconnected nature of the internet, national laws prescribing the filtering or removal of content can easily have adverse effects on sites and individuals in other jurisdictions. To these ends, internet policies must be: aimed at addressing specific challenges, narrowly targeted, and minimize their reach to what is strictly necessary, rather than risk curtailing the rights of all.

Keeping Pace. Keeping pace with developments is particularly difficult for technology regulation. Regulation in many jurisdictions may be decades old and ill equipped to deal with the contemporary landscape. Regulation may also easily become outdated even before it is finalized, thereby missing its target, stifling technological growth, and jeopardizing user rights. While retaining specificity, regulation should be flexible enough to protect basic rights as innovation occurs.

Ensuring Transparency, Accountability, and Appealability. As with every regulatory mechanism, transparency, accountability, and appealability are crucial. Given the potential of internet regulation to infringe upon a number of different rights, it is important to have public checks on those implementing regulation. For example, the pretense of fighting cybercrime may provide governments with a convenient cover for implementing repressive policies affecting individuals. It is important for state and non-state institutions regulating internet content and access to fully disclose all actions. Such steps need to be embedded in frameworks with independent (judicial) oversight and provide users affected with the ability to appeal regulatory case-decisions.

Beware of Industry Self-Regulation. The principles outlined here, which are targeted at governmental regulation of the internet, should also form the basis for any corporate self-regulatory approaches. While not all regulation needs to be state controlled, industry self-regulation must be not be a substitute for the State, particularly when it comes to the protection of human rights. Where corporations implement self-regulation, it is critical for it to be of the highest standard rather than reflecting a minimal compliance approach, and must be subject to adequate oversight by national governments, who ultimately are responsible for ensuring that the human rights of their citizens are respected and protected. Self-regulation must equally respect the principles of transparency, appealability, and include strong enforcement and accountability mechanisms.

Engaging multiple stakeholders. What the recommendations on each of these themes also share is the stress on empowering individuals to enjoy their rights as citizens of the internet, and to not merely be treated as buyers of a service. Implicit in this concept is the notion that wherever discussions on regulation take place, all parties must be involved, especially civil society. Where applied, multi-stakeholder approaches have brought substantial benefits (as we see with the Internet Governance Forum) to the internet and its users, and they should continue to do so.

It is critical that governments apply these principles in all areas of internet policymaking. To this end, this paper describes how these principles may be applied in five prominent areas of internet regulation and offers a series of pragmatic policy recommendations for each topic. What follows is a broad overview of the conclusions of each section.

PRIVACY

Given the wide risk for abuse that otherwise exists, states should adopt comprehensive privacy regulation. Privacy regulation needs to ensure user awareness, consent, and control over what personal information is collected and how it is used. This includes privacy policies that are clear (easy to understand), comprehensive (listing the information stored, to what length it is stored, to what length it can be shared, with whom it can be shared, what can be shared, and for what purpose), as well providing users with control over their data (ability to see exactly what information on the user is stored, and the power to correct or delete that information). Corporations must ensure that users have the ability to give explicit and informed consent to privacy policies and other terms of use, with the opportunity to withdraw this consent at any time. Moreover, data-holders have a duty to protect user data and inform users about any unauthorized access to their data.

NATIONAL SECURITY / CYBERCRIME

Regulation that provides for surveillance mechanisms by security and intelligence agencies into internet gateways, and/or legislation that provides for the aggregation of user data over longer periods can remove the presumption of innocence of citizens, turning all individuals into suspects. Moreover, it subjects all users to the risk of abuse of the mechanisms and data obtained. Such regulation should be avoided. Any measure restricting expression on national security grounds must be targeted, proportional, and in line with the internationally established rights to freedom of expression and privacy. States should not regulate to prohibit the use of encrypted technology, and, as with non-encrypted communication, must not conduct blanket monitoring of content. Any attempts to obtain the legal or technical capacity to shut off internet connectivity to a geographic location — an "internet kill switch" — should not be regulated for in any situation. In addition, States should consider regulation to defend the human rights of users, to protect vulnerable civil society sites from cyber attack, and to maximize safety for users suffering as a consequence of such attacks.

FILTERING

Filtering should generally be avoided as a policy measure to tackle societal ills. Indeed, Access is strongly opposed to any use of filtering except for the purposes of network security and management. The use of filtering technology and legislation that provides for the censoring of content is insufficiently effective at curtailing illegal activity; it also leads to undesirable outcomes and can pose significant risks to fundamental human rights. Filtering to protect society, even when child pornography is concerned, is prone to intended or unintended mission and technology creep. Moreover, filtering poses real threats to the architecture and integrity of the internet. In order to prevent abuse, if filtering is still imposed, it must be based on transparency, accountability, and rule of law, including clear and accessible appeal procedures.

COPYRIGHT ENFORCEMENT

Access is deeply concerned by national trends and international treaty proposals that attempt to regulate and enforce copyright. Access believes that the imposition of liability on internet intermediaries for the actions of their users, as well as disproportionate sanctions imposed on alleged copyright infringers, can have a chilling effect on free speech. Any measures enforcing intellectual property rights must be respectful of fundamental human rights, and incorporate safeguards to prevent abuse. Such safeguards include providing users whose content is targeted with clear appeal opportunities, providing

transparency on imposed measures, and limiting sanctions for non-commercial violations. Access is fundamentally opposed to any regulation calling for measures to disconnect users from the internet as a result of copyright infringements.

RIGHT TO INTERNET ACCESS

Despite an explosion of mobile internet users, the gap between internet usage in developed and developing nations remains large. States should regulate internet access by establishing in law that all inhabitants of the state must have the ability to access the internet, including in areas that are considered rural or remote. As the flourishing of internet use is increasingly dependent on equality of access, access must be based on net neutrality principles. Where network neutrality regulation is in place, ISPs act as neutral carriers of data, do not impose filters on content or type of content, and do not selectively affect the quality of specific web services. This protects users from additional per-service charges, ensures that entrepreneurs can have equal access to the communication network, and allows all internet users to continue using a universal, rather than fragmented web. States should establish net neutrality principles into law, which has been linked to the protection of fundamental rights (including privacy and freedom of speech) as well as aiding in development and increasing economic growth.

PRIVACY

As users increasingly turn to Information Communications Technology (ICT) for communication and all manner of educational, economic, social, and work-related tasks, the amount of personal information collected online and potentially misused or exposed has grown exponentially.

Access believes that privacy regulation needs to be informed by user awareness, consent, and control over what personal information is collected and how it is used. Access would like to acknowledge that the use of the aforementioned terms is sometimes misleading, as the reality is that users typically do not take part in the formation of regulation or the design of new technologies. Furthermore, due to the prevalence of pervasive monopolies or dysfunctional markets, users are often forced to accept whatever conditions are set forth by service providers, making "consent" an especially fleeting principle. However, as technology becomes ever more ubiquitous, the protection of privacy is an increasingly fundamental principle, and has rightly been identified as a key enabler for continued growth in e-commerce.[2] Access believes that these three principles – awareness, consent, and control – should thus guide policy, and as privacy fosters consumer trust, both in the online and offline environment, adequate enforcement mechanisms should guarantee compliance with national and international laws by the private and public sectors. Furthermore, compliance with privacy regulation should include privacy by design, where privacy features are weaved into the design of new technologies automatically. Finally, states should direct resources to the establishment and strengthening of independent data protection authorities who are adequately empowered to ensure compliance in all sectors of society.

AWARENESS AND CONSENT

The fact that users are rarely aware of what privacy policies the internet services they use have in place is a fundamental flaw in the interaction between these services and their users. Whereas the privacy policies of the services are generally easily found on their website, sometimes explicitly asking users to agree to them in order to access said services, these agreements in practice vary little from so-called "small print" conditions: difficult to read (lengthy), difficult to understand (employing legal jargon, and often not in the user's native language), and are therefore generally avoided by users. This "fact of life" does not absolve users of the responsibility to be aware of what they consent to, but it signifies the distance between common practice and a privacy policy that allows a user to make a truly informed decision about what rights they are ceding to what are often corporate providers interested in monetizing their data.

2 http://onemvweb.com/sources/sources/trustworthiness_ecommerce_role.pdf

As part of a best practice user-focused policy, internet services should make privacy policies as much as possible accessible in the native language of the user, in terms universally used across multiple platforms (including the use of symbols), and in "plain language" that is understandable to all. These policies should include clear and specific information on how long data are stored, to what length they can be shared, with whom they can be shared, what exactly is shared, and for what purpose(s).

Corporations and governments obtaining personally identifiable information through web services should seek explicit, informed, affirmative consent for using this data. Where possible, guidelines with examples indicating clearly what data are shared can help clarify what users can fairly expect will be done with their data. Corporations should be encouraged to adopt and publish such codes of conduct, and governments should ensure that they are abiding by them through regulatory instruments like Section 5 of the U.S. Federal Trade Communications Act whose mandate includes investigating and punishing unfair and deceptive practices.[3]

Recommendations

1. The law must stipulate that any personally identifiable information stored by an online service must require explicit, informed, and affirmative consent before collecting these data.
2. Informed consent entails that internet services storing personally identifiable information need to make clear to users what personal information is stored, for what length it is stored, to what extent and with whom it can be shared, what exactly is shared, and for what purpose(s). Users need to explicitly consent to these policies.
3. Limitless data retention should be rejected.
4. The law must stipulate that users should be able to request and be clearly informed about what information, which already identifies the user in question, corporations, governments, or other data holders have stored about them.
5. As part of the ability of users to control their personal information, data holders (in particular corporations) should seek explicit, informed, and affirmative consent from users for sharing information beyond what is explicitly noted in their terms of service and privacy policies or what has been protected under sensitive personal information clauses in the law. This consent-seeking requirement also applies to features using private information added after prior consent by the user.
6. In order to ensure transparency and user awareness, data holders should adequately archive the various Terms of Service Agreements — including Privacy Policies and Acceptable Use Policies — and ensure they are publicly available and readily accessible to users.
7. Additionally, in the case of changes in any Terms of Service, data holders must alert and provide a copy to users through email or other appropriate correspondence.

PROTECTING DATA AND DATA BREACH REPORTING

A crucial aspect of knowing how data are being used, shared, and protected is being made aware of security risks and unauthorized access to user data. With near weekly reports recently about data breaches, ranging from personal census information to credit card details, the vulnerability of individuals' personal information online is highlighted time and

3 http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf

again. While data retention will be discussed at length in the section on national security and cyber crime, it should suffice to say here that internet services, and other actors in the private and public sectors, have a responsibility to protect internet users' data in their possession, and inform users of security risks and violations of their privacy.[4]

Aside from protecting these data, data holders must also report any threats to the integrity of user data to the individuals concerned. Ultimately, it is the user who is the victim of data breaches and who will be further victimized by abuse of data obtained.

