

**Access Now submission to the UN Special Rapporteur on the protection of the right to freedom of opinion and expression study on Telecommunications and Internet Access Sector**

December 2016

Table of contents

A) Introduction 2

B) Questionnaire for States 2

Direct access in India 3

Data Retention In Latin America 4

Data retention in the EU 6

In Depth: Prevention of Electronic Crimes Bill (PECB) 7

Access to metadata and users’ communication content: 8

Broadband privacy in the EU 8

U.S. broadband privacy rules 8

Government hacking and unlawful access 9

Export controls and surveillance technology 13

Cybersecurity 15

Transparency reporting and laws on disclosure of government requests 15

Remedy and oversight of cross-border data flows 16

Safeguarding access to the open and secure internet: net neutrality and zero rating 18

C) Questionnaire for companies 20

Principles and guidance to prevent infringement: Telco Action Plan 20

Internet shutdowns: The risks and opportunities for technology investors 21

Commonwealth of Surveillance States: Russian spy tech 21

Telecom’s legal challenge to data retention 22

Robust and uniform transparency and disclosures 22

Regulatory action in response to unlawful tracking 23

Mitigating and remedying abuses: Telco Remedy Plan 23

D) Internet governance and relevant standards 25

Fake Domain Attacks 25

## A) Introduction

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.[[1]](#footnote-1) By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. We are a team of 40, with local staff in 10 locations around the world. We maintain four legally registered entities - Belgium, Costa Rica, Tunisia, and the United States - with our tech, advocacy, policy, granting, and operations teams distributed across all regions.

Access Now’s policy team works at the intersection of human rights and technology, furthering Access Now’s mission by developing and promoting rights-respecting practices and policies. We defend privacy, Net Neutrality, and access to the open and secure internet globally, and work to advance public and private transparency policies, among other measures.

We commend the UN Special Rapporteur on the protection of the rights to the freedom of opinion and freedom of expression, and for leadership in furthering the protection of human rights online and offline. We welcome this opportunity to input into the Special Rapporteur’s project on the corporate responsibility of information and communications technologies companies, specifically the Telecommunications and Internet Access Sector, to human rights.

We doubly appreciate the Special Rapporteur’s decision to begin substantive reporting to the Human Rights Council on this project by focusing on the human rights responsibilities of the substrata of stakeholders in the infrastructure world, often lesser-known entities who nonetheless play essential roles in enabling the free flow of information. These stakeholders often emerge from legacies of government ownership or oversight, where they provided law enforcement assistance and swapped employees with state security and intelligence agencies, and continue to see the national security apparatus as their largest clientele base. Since deregulation, they face market pressures and competition that incentivize courses of action, like price discrimination and prioritization of certain content or applications, that often do more to restrict freedom of expression and access to information than promote these rights.

## B) Questionnaire for States

*Trends in State regulation, public-private contractual arrangements and extralegal measures identified in the* [*Questionnaire for States*](https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/QuestionnaireStates.docx)*,[[2]](#footnote-2) including variation for local, regional, and industry conditions, with positive and negative examples*

**1) Laws, regulations and other measures (including, where applicable, contractual arrangements and extra legal measures) that may permit authorities to require Telecommunications and Internet Service Providers to:**

**a) suspend or restrict access to websites or Internet and telecommunications networks; and**

Please see our previous submission including the Access Now Primer on Shutdowns and the Law, and Chart of the laws allowing internet shutdowns.

**b) provide or facilitate access to customer data;**

The global trend is toward greater law enforcement access to customer data, and for longer and broader requirements on companies to retain, decrypt, and facilitate access to that data. Our international team has spotlighted a number of issues, bills, and regions showing this pattern to rise above any particular nation’s security or law enforcement needs, below. Yet there are bright spots as well, where courts are upholding fundamental rights and reducing data retention periods and enforcing smarter privacy regulations, which we highlight.

Direct access laws directly threaten the human rights of users, by removing the insulation that third party entities can provide between governments and user data. Direct access laws remove one important barrier to blanket government access to user data: corporate policy and discretion. Companies increasingly see the protection of user data from government interference as a necessary effort to meet their human rights responsibilities. Technically, these laws force companies to create avenues of access, or “backdoors,” that an attacker or unauthorized third party can also exploit. The laws may also prevent companies from instituting strong encryption to protect user data. Simply put, when required to provide direct access, companies cannot meet their responsibility to safeguard user data from abuse.

### Direct access in India

Indian government and law enforcement agencies have been consistently applying pressure on telecom companies and other network service providers licensed in the country to facilitate direct access to networks for surveillance purposes. Most such efforts have recently focused on the deployment of the Union Government’s Centralised Monitoring System (CMS) programme.[[3]](#footnote-3)

The description of the CMS programme from official government sources has explicitly indicated it is meant to enable direct access:

The aim and objective of CMS include electronic provisioning of target number by government agency without any manual intervention from telecom service providers (TSPs) on a secured network, thus enhancing the secrecy level and quick provisioning of target…. “Secure flow of intercepted communication on near real time basis between law enforcement agency and TSPs on secured and dedicated CMS network,” the Minister said.[[4]](#footnote-4)

Besides the deployment of the infrastructure and operations for the CMS programme, the Union Government also proposed amendments to the legal environment on interception in India, in the form of a proposed Rule 419B to the Telegraph Rules. This would have provided legal cover for the CMS programme and real time surveillance operations on Indian licensed network operators. Proposed in 2013, this amendment to the Telegraph Rules has not yet been advanced. Provisions already exist in the updated Unified Service License requiring telecom licensees to install legal interception monitoring (LIM) nodes in their networks and comply with communications sent by the Union Government in this regard.[[5]](#footnote-5)

### Data Retention In Latin America

Data retention requirements do not comport with the requirements of necessity and proportionality. Rather, they are blanket mandates that treat all users and their data as suspect, and create human rights risks by requiring the creation of valuable storehouses of information.