A policy of informing users of data breaches is already in place in the European Union under Directives 2009/136/EC[5] and 2002/58/EC[6] (Directive on privacy and electronic communications). Similar provisions are also present in the laws of several countries, including Canada,[7] Argentina,[8] South Africa[9] and Hong Kong,[10] in addition to U.S. state laws, which are being discussed on a federal level, for example under the White House Data Breach Notification proposal.[11]

Recommendations

1. The law must stipulate that web services storing personally identifiable information must take extensive measures to secure data, and must report any unauthorized access to user data as soon as possible to users potentially affected, even if there is no evidence of the data being misused.

2. All data holders must inform users of any credible risk that poses a clear and present danger to user security or privacy as expeditiously as possible.

RIGHT TO CONTROL DATA

An important part of control — and awareness — is being able to know what information is collected about oneself. Users should be able to request corporations, governments, and other data holders turn over a copy of whatever information they have stored about the user. The user should then have the ability to correct or contest any of their own data that is stored.

Users should further have the ability to request permanent removal of all private data stored by non-governmental online services and for any data collected in accounts that users themselves have created, rather than the mere temporary suspension of a user account. Such a measure may exclude information directly recording the transactions between the user and the online service, as well as basic identification information about the individual concerned. Standard opt-out procedures should include the option to remove personal information.

While encryption will be discussed later in this paper in relation to national security and cyber crime, it is worth noting here, that part of giving users control over how their data are used and shared with is allowing users access to encryption.

Recommendations

1. Users should have the ability to know what information has been collected on them by all data holders including governments and corporations.

4 2002/58/EC Article 4

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF

6 http://www.dataprotection.ie/documents/legal/directive2002_58.pdf

7 http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

8 https://www.privacyinternational.org/countries/argentina/argentine-dpa.html

9 http://www.info.gov.za/view/DownloadFileAction?id=68060

10 http://www.pcpd.org.hk/english/ordinance/section_68.html

11 http://www.whitehouse.gov/omb/legislative_letters

2. The user should have the ability to correct or contest any piece of their own data stored in public and private databases.

3. The law must stipulate that users should have the ability to request permanent deletion of all private data stored by non-governmental online services and for any data collected in accounts that users themselves have created, excluding information directly recording the transactions between the user and the online service.

PRIVACY BY DESIGN

Corporations and governments holding on to personal information should heed the "Privacy by Design" (PbD) principle, which encourages governments and corporations to incorporate privacy settings into the original design of new technologies.[12] Championed by Ann Cavoukian, Information and Privacy Commissioner of Ontario, who has intuitively stated that "the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."[13]

The PbD approach is three-pronged, and applies to IT systems, accountable business practices, and physical design and networked infrastructure. Access is fully aligned with Cavoukian's approach and encourages similar initiatives of this nature. As part of the ability of users to control their personal information, corporations should seek explicit, informed, and affirmative consent from users for sharing information beyond what has explicitly been noted in their Terms of Service and Privacy Policies, or what has been protected under sensitive personal information clauses in law.

Cavoukian's 7 Founding Principles,which collectively comprise the concept of Privacy by Design include the notion of "Privacy by Default," which states that the individual is guaranteed maximum privacy in any given product or service.[14] Specifically, these privacy settings are built into the system by default, requiring no action on behalf of the user. Despite these best practice guidelines however, the policies of internet services have caused serious concern about how they treat privacy-sensitive information, oftentimes without seeking consent of users concerned, or requiring additional steps, or opt-in features, to achieve basic levels of data protection.[15] Access believes that resources should be directed toward the strengthening of independent data protection authorities, who can advocate for user interests by ensuring compliance to applicable privacy regulations by the public and private sectors, including increasing enforcement capabilities (such as larger fines).

With regard to the cross-border transmission of data, corporations and governments obtaining user data as a third party should be obliged to respect the same (or at least as protective) privacy policies as are in place by the party to which the personal information was disclosed by the user. More broadly, one of the most complicated aspects of the cross-border transmission of data, however, is determining which jurisdiction's laws govern the protection of those data. For example, if a user in China is using a website whose corporate headquarters are in Canada with servers located in Germany, which country's laws govern the use and protection of their data? Access believes that users should be entitled to the greatest protection available in any of the jurisdictions that their data passes through (e.g., where the user is located, where the servers that store or process the data are located, or where the website has their offices). While specifying a mechanism for comparing relative protections for data is beyond the scope of this paper, this is certainly a worthwhile and important area of research for implementing this recommendation and resolving one of the major jurisdictional questions impeding the advancement of digital rights.

12 http://privacybydesign.ca/

13 http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

14 http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

15 https://www.accessnow.org/policy-activism/press-blog/facebook-comes-under-fire-for-facial-recognition-software

Recommendations

1. The law must stipulate that state and non-state actors obtaining personally identifiable information as a third party should be obliged to respect the same (or at least as protective) privacy policies as are in place by the party to which the personal information was originally disclosed by the user.
2. States should ensure that minimum standards of privacy are established in law, where independent data protection authorities are given adequate tools for enforcement and compliance in both the private and public sectors.
3. The law should stipulate that users should be entitled to the greatest protection available in any of the jurisdictions that their data passes through (e.g., where the user is located, where the servers that process or store the data are located, or where the website has their offices).
4. All bodies collecting data should adhere to principles of "privacy by default," with a view to enable users to maintain awareness, consent, and control of their data.
5. New, potentially privacy-sensitive features also require explicit and informed consent by the user (i.e. opt-in by default).
6. As a basic primary requirement, all data holders (including web services, mobile applications, etc) must have clearly articulated Privacy Policies.

DEEP PACKET INSPECTION

Advanced surveillance technologies — such as deep packet inspection (DPI) — make it possible for internet service providers to monitor the content of the internet traffic that they manage. Whether such monitoring is done on a government's behest for surveillance or censorship, for commercial reasons such as enforcing copyright, or for network management, such technologies make large-scale privacy invasion of individual internet users possible. For this reason, any use of DPI should be limited to network security and management purposes (e.g., spam, malware, and cyber attacks), or in specific cases when authorized by a court order and assessed by an independent oversight body, for a declared, necessary, and proportional purpose.

The Netherlands recently became the second country in the world, after Chile, to require that internet providers abide by the net neutrality principle. This legislation would not only prohibit providers from throttling or filtering the connections of their customers, but they would also be prevented from using DPI to spy on their customers. Indeed, the law specifies that network operators and service providers may only inspect or check communications per user request (and this consent may be withdrawn at any time) or insofar as network management purposes or legal orders prescribe.[16] Furthermore, the Dutch telecommunications watchdog, OPTA, will inspect providers to ensure compliance. Access believes this is landmark piece of legislation which other nations should emulate.

Recommendations

1. The law must stipulate that no network operator or service provider may intercept user communication unless for network security and management purposes, or in specific cases when authorized by a court order for a declared, necessary, and proportional aim.

16 Artikel 11.2a, https://zoek.officielebekendmakingen.nl/kst-119245.html.

NATIONAL SECURITY / CYBER CRIME

Regulation to protect national security has traditionally reached farther, and sometimes with fewer checks, than other policy instruments. Over the past decade, partly prompted by the terrorist attacks of September 11, 2001, new laws and regulations to protect national security have intensified worldwide. Given their perceived overriding importance, there is often reduced political space for opposition to national security policies, the rule of law may be less strongly adhered to, and the implementation of policies may be obscured from the public's view.

As societies increasingly rely on the existence of stable information systems, cyber crime has become a top priority for national security. In a broad sense, cyber crime can be defined as any crime where the computer is a target, tool, or incidental in carrying out the illicit act. Increasingly, cyber crime and online national security threats are conflated, which dangerously risks putting the farther-reaching regulation of national security tools into the hand of law enforcement for potentially less serious crimes. These tools may eventually include, and not be limited to, monitoring private communications to track copyright violations.

Since the instruments governments use to address cyber crime and national security threats often overlap, this section incorporates both policy areas. Emblematic of the increased attention given to this sphere are the announcements of a greater focus on cyber threats by the British Ministry of Defence and the FBI in recent months, which have both extended their reach further than merely national security issues.[17] The relative novelty of these fields, and the far-reaching tools that they offer, underlines the importance of ensuring that national security and crime-fighting regulations online respect and protect the rights of the public at large.

REGULATION THAT PROVIDES FOR ACCESS TO USER DATA AND SURVEILLANCE

Regulation that authorizes law enforcement and intelligence gathering for national security purposes or (cyber) crime fighting, often involves requesting insight into the data accessed and transmitted by specific individuals. Some of these regulatory measures even involve the potential for real-time surveillance of every individual on a certain network.

As the collection and storage of information becomes increasingly easy and less expensive, the retention of data is becoming standard protocol in the public and private sectors. These advances in data retention combined with the security rhetoric of the post-9/11 era have led to the introduction of a plethora of privacy-invasive security regulations around the world.[18] Nonetheless, data retention provisions have not always proven to be effective in tackling cyber crime.[19] Given the significant human rights implications of such regulation and the lack of transparency often attached to such provisions, this raises questions about the nature of the measures and their efficacy to achieve their stated aim. Access remains skeptical about the necessity and proportionality of creating additional regulatory frameworks that enable databases containing sensitive information of innocent individuals for often indefinite periods of time.

The EU Data Retention Directive,[20] which requires the indiscriminate collection and storage of all telecommunications data of every single European citizen, has rightly been described by Peter Hustinx, the European Data Protection Supervisor, as the most privacy invasive instrument ever adopted in the history of the EU.[21] In the United States, telephone companies are currently required to retain data (for long distance calls only). This past January, the Department of Justice has renewed

17 British MoD: 2010 Strategic Review. FBI: Congressional testimony by Director Mueller of June 8, 2011.

18 E.g. currently the European Union, the United States, Canada, and Australia are negotiating terms for a Passenger Name Records regime, which would require airlines flying into and out of the EU to give travellers' personal information to national authorities in the Member State of departure or arrival. Such data include, for example, home address, mobile phone number, frequent flier information, email address, and credit card information, in addition to the existence of a number of other databases related to travellers already in existence in the EU, such as the Schengen Information System (SIS), the Visa Information System (VIS), and the Advanced Passenger Information system (API).

19 http://www.pcworld.com/businesscenter/article/229901/german_crime_stats_deal_blow_to_eus_data_retention_ laws.html

20 2006/24/EC

21 http://www.computerworlduk.com/news/public-sector/3252025/european-privacy-regulator-criticises-data-retention-legislation/

calls to implement mandatory data retention by ISPs,[22] reflecting the eagerness of Western Democratic governments to implement invasive surveillance measures over all internet users. Legislation, however, may not change the practices currently in place. As privacy experts have noted, a voluntary data retention regime already exists in the US, where many telecommunications corporations– such as AT&T and Verizon – are paid 8 million USD a year by the FBI to provide real-time access to two years of stored data.[23] These regulatory measures are grossly disproportionate and impede the ability of individuals to know what and how much data is being collected, in addition to undermining the right to privacy and freedom of association.

Regulation that allows for indiscriminant surveillance by security and intelligence agencies as well as aggregating user data for indefinitely long periods of time effectively reverses the presumption of innocence, turning all citizens into suspects. Moreover, the mechanisms used to store and access these data, while often convenient for law enforcement; also substantially risks violating the privacy of users, as such systems open a backdoor which can be exploited by hackers and authorities. Indeed, such mechanisms have also been abused in the past by hackers to receive access to vast amounts of private information, and should be avoided.[24]

With the rapidly increasing requests to access user data by state actors and law enforcement authorities, there is a further risk of intermediaries facilitating automated entrances for law enforcement officials.[25] Intermediaries storing personally identifying information should insist on "one warrant, one user" provisions, that would require authorities seeking access to user accounts to obtain a specific court order, based on probable cause, for each user whose data they are requesting.

Recommendations

1. Regulation providing for access to data of individuals should be strictly limited. Any policies currently in place that allow for the indiscriminate government collection of telecommunications data of innocent citizens should be repealed.
2. Any regulations authorizing data retention need to be based on probable cause and subject to a court order, strictly limited in the length of their mandate in relation to their proportionality and effectiveness, and be void of blanket permissions to access user data. Surveillance measures should not subject all persons on a network to privacy violations, and must be user-specific and court-ordered based on probable cause.
3. Alternatives to blanket data retention, such as data preservation or "quick freeze," are a far safer, proportional, and targeted method for protecting the privacy of users and preventing abuse.
4. The law must stipulate that internet service providers and other online services should maintain sole access to their user information, and require human intervention to give legitimate law enforcement agencies access to information of/on a specific user.

ENCRYPTION

The use of encryption is an important way for people to ensure that their communications remain private. By ensuring this

22 http://www.computerworld.com/s/article/9206379/DOJ_seeks_mandatory_data_retention_requirement_for_ISPs

23 http://ediscoverymap.com/2011/01/computer-privacy-data-protection-european-data-protection-in-good-health-part-2/

24 Two prominent examples where hackers used lawful interception backdoors in communications infrastructures to access payload data: the "Athens Affair", which targeted Vodafone subscribers in March 2005 (http://spectrum.ieee.org/telecom/security/the-athens-affair/0) and an attack in 2010 on Google and 20 other companies operating China (http://www.macworld.co.uk/digitallifestyle/news/index.cfm?newsid=28293).

25 E.g., the failed "Clipper Chip" initiative in the US during the Clinton Administration and the current efforts by the U.S. law enforcement community to have Congress expand the Communications Assistance to Law Enforcement Act to require backdoors into all communications services, including all encryption software and peer-to-peer software (c.f., https://www.eff.org/deeplinks/2011/04/newly-released-documents-fail-provide).

privacy, encryption is also a key enabler of free expression. Worryingly, some states are imposing regulations that make the use of encrypted communication illegal, and threaten the privacy which encrypted communication is intended for.[26]

Several states, including Saudi Arabia, the United Arab Emirates, Kuwait, India, Indonesia, and Russia have all recently announced either formal agreements with RIM or developed surveillance technologies that compromise the encryption of user communications. According to Reporters Without Borders, "pressure on RIM has been growing since it provided information to the British authorities during the rioting in London in August, when claims that rioters were using the BlackBerry messaging service to communicate with each other caused a stir."[27] Such formal regulations and coercive agreements that provide for blanket access of state agencies to private communications should be prevented, and, where in place, repealed. Any regulation must stipulate clearly that States should only receive access to private communication when the specific need for accessing communication of a specific individual is made evident, and only after a court order based on probable cause.

Similarly, there are reports that the VoIP service Skype is under pressure to submit its encryption keys to security and intelligence agencies. Skype is recognized for providing relatively safe communication, and is therefore quite popular with activists living in countries with repressive governments. While it should be acknowledged that those intending to do harm could also use the safety of encrypted communication, this does not legitimize real-time access to the communication of all users as such a measure is grossly disproportionate to its aim. Specifically, violating the privacy of an entire population, or for example, all users of Skype in a certain country or region, in order to prevent a small fraction of individuals who may or may not intend to do harm, is not justifiable and should thus be avoided. As a security expert has rightly pointed out, " ... The good uses of infrastructure far outweigh the bad uses... And while terrorism turns society's very infrastructure against itself, we only harm ourselves by dismantling that infrastructure in response — just as we would if we banned cars because bank robbers used them too."[28]

In this vein, the U.S. Department of Commerce regulations prohibiting the export of encryption technologies to sanctioned countries is worrying, as it hurts the citizens of these nations, rather than just the repressive regimes who are actually the target of these sanctions.[29] The current list of countries that are unable to import encryption software from the US includes: Cuba, Sudan, North Korea, Iran, and Syria.[30] Access believes that this policy must be seriously reviewed in order to take into account the importance that private communications play for individuals living within repressive regimes.[31]

Recommendations

1. States should refrain from adopting measures impeding or criminalizing the use of encryption technology. Legislation that exists in States to this effect should be repealed.

2. When imposing sanctions on other countries, States should be sure that such measures keep pace with advances in what technologies are available and how they are used, with an eye to ensuring that sanctions affect only their desired targets (typically national governments), not the people living in these countries.

26 For a detailed list of restrictions on the import, export, and use of cryptology by country, please see: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm

27 http://en.rsf.org/united-kingdom-concern-that-social-networks-to-be-12-08-2011,40776.html

28 http://www.schneier.com/essay-258.html

29 Baker, L. (2010). The unintended consequences of U.S. export restrictions on software and online services for American foreign policy and human rights. Harvard Journal of Law and Technology, 23 (2), pp. 537-566.

30 http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html

31 Access notes the positive steps taken by the Department of Commerce earlier this year to ease Export Administration Regulations (EAR) on the export of open-source cryptography to Cuba, Iran, North Korea, Syria, and Sudan, but believes that substantial reform in US sanctions policy is still needed (c.f., http://www.theregister.co.uk/2011/01/07/open_source_crypto_curbs/).

3. States should only regulate to receive access to private communication when the specific need for accessing communication of a specific individual is made evident, and only after court order. This means that communication providers should not provide States with blanket access to the encrypted communications that they service.

EMERGENCY MEASURES: THE INTERNET "KILL SWITCH"

States should avoid legislation that would facilitate centralized control to completely "turn off" the internet. Such measures, imposed in Egypt in 2011 and in several other States previously, do not address national security concerns, the pretense under which they are usually employed. Like internet censorship (as discussed in the section on filtering), such measures are often employed in times of political turmoil for the purpose of suppressing political dissent, rather than for the defense of the State and its citizens. Perhaps inspired by the Mubarak regime, some governments are now seeking to establish laws and/or centralize control over internet infrastructure that would effectively enable an "internet kill switch," in an effort to prevent their citizens from communicating with each other in order to coordinate peaceful protests, demonstrations, and related civic actions; others, like the U.S., are trying to prepare for vaguely defined cyber emergencies. Access condemns any attempts to use, or even build, the technical capability or regulatory authority to cut off internet access. Moreover, given the internet's networked architecture, taking internet infrastructure offline can easily affect users outside of the jurisdiction of the State concerned, in addition to a number of other negative externalities.[32]

Access believes that States should necessarily uphold an affirmative obligation to ensure that access is maintained in time of national crisis (such as natural disasters, terrorist attacks, etc). Certain exceptions regarding national security, such as critical infrastructure attacks, should be the only instances when segments of the national network may be temporarily shut down.

However, some States have used a more subtle approach to denying their citizens' access to the internet, or at least the sites that they don't like, namely by throttling their connections to an unusable level. This allows websites to appear to be online, but in practice, achieves the same end goal of censorship, while prompting far less international condemnation, such as Egypt received when it ordered the shutoff all telecommunications services during the height of its recent Revolution.

During the Green Revolution[33] in 2009, for example, the Iranian government dedicated less bandwidth to internet connection providers, in addition to interrupting cell phone service. The democratic movement was disrupted as internet traffic dropped by 54%, illustrating Iran's more nuanced approach to control the internet, which allows it to operate – albeit at a drastically reduced speed – while utilizing the extensive state-run web-blocking infrastructure.[34] Libya, in the face of its own popular uprising also throttled its internet connection in many parts of the country rather than disconnecting the internet entirely.[35] Access believes that throttling bandwidth is the same as shutting off the Internet, as by rendering the internet unusable, the State effectively deprives its citizens of their human right to access the internet, in addition to denying their right to freedom of expression and association as enshrined in the Universal Declaration of Human Rights

Recommendations

Access believes that the State should refrain from regulating in this area.

1. No state or non-state actor should have the legislative authority or technical capacity to throttle or implement a wholesale disconnection of an entire country or region from the internet. Any laws or regulation that allows for this should be repealed.

32 For a good discussion of the flawed assumptions inherent in shutting off critical internet infrastructure during an emergency, see: https://www.schneier.com/blog/archives/2010/07/internet_kill_s.html

33 http://en.wikipedia.org/wiki/2009%E2%80%932010_Iranian_election_protests

34 http://online.wsj.com/article/SB124519888117821213.html#mod=todays_us_page_one

35 http://www.computerweekly.com/Articles/2011/03/07/245732/Libya-internet-blackout-continues.htm

RESTRICTING EXPRESSION: CENSORSHIP AND ARRESTS

As mentioned in article 19.3 of the International Covenant on Civil and Political Rights (ICCPR), national security motives can, under international human rights law, in some exceptional circumstances be legitimately used to restrict the right to freedom of expression. The UN Special Rapporteur on the right to freedom of opinion and expression argued that "protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless the Government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence."[36] Of course, as with any restriction on human rights, any limitation on the freedom of speech must be approached with great caution, subject to independent oversight and must be narrowly targeted, necessary, proportionate, and achieved through the least restrictive means possible.

Various States have imposed a wide array of measures under the banner of "national security" to silence speech. Thai prosecutors charge people critical of the royal family under national security laws, and numerous websites with similar content are banned on the same grounds.[37] Chiranuch Premchaiporn, Director of Prachatai, an independent online newspaper which reports on freedom of expression issues in Thailand, was charged and jailed for a comment left on her blog by an anonymous poster. She and countless others have been criminally prosecuted under the controversial lèse majesté laws in Thailand, where anyone who "defames, insults or threatens" the Royal Family may be imprisoned for up to fifteen years, even if they did not create or influence the allegedly defaming content.[38] This tendency is also reflected in various other countries — in liberal democracies and repressive regimes alike — where internet users voicing their opinion are imprisoned under national security provisions. Recently the Vietnamese government issued an executive decree, which grants authorities more power to penalize journalists, editors and more specifically — in a country with a bourgeoning internet culture — bloggers who report on issues loosely deemed sensitive to national security.[39]

Similarly, intermediaries are also often implicated in national security measures. For example, the Chinese government obliges internet and telecom companies to, according to Reporters without Borders, "block the transmission of vaguely defined state secrets over their networks."[40]

Recommendations

1. States must abide by the basic principles of human rights law as outlined in the Universal Declaration of Human Rights of the UN, which includes the right to freedom of opinion and expression. States should furthermore transpose these principles into national law for further codification and clarification. Finally, these laws must stipulate that these right can only be restricted in exceptional circumstances (namely the threat of imminent violence) that pass the test outlined by the Special Rapporteur for Freedom of Expression cited above. Any measure restricting the right to freedom of expression needs to be lawful, necessary, proportionate, and the least restrictive possible (see also the section on filtering).

2. In addition, whenever national security considerations serve as an incentive to restrict expression, they need to specifically describe the perceived immediate threat, rather than a general "threat to national security."

36 The Johannesburg Principles. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," 16 May 2011. Par. 36.

37 http://www.guardian.co.uk/world/2011/oct/10/us-man-insulting-thai-monarchy

38 http://www.frontlinedefenders.org/node/13727

39 http://www.cpj.org/2011/01/concern-as-vietnam-plays-national-security-censors.php

40 RSF Internet Enemies Report 2011, p. 16.

CYBER ATTACKS

In the last few months, the world has witnessed a number of attacks on government and corporate websites and databases (e.g. Sony, Epsilon, Citi Bank, RSA Security, Lockheed Martin, and the IMF[41]). While some of these breaches have been acts of cyber crime for monetary gain, many have been symbolic attacks intended to demonstrate the flaws in these sites' security systems.[42] With increasing amounts of private user data being stored online, securing communication networks and internet services has become increasingly important, and a duty to protect should be imposed on government and corporate entities by law (see also the section on privacy).[43]

With threat matrices spanning public disclosure of confidential information to defacement of websites and to distributed denial of service (DDoS) attacks that paralyze websites, the challenges to properly defending citizens can be manifold. Attacks on internet infrastructure, whether instigated by state or non-state actors, are increasingly taking a toll on internet users.[44] Yet, while attacks by Anonymous and LulzSec have dominated the news recently, these are just a very small number of the billions of cyber attacks (including malware and spam) that occur each day.[45] Today, there is more malware and spam sent over the internet than legitimate content, which is made possible by vast botnets all over the world.[46] With the Pentagon currently making rules for its cyber-conduct, and other states developing offensive cyber capabilities, it is important to make sure that internet users will not fall victim to cyber warfare and cyber crime.

An additional threat to the stability of the open internet is a proposal tabled at the UN General Assembly by China, Russia, Tajikistan, and Uzbekistan, which call for the adoption of a 12 point code of conduct, to "prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States..."[47] This is problematic for several reasons, as much of the language is broad and "could be easily interpreted by governments as allowing them to severely limit within their countries the right to freedom of expression. The caucus also says the proposed "code of conduct" excludes seeking a multi-stakeholder approach, which was outlined in the Tunis Agenda and adopted by Heads of UN member states at the 2nd phase of the World Summit on the Information Society.

At the same time, States are racing to build offensive cyber capabilities to hack each other's networks, with, for instance, al-Jazeera recently reporting that North Korea has trained a force of 3,000 "cyber warriors." There is also a separate class of "patriot hackers" who are sympathetic to a particular government, but have no direct connection to that State's government nor receive any orders from them. Another class of cyber attacks stems from people who are paid a miniscule amount of money to carry out attacks on others within and outside of a State's borders (e.g., the Chinese "fifty centers," a reference to their approximate daily wage). While reports about the U.S. Government's deeply troubling plans to develop "sock puppet armies" have recently leaked,[48] it has become glaringly apparent that cyber attacks, while ranging in severity in terms of potential damages and victims targeted, are a relatively new area that require thoughtful, comprehensive policies that

41 http://www.pcworld.com/article/230157/imf_hacked_no_end_in_sight_to_security_horror_shows.html

42 For example, hacker group LulzSec recent attack on the CIA's website in June 2011: http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html

43 A very good model for this kind of government-mandated duty to protect user data, can be found in the HIPAA (in particular Title II) and the HITECH Act, which together are the dominant legislation protecting patient heath data in the U.S..

44 It should be noted that not all hackers are "bad." For example, there are many quite well-established ethical hacking certification programs, which, among other things, train people on how to penetrate computer systems, with an eye to helping to make sites more secure and averting cyberwar. There are still more people that consider themselves "hackers" that build new technologies to help people, for example, by building blackout-resilient wireless mesh networks.

45 http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened

46 Ibid.

47 http://blog.internetgovernance.org/blog/_archives/2011/9/20/4903371.html

48 http://www.networkworld.com/community/blog/project-pm-leaks-dirt-romascoin-classified-in, http://english.aljazeera.net/indepth/features/2011/06/201162081543573839.html, http://hosted.ap.org/dynamic/stories/U/US_WAGING_CYBER_WAR?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2011-06-22-04-23-58.

focus on apprehending criminals while ensuring minimal collateral damage to the openness of the web.[49]

It has recently come to light that before the NATO attack on Libya in March 2011, the Obama administration "intensely debated" the option of waging a cyber offensive, which would have severely disrupt Libya's air-defense system.[50] The exact technique, however, remains shrouded in secrecy, but it does illustrate the impending possibility that large-scale war will soon be fought online. The acquisition of what are called "zero-day exploits," hacks that have never been seen before, making them almost impossible to prepare for. Unlike other conventional weapons, zero day exploits are "one use" weapons. Within days, if not hours of a zero day exploit being used, the cyber security community will fast become aware of this new attack write patches to reduce it's effectiveness to, ironically, zero. So zero day exploits are treasured and kept for scenarios that "really matter." It is likely that the Gadaffi threat was not considered significant enough to be worth reducing the capability of the US "zero day pool." A nation's zero day pool is like a box of matches. Whenever a match is used, it is gone and the number of "live" matches left in the box is reduced. It is worth noting that we have already seen the use of zero day exploits in fighting opponents (e.g. the Stuxnet attack on Iran).

Perhaps one of the greatest threats to freedom of speech online, and in particular to human rights organizations and other voices critical of governments, comes from the increasing prevalence of DDoS attacks. These attacks temporarily take websites down by overwhelming the site's servers with bogus requests from a botnet. Moreover, the perpetrators of such attacks may achieve "censorship by economics," given the limited financial capacity of many activist sites to pay for the increased bandwidth costs associated with DDoS attacks.

Cyber attacks may also affect more common usage for individuals' access to the web, including online financial services, playing games on the internet, and safely accessing private e-mails. These attacks not only temporarily close down services, they also cast serious doubt about the security of personal data (as is addressed in the privacy section). While the primary responsibility for securing against attacks lies with the online services themselves, governments need to penalize cyber attacks, and cooperate to prevent, investigate, and prosecute cyber attacks.

There are many established international mechanisms, organizations, and frameworks that enable States to work together to fight offline crime, which could be utilized to help crimes committed on the internet; such cooperation would also aid in reducing the jurisdictional challenges to prosecuting online crime.

Recommendations

1. The law must stipulate that any attack which is deliberately attempting to destabilize or impede on the integrity of a secured system must be penalized.
2. The law must stipulate that web services storing personally identifiable information must take extensive measures to secure the data of its users.
3. The law must stipulate that web services storing personally identifiable information must report any instances of unauthorized access to user data as soon as possible to users potentially affected, even if there is no evidence of the data being misused (See also the section on privacy).
4. Greater cooperation between international law enforcement authorities and governments should be encouraged to facilitate more effective measures enabling prosecution of cyber crimes at their source.

49 For example, the recently discovered Stuxnet virus, whose complexity suggests it may have been written by a nation state, is the first known worm designed to target critical real-world infrastructure: http://www.bbc.co.uk/news/technology-11388018

50 http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1&hp

5. Corporations and government agencies should cooperate in investigating cyber attacks, to take measures to mitigate the effects such attacks may have on the operability of systems and on the security of data, and, where possible, to maintain maximum transparency on occurring threats.

FILTERING

Filtering online content raises legitimate fears of censorship and other measures that restrict basic human rights such as freedom of expression, access to information, and privacy. Most governments around the world, democratic and non-democratic alike, restrict certain content online that quite often constitutes legal behavior. Due to the very real threats that filtering poses to the rights of users and for other reasons described below, Access is strongly opposed to any filtering except for the purposes of network security and management, and believes any laws currently enabling filter for other ends should be repealed.

The outcome of regulation that provides for internet filtering is especially problematic for five reasons: 1) Mission, technology, and geography creep is hazardous to freedom of speech and user privacy 2) Outsourcing crime fighting to private companies undermines the rule of law; 3) Widely-available circumvention technology renders filtering ineffective; 4) Filtering poses real threats to the architecture and integrity of the internet, and 5) Governments often deliberately use filtering to suppress content they find politically undesirable.

Access strongly encourages states and corporations to devise well thought out and citizen-centered regulations that guarantee the protection of human rights both off- and online. Access is strongly opposed to any measures which restrict internet access, filter, or remove content, as these threaten the fundamental rights to freedom of expression, access to information, privacy, and other rights.

FILTERING IS OFTEN INEFFECTIVE

Many states and internet regulators use the filtering (also referred to as blocking)[51] of abhorrent or immoral content, such as child exploitation, to justify censorship on the web. While child pornography and other forms of sexual exploitation of minors is reprehensible, immoral, and in clear violation of many national and international laws, Access encourages States to deal with this issue by focusing their efforts on pursuing the perpetrators of these crimes. Instead of ineffectively filtering websites, States should focus their legislative and investigative efforts on punishing the creators and viewers of child pornography, forming a strong international coalition, and supporting national legal infrastructure to deter this unlawful activity at its source.

Restricting access to criminal websites is largely cosmetic and ineffective, pushing measures to fight criminal activity away from effective enforcement and judicial processes. While many argue that filtering is at least "doing *something*," filtering actually can have a *negative effect* on the prosecution of these crimes, as it takes pressure off governments to take real action.

Not only does filtering risk contravening key international norms on freedom of expression, it is not effective in achieving its goals either. The reality is that websites change location and web addresses with such ease and frequency that it is impossible to keep any filter up to date, and as such will do little to stop deliberate access to such sites and thereby "kill the market" for perpetrators of crimes. Furthermore, research shows that criminals are increasingly sharing through peer-to-peer networks, and thus less content is actually being hosted on websites that could be filtered.[52]

Moreover, given the preponderance of circumvention tools that are easily available to internet users, those who wish to

51 Access would like to clarify that "blocking" means that the targeted websites would remain online, but that access to these websites is made more difficult. Regardless of the method used, access is always still possible.

52 http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1892&issue_id=92009

access filtered websites will continue to be able to do so.[53] Alternatively, those, particularly in the EU, that employ Privacy Enhancing Technologies (PETs) — the development and deployment of which is actively encouraged by the European Commission[54] — to access the internet will find themselves accidentally circumventing filtering systems.

MISSION AND TECHNOLOGY CREEP

While states and policy makers may have good intentions in filtering access to sites that morally offend or are a threat to national security, regulation that allows for filtering regimes of any kind is a slippery slope; already overzealous politicians and interest groups are lining up with a wish-list of content to be censored in the future. At the time of writing this paper, one of the most powerful copyright lobby groups — the Motion Picture Association of America (MPAA) — has taken a large UK ISP to court, pushing the company to block Newzbin2 (a members only usenet website) with the same system that currently blocks child abuse material.[55] As many States have already implemented filtering regimes[56] with the intention to block gambling and copyright infringing websites, it is likely that more politically sensitive or undesirable content may follow shortly after.

For example, according to research conducted by ONI Asia, "Pakistan was the first Islamic country to implement faith-based filtering to disguise the blocking of political discourse and curb freedom of expression online, and religious censorship has remained a focus of the Pakistani authorities."[57] Despite being a nominally democratic country, the internet remains restricted and is aggressively monitored by government agencies without any legal or judicial oversight. Recently, at least 13 of Pakistan's ISPs have started blocking the American magazine Rolling Stone, the name of the current president, Asif Ali Zardari, and several news sites related to Balochistan, where a strong nationalist independence movement exists.[58] This highlights the fact that the technological infrastructure that filtering and censorship mechanisms require and enable poses a threat to the openness of the web, as it technically allows future governments and corporate actors to filter virtually any type of content on the internet.

It should be noted that "blocking" is an approach to restrict content, and not limited to a specific technology. Thus if the regulatory framework is in place, the implications of content-restrictive policy may also change when technology changes, without any democratic intervention. Such technology creep, where increasingly invasive technologies are developed or implemented to achieve the same "mission," may have serious consequences on the human rights of internet users.

A relatively new trend, "just in time blocking," illustrates the steps governments take to develop more invasive and restrictive measures to suppress and control content online. "Just in time blocking" is "a phenomenon in which access to information is denied — through throttling or filtering access to specific websites — during important political moments when the content may have the greatest potential impact such as during or in advance of elections, protests, or anniversaries of social unrest."[59] As popular protests grew in Egypt in the beginning of this year, the Mubarak government, which heretofore had left the internet largely unfiltered, began filtering access to YouTube, DailyMotion, Facebook, and other sites. When this failed to quell the protests, the government ordered the nation's ISPs to shut down all internet and mobile phone connectivity in Egypt (see more on this in the section on national security).[60]

Where a complete shutdown of national connectivity by governments may be the extreme case, national authorities in a

53 Such as www.proxyforall.com and www.zend2.com

54 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF

55 http://www.bbc.co.uk/news/technology-14035502

56 EU countries that currently block sites relating to copyright infringement and/or online gambling: UK, France, Italy and Bulgaria. For an interactive map on global internet filtering practices, see: http://map.opennet.net/filtering-pol.html

57 http://opennet.net/blog/2011/06/new-internet-filtering-pakistan#footnote1_3876sff

58 http://english.aljazeera.net/indepth/opinion/2011/07/201172511310589912.html

59 http://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking

60 Ibid.

number of countries, such as Belarus, Iran, Kyrgyzstan, Bahrain, Yemen, Uganda, and China, have all controlled access to communication technology in order to suppress social movement during key political events. However, as these countries' experiences demonstrate, once the door to filtering is opened, governments will continue to develop increasingly more invasive technology to maintain their filtering regimes.

Access is strongly opposed to all filtering of the internet except for the purposes of network security and management (e.g., spam and malware).

Recommendations

1. States should promote user-based (client-side) solutions for those who wish to have filtered access to the internet (and the use of such software should be strictly optional), rather than filtering at the national internet infrastructure or DNS levels.[57]

2. Regulation that that allows governments and private actors to control the right to freedom of expression and privacy online should be reviewed with a view to ensuring that any measures that restrict fundamental rights are targeted, necessary, and proportional.

3. ISPs cannot and should not be held liable for any content hosted on their platforms/sites.

61 Access notes that the UN Special Rapporteur on the right to freedom of opinion and expression has outlined a three-part test to guide States that feel that it is absolutely necessary to engage in filtering for certain exceptional circumstances, such as child pornography: "(1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights, namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality)."

Access believes that this test does not include enough safeguards on countries that would filter. To reiterate, Access is adamantly opposed to any filtering except for the purposes of network security and management. In the exceptional circumstances when nations insist on filtering, we believe this activity should be circumscribed as much as possible, specifically:

1. Regarding the principle of predictability and transparency, the law must stipulate specifically what content is not allowed, beyond general frameworks such as the protection of national security and the protection of children.

2. The law must stipulate who the competent authority is to make decisions on filtering, and exactly what methodology it employs to determine which web content (including websites and pages) to add to filtering lists.

3. The law must stipulate that the censoring authority make a good faith effort to contact the owner of any content to be filtered to inform them of this decision and give them an opportunity to appeal.

4. The law must stipulate that whenever an internet user attempts to access filtered content, he/she must be redirected to an information page where the filtering decision is explained, pointing to the relevant legal informed, describing why the site was blocked, , and linking site visitors to a web page providing more information on filtering procedures, including an explanation of appeal processes.

5. The law must stipulate that the content-owners of filtered material and other interested parties, including internet users desiring access to the content in question, must be able to appeal the decision to filter said content.

6. Any filtering that takes place must include a periodic review of all filtered sites to check whether continued filtering of a site/page/application remains necessary.

7. The law must stipulate that dynamic filtering through deep packet inspection is not an acceptable method of filtering, except for the purposes of network security and management. Its use poses real privacy risks to users, and fails to meet the necessity of human intervention when taking a decision as critically impeding on the right to freedom of expression.

8. To meet the ends in recommendations 1-6, the law must stipulate that an independent regulatory body with judicial oversight must oversee the implementation of filtering decisions, and ensure transparency in decision-making, and provide opportunities for appeal.

9. If child pornography is filtered, the law must stipulate what types of audiovisual material fall under the definition of child pornography (e.g., the Council of Europe's Convention on Cybercrime (art. 9) and Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution (art. 2c)).

10. Governments should not put pressure on private companies/ISPs to uphold and defend the morality of society.

Furthermore, we believe that access to the internet and information communication technologies are of the utmost importance for the flourishing of human rights and participation in society. As such, governments do not and should not have the authority to shutdown national connectivity to communications technology.

THREATS FILTERING POSES TO INTERNET ARCHITECTURE

With the exception of countries like Iran and China, there is relatively little censorship occurring in the global Domain Name System (DNS). However, if more countries — and the US in particular — were to start exercising control over critical DNS infrastructure, there would likely be a flood of users shifting to alternative DNS mechanisms.

The US Congress is currently considering the PROTECT IP Act (previously called the Combating Online Infringement and Counterfeits Act, or COICA), a bill nominally designed to deter and penalize copyright infringement that poses a fundamental threat to the DNS. This bill, if passed, would replace the current Digital Millennium Copyright Act (DMCA), which, though deeply flawed (see the section below on copyright enforcement), is the dominant model of online copyright enforcement worldwide.

As internet engineers warned in an open letter in September[62] and again in a report in May of this year,[63] PROTECT IP will cause grave problems for the Domain Name System, which translates URLs like https://www.accessnow.org into IP addresses like 69.25.202.113. Essentially, the DNS is like the internet's phonebook, connecting names (domains) with numbers (IP addresses). So if the US government exerts its significant authority over the DNS to erase the entries of sites allegedly engaging in or facilitating copyright infringement, it is very likely that users will "switch phonebooks," to ones outside of the US that have not been censored.

If such a migration were to take place, the EFF reports, the inconsistencies between the official DNS and these censorship-free alternatives will "inevitably cause non-blacklisted websites to be unreachable at various times" due to propagation delays in communications between servers, make it "harder for CDNs [Content Distribution Networks] to send their clients to the right server," increase internet backbone costs by at least 20%, and cause a variety of other cyber security problems including creating obstacles for the development of DNSSEC.[64]

Top venture capitalists and independent entrepreneurs have also written to Congress about the PROTECT IP Act and how it will chill their investments in innovation.[65] Additionally, top law professors have written to Congress to express concerns about how PROTECT IP is unconstitutional.[66] In addition to these concerns, given the US' power to dictate the terms of copyright enforcement globally, PROTECT IP's passage could have dangerous repercussions worldwide.

Recommendations

1. As filtering poses significant threats to the architecture and integrity of the internet, Access urges States to assess and ameliorate any internet policies that pose a risk to the internet infrastructure, architecture, or integrity.

2. No law should stipulate tampering with the DNS for any reason.

THE DANGERS OF CORPORATE SELF-REGULATION

"Self-regulation" — cooperative regulatory solutions where industry bears primary or exclusive responsibility for enforcement — has been the dominant form of internet policy to date, given private corporations' greater adeptness at keeping pace with advances in technology, which is difficult for governments with their long regulatory processes to keep up with. Self-regulation further allows corporations to effectively manage their networks and to protect consumers

62 https://www.eff.org/deeplinks/2010/09/open-letter

63 http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf

64 https://www.eff.org/deeplinks/2010/11/case-against-coica For a more academic and detailed report on the implications of filtering to global internet architecture, see: http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf

65 http://bit.ly/vcpipaletter and http://bit.ly/qKf6fY

66 http://bit.ly/lawyerspipaletter

from problems such as malware and spam.[67] However, governments are putting increasing amounts of pressure on intermediaries to police and punish their users, whether to protect copyright or other intellectual property interests, tax revenues from online gambling, or combat child exploitation. Access does not wholesale reject self-regulation, but rather is concerned about the growing trend by governments to outsource the enforcement of the law to private companies. Internet intermediaries, as private enterprises, are ill equipped to play the role of judge, jury, and executioner over the content that is transmitted over their networks and platforms. Any self-regulatory measures must be must be transparent, accountable, based on the rule of law, include law enforcement (if the accusation is illegal activity), the possibility for judicial review, and must have appropriate due process safeguards.

Furthermore, it is important that such self-regulatory initiatives remain truly "voluntary" and not forged under undue governmental pressure, so that they not result in hasty, reactive policies that would infringe on the rights of users or would be in violation of international human rights standards.

Recommendations

1. Self-regulatory measures must be transparent, accountable, and based on the rule of law. They must also include law enforcement (if the accusation is illegal activity), judicial review, and must have appropriate due process safeguards.
2. As corporations do not have the legal competency to determine the legality of content or activities of users online, these determinations should not full under the scope of self-regulation.
3. Self-regulatory schemes need to guarantee transparency and protect the rights of users, for which oversight by an independent body is a key element.
4. The crafting and implementation of private, self-regulatory initiatives should be based on principles of multi-stakeholderism, in particular the rights and interests of users must be adequately considered and protected.
5. Self-regulatory initiatives should remain truly voluntary, and not the result of governmental pressure.

THE SALE AND PROLIFERATION OF FILTERING SOFTWARE

Another dangerous corporate trend that threatens the right to freedom of expression and privacy online is the production and sale of censorship and surveillance technologies by Western corporations (with at least the implicit consent of their governments) to repressive regimes. These companies, which operate within Canada, the United States, and the European Union, limits the moral authority of these governments to criticize the practices of repressive regimes, as they are often the actors who have provided the technology — such as Deep Packet Inspection (DPI) — in the first place. The export of advanced censorship and surveillance technology jeopardizes the rights of citizens living under these regimes. Western companies are thus playing a direct role in the proliferation of filtering technologies, and by making this type of hard- and software available to repressive regimes, they are taking sides against citizens who are censored, surveilled, prevented from disseminating content, and from participating freely, fully, and safely in society.[68]

Currently regulation surrounding the issue of the exportation of dangerous, so-called "dual-use" technologies — tools that can be used for both peaceful and military aims — is grey, as governments attempt to grapple with how best to mitigate the exportation and proliferation of these potentially harmful products. While not all companies in this industry can be

67 Successful French initiative, SignalSpam, which may be exported to other countries, such as Holland: http://woutdenatris.wordpress.com/2011/02/15/will-signal-spam-take-off-in-the-netherlands/

68 http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

lumped into the same group, it is possible to identify a handful of companies that are active in selling surveillance and censorship technology.[69] One approach to this problem has been the development of self-regulatory frameworks to control the exports of these technologies, such as the Global Network Initiative (GNI). Despite attempts to bring these companies on board however, not a single hardware vendor has joined the GNI.[70] To maintain a consistent position on democracy and human rights, particularly in regard to the democratizing potential of ICT, it is imperative that policy makers pursue strong public policy solutions to curtail the export of censorship and surveillance technologies.

The European Parliament has taken a proactive step to control the exports of dual use technologies, recently adopting a resolution that would prohibit their export to select countries (such as India, China, Turkey, and Russia) where they may be used "in connection with a violation of human rights, democratic principles or freedom of speech."[71] Access hopes this will be followed by more concrete regulation and that other countries will soon emulate this approach.

Recommendations

1. It is imperative that states develop strong and effective regulation on the production, sale, service, and proliferation of censorship and surveillance (or "dual use") technologies to other nations, in particular to States with records of human rights abuse.

2. States should take steps to end the sale and service of filtering and surveillance technologies for any purposes other than network security and management (e.g., malware, spam). They must exercise great caution and oversight in exporting these technologies to countries with poor track records of respecting human rights.

COPYRIGHT ENFORCEMENT

The enforcement of copyright is increasingly challenging the open exchange of information and communication via the internet, often to the detriment and disadvantage of internet users. The internet is not and should not be a free haven for illegal activities. However, while the objectives of copyright enforcement may be legitimate, the methods currently used by governments often significantly impinge upon the rights of users. More specifically, the imposition of liability on internet intermediaries for the actions of their users, as well as disproportionate sanctions imposed on alleged copyright infringers, is having a chilling effect on the right to freedom of expression and severely undermining the right to privacy. Intermediaries are incentivized to remove content of users, without knowing whether the content is infringing, and the fear of potential legal ramifications lead users to censor themselves.

As access to culture, freedom of communication, and privacy are key to enabling citizens to freely, fully, and safely participate in society, measures to protect intellectual property, and copyright in particular, must be targeted, necessary, and proportionate. Specifically, states and private actors should limit the enforcement of copyright with a view to reversing the risk it poses to the rights to freedom of expression and privacy, characteristic of current notice and takedown regimes in many countries in particular. This includes, but is not limited to, minimizing intermediary liability for content hosted on web platforms, restricting the release of identifying information of alleged infringers, including fair use provisions, and

69 Nokia Siemens Networks exported surveillance technology to Iran and Bahrain; Giza Systems, Narus and Gamma International to Egyptian state security; Trovicor to Bahrain; Amesys, ZTE Corp. and VASTech furnished Libya with the basis of its censorship and surveillance structure; Cisco has been accused of providing a substantial part of China's censorship infrastructure, dubbed the "Great Firewall of China"; and the McAfee Smartfilter — a database of sites used to identify sites which will be censored — has been used in Tunisia and throughout the Middle East and North Africa. (cf: Wagner, Ben. "Exporting Censorship Technology – Human Rights Impact in Tunisia and Beyond". Background Document prepared for Workshop 77 at the Internet Governance Forum 2011, Nairobi.)

70 Wagner, Ben. "Exporting Censorship Technology – Human Rights Impact in Tunisia and Beyond". Background Document prepared for Workshop 77 at the Internet Governance Forum 2011, Nairobi.

71 http://www.europarl.europa.eu/en/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports

ensuring sanctions imposed are fair in relation to the damage done.

Wherever possible, regulators should ensure that policies are designed to enable greater access to cultural works. For example, by amending legislation on orphan works, where strict copyright terms prevent public libraries, educational institutions, museums, and other non-commercial actors from digitizing or making content available to the general public.

INTERMEDIARY LIABILITY

Many states make intermediaries, including webhosting companies and online services, liable for content that they host or transport. This liability often focuses on copyrighted material, but also extends to other material deemed unlawful, including defamation and hate speech.

Laws imposing liability place a significant burden on intermediaries, at times requiring them to actively monitor content and to engage in taxing legal procedures. Such a burden stifles innovation, risks chilling online expression, and undermines privacy. The internet's success and the thriving of users' online activities require safe harbors to protect intermediaries from liability over content that they did not create or influence.

In the United States (Digital Millennium Copyright Act, art. 512), in South Africa (Electronics Communications Transactions Act, chap. XI), in South Korea (Copyright Act of Korea) and in the European Union (E-Commerce Directive), liability for intellectual property rights violations is limited by providing "notice and takedown" procedures: intermediaries can avoid liability by removing suspected content expeditiously after notification by the claimant (generally an alleged rights holder).

Even though such laws have shielded intermediaries from undue pressures and played critical roles in facilitating the growth of web services, thereby creating spaces for free expression, they are flawed in key respects. Limited liability laws have been successful in protecting the interests of intermediaries and of rights holders, but they have been remiss, or inconsistent, in protecting the rights of users. Copyright enforcement has led to inadvertent or deliberate removals of non-infringing content, and the near-automated process by which the "notice and takedown" regime is executed has adversely affected individuals' rights to privacy and freedom of expression.

To protect intermediaries, and to protect the rights of individuals online, regulation should ensure liability is limited to very specific circumstances. At the same time, copyright enforcement regimes need to provide additional safeguards for end-users. An ideal system will maintain the streamlined process with which infringing material can be removed under notice and takedown regimes, while providing stronger protection for the rights of individual internet users, and remove the incentive for providers to automatically choose the side of the claimant by removing content.

To protect the right to freedom of expression, Access supports legislation adopted in countries such as Chile and Australia, which require court orders to remove material, and in Canada, where a notification-based system discourages users from infringing, rather than summarily removing their material. Intermediaries and end-users are better served under a clear regulatory and legal framework that establishes procedures with checks and balances, rather than an undefined notice and takedown regime.

There are useful alternatives to a notice and takedown or a strictly "court-ordered" system. For instance, Mark A. Lemley and R. Anthony Reese have developed ideas for a system based on the domain name trademark Uniform Dispute Resolution Policy, and the Australian internet provider iiNet has suggested a piracy-mediation model.[72]

In a recent paper on copyright enforcement and intermediary liability,[73] Access proposed, as a proof of concept, an alternative to the notice and takedown, the dominant copyright enforcement model worldwide, which relies on a special

72 Mark A. Lemley and R. Anthony Reese, "A quick and inexpensive system for resolving peer-to-peer copyright disputes," *Cardozo Arts & Entertainment*, Vol. 23:1, 2005. "Encouraging legitimate use of Online Content. An iiNet view," iiNet, 15 March 2011, http://www.iinet.net.au/press/releases/201103-encouraging-legitimate.pdf.

73 c.f.: Access, "Towards a Rights-Respecting Copyright Enforcement Mechanism: An Alternative Approach to Notice and Takedown", 2011: https://s3.amazonaws.com/access.3cdn.net/1a153f88d1ada103f3_1cm6ivbpt.pdf

administrative mechanism to supplement a court-based system. This model would still allow for expeditious determinations on the legality of content, but without undermining users' rights. While in the notice and take down system the burden of addressing copyright infringements mainly lies with online intermediaries, the model proposed by Access takes a rights-based approach, in which due process is observed and a final decision regarding the infringement is taken by a legally competent body (rather than by a private corporation). All parties still retain the option to seek access to court a proceeding, but the system puts a critical check on the removal of content, and on prematurely disclosing the identity of users.

Recommendations

1. All action taken against illicit activity on the internet must be aimed at those directly responsible for such activities, and not at the means of access and transport — namely online intermediaries — always upholding the fundamental principles of freedom, privacy, and the respect for human rights.
2. Intermediaries must not be put in a position where they have to judge the legality of online content. The state shall provide legal certainty regarding the role of intermediaries and what they can expect in terms of rights and obligation.
3. Intermediaries must not be obliged to monitor or investigate the presence of potentially infringing material on their networks or service.
4. Material removed should be limited to only the specified items that demonstrably infringe copyright.
5. Intermediaries should clarify in their terms of service to both claimants and users how they will handle content removal requests, and clearly explain how users whose content's legality is being questioned can appeal such decisions.
6. Intermediaries should provide for accountability by publishing removal requests and their outcomes in depositories like ChillingEffects.org to ensure transparency and to facilitate a public check on frivolous and vexatious copyright claims.

ANTI-PIRACY CRACKDOWNS

The increased focus on copyright has led States to use the veil of anti-piracy efforts — an objective supported by many states — to suppress dissent. Following raids by Russian law enforcement on the offices of human rights, environmental activists, and dissidents conducted on the pretense of defending Microsoft's copyright, Microsoft has responded to public pressure on this issue by granting free software-licenses to NGOs in twelve countries.[74]

In late 2010, the U.S. Immigration and Customs Enforcement (ICE) launched rounds of domain name seizures for sites hosting allegedly infringing material, including a Spanish site declared by the Spanish courts to be non-infringing, *rojadirecta*, that was operating outside of the United States.[75] These types of website seizures raise important questions relating not only to the appropriateness and strictness of copyright enforcement, but of "geography creep", the dangerous precedent of imposing domestic laws in other national jurisdictions.

The collateral damage that IP blocking — a common method employed to restrict access to allegedly infringing websites — poses to the openness of the web is not proportionate to goals of copyright law. As many websites share IP addresses, which

74 http://www.nytimes.com/2010/10/17/world/17russia.html

75 http://www.publicknowledge.org/blog/more-domain-seizures-dojice-spanish-website-s

are often used for hundreds of separate and unrelated websites[76] — blocking an IP can involve the blocking of large numbers of perfectly innocent sites.

Such instances have already occurred in the US, where the Department of Homeland Security (DHS) accidentally seized the domain of a large DNS provider in an effort to target ten websites accused of selling counterfeited goods or hosting child abuse material; the collateral damage was disproportionate to the stated aim as 84,000 unrelated websites were taken offline.[77] For more elaboration and specific recommendations regarding the threats blocking imposes to the integrity of the web, please see the section on filtering.

Recommendations

1. Conforming to the rule of law, States should be consistent in addressing copyright infringement, and refrain from targeting civil rights organizations specifically.
2. Efforts by rights-holders to provide free licenses to civil society organizations in repressive regimes, partly to undercut directed anti-piracy crackdowns on such organizations, should be welcomed. This should also be replicated or followed up with low-cost alternatives by other companies.
3. IP blocking is a blunt tool often involving significant, disproportional damage, and should thus be avoided.

END-USER SANCTIONS AND TRADE AGREEMENTS

Trade agreements are increasingly incorporating copyright provisions that may threaten the rights of internet users. Through prescribing the implementation of these provisions in national regulations, these international trade agreements serve to quickly spread a web of unified economic and legal pressures to enforce copyright without guaranteeing proper safeguards. They risk overlooking local circumstances, and disregard the rights and interests of internet users, further exemplified by the secretive process often surrounding negotiation of the agreements.

The Anti-Counterfeiting Trade Agreement (ACTA) — a multi-lateral agreement negotiated in secret by a handful of countries which seeks to establish international standards for intellectual property rights enforcement — is controversial in both process and substance.[78] The agreement contains a number of provisions, which if signed and ratified by signatories, would have serious implications from a variety of perspectives, including harming international trade, stifling innovation, undermining democracy, and severely restricting fundamental human rights. This agreement is only one example of the growing trend to disproportionately criminalize forms of intellectual property violations, namely copyright, where the interests of private rightsholders (which are usually large corporations) trump those of user-citizens.

The Agreement has been signed by a handful of negotiating countries and is currently making its way to individual member states of the EU, eventually to the European Parliament for a final consent vote. Digital rights groups have long campaigned against such measures that undermine human rights and threaten the openness, neutrality and resilience of the internet, and strongly urge countries to swiftly reject ACTA and similar agreements that call for such blatantly disproportional enforcement of intellectual property.[79]

The Trans-Pacific Partnership Agreement (TPP) is the next major international trade agreement which the United States

76 http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/

77 http://yro.slashdot.org/story/11/02/16/2239245/US-Govt-Mistakenly-Shuts-Down-84000-Sites%22%20%5Ct%20%22_blank

78 Negotiating countries: Australia, Canada, the European Union, Japan, Mexico, Morocco, New Zealand, South Korea, Singapore, Switzerland and the United States.

79 For more information on the contentious aspects of ACTA, a short booklet has been prepared by Access, EDRi and the Trans Atlantic Consumer Dialogue (available in English, Czech, Polish, German, Romanian and French): https://www.accessnow.org/policy-activism/press-blog/access-acta-overview-anti-counterfeiting-trade-agreement

is negotiating in secret with other countries that have not signed ACTA. The current draft of the TPP prescribes ISPs to implement a "policy that provides for termination in appropriate circumstances of the accounts of repeat infringers."[80] Furthermore, it contains provisions requiring intermediaries to give information on the identity of a suspected infringer, without judicial intervention.[81] TPP further includes criminal enforcement measures, which even users that access infringing content for private use, without commercial advantage, can be subjected to.[82]

A particularly troubling aspect of many proposed laws aimed at protecting copyright is the suspension of internet access for users who are found to be repeat infringers. It should be clear that access to the internet must not be revoked from anyone.[83] To protect the users' access to the internet, the Netherlands adopted legislation prescribing to only allow ISPs to cut off web access under limited predefined circumstances, excluding violations of copyright.[84]

Recently, the G8 convened in Deauville, France, and discussed the internet and its role in society and the economy. Its final communiqué, while containing some rights-respecting language such as broadening internet access and stressing the importance of the internet as a tool for democracy, does include strong language about the protection of copyright, including intentions to develop improved methods of intellectual property rights enforcement. The increasing rhetoric about "balancing" human rights with the right to property underscores the threat that the entertainment lobby and other actors pushing for strict intellectual property enforcement pose to users' ability to freely, fully, and safely participate in society. As such, it is critical that States develop fair, justified, and reasonable approaches to the protection copyright in the online environment.

Recommendations

1. Any regulation prescribing sanctions against copyright violators should specify exactly what the threshold for violation is and what penalties violators can expect.
2. The law must specify that online intermediaries should not be considered publishers of content that they did not create or influence, and should not be liable for all that being a publisher entails in the offline world, especially as regards defamatory comments and actions by third-party users of a website (akin to the US's Communications Decency Act).
3. Sanctions imposed must be in fair relation to the damage done. The law must place proportionate limits on damages sought by rights holding claimants.
4. The law must not prescribe cutting off access to the internet. The law must inhibit releasing private information on the identity of alleged infringers to claimants without judicial intervention.
5. Multi stakeholders shall participate in the discussions and negotiations of trade agreements that might affect their rights. Individuals must enjoy their rights as citizens of the internet, and not merely be treated as buyers (or non-payers for that matter) of a service.

As will be discussed in greater depth in the section on the right to access, this organization believes that access to the internet is a human right which should be enshrined in law. No regulation should prescribe cutting off internet access as a punishment, deterrent, or as a means to prevent further copyright violations.

80 "Trans-Pacific Partnership - Intellectual Property Rights Chapter - Draft," 10 February 2011, Art. 16.3b.VI

81 TPP, Art. 16.3b.XI

82 TPP, Art. 15.1b

83 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," 16 May 2011. Par. 49, 78-79.

84 https://zoek.officielebekendmakingen.nl/dossier/32549/kst-32549-40.

RIGHT TO INTERNET ACCESS

GETTING ACCESS

Even though the gap between those who have and do not have access to the internet remains — the so-called "digital divide" — the number of internet users is increasing exponentially around the world. Approximately 1.86 billion people have access to the internet, where access to mobile networks is now available to 90% of the world population and 80% of the population living in rural areas.[85] This has, at least in part, been stimulated by the rapid expansion of mobile broadband in developing countries. Mobile broadband, in particular, is one of the facilitators of internet in rural and remote areas, where fixed line internet access remains elusive.

One of the most important impediments for individuals to benefit from access to the internet is exactly that, making sure that access the internet is available and affordable. With economic forces largely determining who has access — for example in terms of investment in infrastructure and in purchasing power for equipment and subscriptions — the web remains unreachable for many. Governments can have a role in changing this, by legislating to facilitate access, by stimulating competition, and by promoting demand.

With more and more governance information as well as government services being placed online, citizen interaction with governments is increasingly conducted over the internet, which makes ensuring internet access an even greater imperative for States, as it is a prerequisite for free, full, and safe participation in society.[86] The internet allows individuals to communicate with others, to search for information, to be educated, to play, to pursue economic opportunities, to voice their opinions, and much more. Recognizing the increasingly critical role the internet plays, several States have taken measures to legally establish the right to access the internet.

Estonia (2000) and Greece (2001) were the first and second countries to introduce universal service provisions into their laws, ensuring every citizen would be able to connect to the internet. France (in a decision by the constitutional court in 2009), the European Union (2009), and others have followed more recently.[87]

Recommendations

1. Access to the internet should be enshrined in national law. The law must stipulate that all inhabitants of the State must have the right and ability to access the internet, including in areas that are considered rural or remote.

2. Universal access provisions, coverage, and services must be enshrined into law by States. Furthermore, individuals should be able to access the internet via private connections and facilities, and where this is not possible, the State must ensure the availability of public internet access facilities.

IMPROVING ACCESS

Internet access in itself, however, is not sufficient. What also matters is the quality of access and ensuring that access is retained.

To enable effective access to the internet as a whole, internet users must be able to access the web without mandatory filters (see the section on filtering) or surveillance (see the section on national security and cyber crime). In addition, in

85 http://newsbytes.ph/2011/06/07/un-report-says-broadband-dev%E2%80%99t-still-slow-paced/

86 http://datos.fundacionctic.org/sandbox/catalog/faceted/

87 http://igbook.diplomacy.edu/2011/05/right-to-access-the-internet.

order to avoid per-service tariffs imposed on users or web services, which may fragment the internet, net neutrality must be guaranteed (see below).

Going a step further, quality internet access requires high speed and stability. In order to benefit from the internet's full potential, broadband-level internet access has become essential. More and more web services place a high demand on bandwidth, for example by utilizing video or other dynamic content. Furthermore, economies and individual users left without broadband internet access are placed at an immediate disadvantage as opposed to users of high-speed networks, in terms of efficiency, effectiveness, and potential for innovation and participation.

Similar to guaranteeing universal internet access, there has also been positive regulation on this issue. Notably, Finland (2009) and Spain (2011) have adopted laws prescribing universal access to the internet on broadband level for all users at a minimum of 1 Mbps. The Spanish government hopes this will allow broadband access to 350,000 households currently excluded from such service.[88]

It should also be noted that while internet access in developed nations has largely been a gradual process starting at dial-up, then moving onto DSL, then on to high-speed copper wires and recently fiber optic cable and mobile broadband, citizens in developing countries have taken a dramatically different trajectory to gaining access, frequently moving from no access at all to mobile internet access. Indeed, the ITU reports that in 2010, the developing world increased its share of total global mobile subscriptions to 73%, up from 53% in 2005, and now 143 countries offer 3G services commercially, compared to 95 in 2007.[89]

Recommendations

1. The law should stipulate that all inhabitants have the right to universal broadband access; this is especially important when market forces will otherwise fail to offer universal broadband access at a reasonable price.

2. States should incentivize and promote development of mobile internet infrastructure, particularly in the developing world.

NET NEUTRALITY

One of the critical components and enablers of "quality" access to the internet is ensuring that internet service providers (ISPs) act as "neutral" (or "blind") carriers of data. Where network neutrality is in place, network or service providers do not discriminate or impose filters on content or type of content, and do not selectively affect the quality (speed) of specific web services.

Competition among suppliers of internet access is an important counterforce to discriminatory access practices. Network neutrality policies prevent ISPs from charging consumers additionally for access to certain web services and applications, as well as from charging web services and applications for prioritizing their data over the network of the carrier. This neutrality facilitates innovation by providing open and equal access to services and data networks, as well as ensuring that the internet remains universal rather than fragmented. Network neutrality does not preclude ISPs from offering access packages with different (overall) speed or (overall) data bandwidth plans, but within those packages there can be no per-service/application discrimination on access and quality of access (including speed).

Network neutrality is also an issue for the less privileged, as it is about the global flow of information, an important human resource because "poverty has an important informational dimension."[90] The internet is essential for modern society and the world's economic system. The reversal of net neutrality in one country may easily have a knock on effect, prompting ISPs

88 http://www.cincodias.com/articulo/economia/banda-ancha-mega-formara-parte-servicio-universal/20110520csrcsreco_2.

89 http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

90 Ibid p. 72

and their government regulators in other countries to follow suit, which will inevitably negatively impact the developing world. Neutral access is essential for social, political, and economic growth in developing countries. As big strides are made in bridging the digital divide and as developing countries invest in related infrastructure, it is essential that net neutrality is maintained.

Research shows that broadening access to wireless networks has a direct correlation to sustainable development. Governments around the world have recognized the importance of expanding access, for they are supporting the roll out of many e-government services to promote socioeconomic development. Micro businesses in remote areas as well as large multinational companies, having recognized that the Internet can reduce costs, speed up trade, and help connect them in a more meaningful and valuable way with consumers, are also prioritizing access. However, concerning trends in the West to control content and connectivity to the web have a direct impact on the internet policies of emerging economies, where adequate infrastructure and safeguards are not always in place. Thus as the internet plays an increasingly significant role in bettering the lives of individuals in emerging economies, it is crucial that net neutrality is enshrined not only in these regions, but worldwide.[91]

Around the world there have been few, but growing, legislative initiatives to codify network neutrality. In 2010, Chile was notably the first country to adopt legislation explicitly laying out network neutrality principles, guaranteeing "the right of anyone on the internet to use, send, receive or provide any content, application or legal service through the internet without blocking or arbitrary discrimination."[92]

In the United States, the Federal Communications Commission (FCC) ruled in December 2010 that fixed broadband providers should uphold certain network neutrality principles, focused on transparency, no blocking, no unreasonable discrimination, and reasonable network management. Rules imposed on mobile carriers for mobile broadband traffic were less stringent—including allowing for blocking of some applications—on grounds of more consumer choice between carriers, the rapid state of development of mobile internet, and capacity constraints still in place.[93] These arguments are tenuous, at best.[94]

It was mobile broadband that spurred a legislative debate on net neutrality in the Netherlands in spring 2011. The issue came to the fore when mobile carriers proposed additional charges for services like VoIP (e.g., Skype) and text-over-internet (e.g., WhatsApp), explicitly arguing that they needed to compensate for their loss of income from calling and texting services. The Dutch legislature responded swiftly and adopted amendments to the Dutch Telecommunications Act, including explicit network neutrality principles.

Since the debate around net neutrality is often heated and ill informed, a report released in July of 2011 shed light on the subject, revealing that net neutrality is worth 155 billion Euros in Europe alone in 2010. Not only does this principle facilitate greater quality access to users and stimulate innovation, but is good for the bottom line.[95]

The European Data Protection Supervisor, Peter Hustinx, recently published an opinion on net neutrality,[96] which underlines that users should be given an option to have access to monitored or unmonitored networks, without having to pay more. Most notably, however, he added another dimension to the importance of upholding net neutrality by underlining its importance to enable the fundamental right to privacy. Access welcomes Hustinx's opinion as the privacy dimension is often overlooked when it comes to net neutrality. Access hopes this helps build momentum to achieving strong net neutrality regulation in the EU and elsewhere.

91 To read more about the importance of net neutrality in the developing world, see: https://s3.amazonaws.com/access.3cdn.net/950e86b3f6bb1d8467_f1m6bxeco.pdf

92 http://www.subtel.cl/prontus_subtel/site/artic/20100826/pags/ 20100826145847.html.

93 FCC ruling, par. 94-101. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf

94 https://www.accessnow.org/policy-activism/press-blog/not-neutrality-analysis-of-the-american-fccs-open-internet-order.

95 http://businessnews.za.msn.com/WSJArticle.aspx?cp-documentid=159434871

96 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf

Given the extensive nature of network neutrality on how service providers run their networks, legislation has generally provided caveats to respect the need of ISPs to manage traffic to counter cyber-attacks, to prevent spam and malware, as well as to perform data prioritization and other network management functions needed to ensure quality of service. User-requested filtering on ideological grounds (for example, to exclude porn or violence) can be possible only if the parameters are clearly indicated and the user is provided with clear opt-out options. Such additional filtering exceptions however, can complicate the legislation of net neutrality and require regulation to be as comprehensive and clear as possible, so as to not overstep the regulation's original intention (see the safeguards discussed in recommendation 6 below). That said, Access is strongly opposed to any efforts to filter the internet except for the purposes of network security and management, and believes that States should give primacy in regulation to user-based (client-side), opt-in filtering solutions, for those who really want filtered access to the internet.

Recommendations

1. The law must stipulate that access to internet services and applications must not be hindered by Internet Service Providers (ISPs), unless for network management purposes, including preserving the network's security and stability, and preventing abuse (such as spam and malware).
2. The law must stipulate that both wired and wireless providers (including mobile operators) must abide by the principles of net neutrality.
3. The law must stipulate that there must not be discrimination in quality of access to internet services, including speed or stability of access, or per content or type of content.
4. The law must stipulate that ISPs cannot make the price of internet access dependent on access to additional services or applications. Potential per-service charges should in principle only come from the application/web service itself and not from the access provider, unless so requested by the provider of the service or application.
5. Any measure imposed on a specific web service or application for the purpose of network management, or other legitimate ground recognized under (1) needs to be made public by the ISP within three days of first imposition of that measure.
6. The law may stipulate that it is permissible for ISPs to offer, at the customer's request, filtered internet access—either at the provider level or by providing client-based filtering software (such as parental controls)—as long as both filtered and unfiltered service are of the same quality and price, and that customers retain the option to obtain unfiltered internet access service at any time. Access believes that States should exercise great caution in allowing the provision of filtered internet, and States should neither encourage nor mandate that filtered access be provided. Instead States should give primacy to user-based (client-side) filtering solutions wherever possible, for users who are desirous of filtered internet access.
7. ISPs are allowed to charge end-users different prices for overall different speed and data plans.

RETAINING ACCESS

In the past, the internet may have been a luxury, accessed as a hobby or welcome research help, rather than as a critical feature of our every day lives. Now, excluding someone from access to the internet has serious consequences for their ability to participate in society. As rightly stated in a recent OECD report, the world is no longer an information economy,

but an internet economy.[97]

Unfortunately, at the same time that a right to access the internet is legally being established in several States, countervailing forces are seeking to impose sanctions that may include cutting off internet access. This issue is especially coming to the fore in relation to copyright (also addressed as such in the section on the enforcement of copyright). Laws formalizing such a "three strikes" or "graduated response" approach—making it possible to suspend the internet connection of alleged repeated infringers—have been adopted in France (HADOPI) and the United Kingdom (Digital Economy Act 2010). Copyright debates elsewhere, as well as international trade agreements being negotiated, point to similar intentions by others.

It should be clear that access to the internet must not be revoked from anyone. It is an essential means of communication, of engagement in social, civil, economic, and political life, and is critical to many other purposes as well. The UN Special Rapporteur on the right to freedom of opinion and expression has made clear that cutting off internet access is a disproportionate sanction to alleged acts of copyright infringement.[98]

In the Netherlands, a legislative amendment adopted in June 2011 prescribes to only allow ISPs to cut off web access under limited predefined circumstances — per subscriber's request, payment failure, fraud, end of term, court or legal order, or under circumstances beyond the ISP's control — thus preventing cutoffs related to copyright infringement.[99]

Recommendation

1. As access to a quality internet connection — one that is fast, stable, unmonitored, uncensored, and neutral — is fundamental to the realization and enjoyment of a plethora of human rights and free, full, and safe participation in society, no law should prescribe to cut off internet access as punishment, deterrent or prevention of further copyright violations. There should not be positive legislation to impose cutoff-restrictions on ISPs either, unless in circumstances where arbitrary cutoffs are commonplace or where only a single ISP services a geographical space.

97 OECD, "The Seoul Declaration for the Future of the Internet Economy", 18 June 2008: pg 31. http://www.oecd.org/dataoecd/49/28/40839436.pdf

98 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," 16 May 2011. Par. 49, 78-79.

99 https://zoek.officielebekendmakingen.nl/dossier/32549/kst-32549-40.

CONCLUSION

As the internet and related ICT continues to weave itself into the fabric of our daily lives, so too does pressure from the various actors in its decentralized ecosystem to control and regulate this space. The issues addressed in this paper — privacy, national security and cyber crime, filtering, copyright enforcement, and the right to access — show the manifold ways in which users are directly affected by the varying approaches to internet regulation. This paper has shown that these choices are not always straight forward, and the question whether to regulate or not to regulate the internet certainly does not yield a binary answer. Just like the "offline" world, internet usage is governed by rules and regulations. Yet, the internet's decentralized infrastructure does not lend itself well to clear rules of governance or regulation. Technological change outpaces the speed at which policy and regulations can be made, and the consequences of technological policy decisions are often difficult to predict.

As a core principle, governments must respect and protect the rights of its citizens and uphold the rule of law. While society grapples with how best to understand and respond to the risks, opportunities and potential of the internet, it is absolutely crucial that all actors approach these conundrums with the utmost understanding and thoughtfulness, so as not to destroy the conditions that have made the internet such a dynamic success — namely its openness, neutrality, and resilience. As the use of the internet shifts from being an occasional choice to an unavoidable component of participation in society, the responsibility of governments, corporations and civil society to optimize this experience only grows.

Thus, the question is not whether or not to regulate, but *how* to regulate. When implemented, regulation of the internet should only be imposed to further or protect the ability of users to freely, fully, and safely participate in society, and to ensure the openness, quality, or integrity of the internet. Any regulation must be targeted, necessary, proportionate to these goals, and achieved in the least restrictive way possible.

Government (and corporate) policies toward the internet should be focused on an internet with maximized openness, they should keep pace with technological advances, ensure transparency, accountability, and appealability, and they should enlist participation of all stakeholders. Above all, a rights respecting user-centric internet is one that everyone has high-quality access to. This policy paper is intended to serve as a roadmap to regulation that serves the interests of users, as well as to invite policy leadership on ways to achieve the above mentioned ends.