Several Latin American countries currently impose data retention mandates for telecommunications companies and internet services, pursuant to laws and presidential decrees.

In Perú, a routine legislative delegation allowed the president to pass legislative decree 1182 in 2015. This decree established a data retention mandate for all telecommunications services for the period of three years. The data to be collected comprises “data arising from telecommunications” including communications traffic data, terminal ID and location information. Particularly, location data can be accessed by police authorities without a court order in cases of flagrant commission of a crime, which are loosely interpreted in practice and are prone to abuse.[[6]](#footnote-6)

The Civil Framework for the Internet (Marco Civil)[[7]](#footnote-7) in Brazil also creates data retention obligations not only for internet service providers – including telecommunications operators — but also for internet applications providers. Internet service providers, also referred to as “connection providers,” must keep “internet connection records” for a year. Further, internet application providers — those who offer any kind of service over the internet — are required to keep “application access logs” for six months. When requiring this information, law enforcement authorities must produce a court order. However, an exception exists in case of basic subscriber information, including personal data, affiliation, and address, where a substantiated request by an administrative authority will suffice.

Colombia presents the longest period of mandatory data retention for telecommunications operators in the region: five years. This obligation arises from two different pieces of legislation. Decree 1704/2012[[8]](#footnote-8) refers to criminal investigations and mandates telecommunications service providers to retain subscriber information and device location data in real time for a period of five years. Law 1621/2013[[9]](#footnote-9) that regulates intelligence activities, requires the same actors to retain “communications activity history for telephone subscribers, technical identification data for subscribers subject to the operation,” as well as location data.

In Colombia, with regard to criminal investigations in general, the order to access the retained data must come from the National General Prosecutor, and its execution is in the hands of a designated “Judicial Police group.” For intelligence activities, the only restriction imposed by the rule is the existence of an “authorized operation,” although the process to determine what facts merit the conduct of an intelligence operation is not transparent. The law also lacks clarity about who should authorize such operations.

Finally, Mexico has also passed legislation on data retention. Articles 189 and 190 of the Federal Telecommunications and Radio Broadcast Law (LFTR) establish a two-year data retention mandate upon telecommunications operators and “application and content service providers” — including internet applications and services. The information to be retained includes the origin, destination, duration and date of communications as well as location information. Both communications metadata and location data must be handed, according to the LFTR, to vaguely defined “competent authorities,” including “security and justice authorities,” as stated in article 189.

### Data retention in the EU

On the more positive and rights-respecting end of the spectrum, in April 2014, the Court of Justice (CJEU) ruled the EU Data Retention Directive invalid for violating the fundamental right to privacy.[[10]](#footnote-10) Adopted in 2006, the Data Retention Directive required all telecommunications data – including data from mobile, landline phones, fax, and email – to be indiscriminately collected and retained by providers for a minimum of six months and up to two years.[[11]](#footnote-11) This mass retention of citizen’s activities, outside of the context of a criminal investigation, is a significant challenge to the very foundations of the rule of law and international human rights, namely the presumption of innocence. Pursuant to the CJEU ruling, EU states are no longer required to establish data retention laws, but are still allowed to do so for public security or defense purposes. The e-Privacy Directive and recently adopted General Data Protection Regulation include provisions allowing EU states to develop measures which deviate from privacy protection rules, when these measures are necessary and proportionate, justified for a clear purpose, and in line with the EU Charter for fundamental rights.[[12]](#footnote-12)[[13]](#footnote-13)

Several EU states such as Romania or Finland have since put an end to their data retention laws, while others have taken advantage of the inaction of the EU Commission to enforce the CJEU decision and enacted excessive data retention mandates, which have a deleterious impact on human rights, the environment (as data centers require copious energy for cooling systems), and the digital economy. In Germany for instance, lawmakers have been discussing the adoption of the increased surveillance powers. In the United Kingdom, the Investigatory Powers Act 2016 was recently passed into law.[[14]](#footnote-14) The legislation in both Germany and the United Kingdom has the potential to harm human rights around the world as it codifies mass surveillance, undermines encryption, and authorizes mass government hacking.

### In Depth: Prevention of Electronic Crimes Bill (PECB)

In August 2016, the Parliament of Pakistan approved the Prevention of Electronic Crimes Act (PECB), with the stated intent to stop spamming, cyber stalking, and a long list of other actions taken online.[[15]](#footnote-15) The PECB imposes new restrictions — many of which the government has already enforced but are now codified — that will be far reaching, such as a last-minute amendment that will extend the PECB’s reach so that it applies globally. It creates significant and considerable jail time for offenders, which will include security researchers and everyday internet users.

Unfortunately, like many bills intended to make the internet more secure, this law globally undermines digital security and privacy. Opposition parties did not support the PECB.

The PECB is set to further government suppression of online speech, in line with regular government restrictions of online platforms in recent years. The law formalizes the power of government authorities to block access to content for “public order, decency, or morality.”[[16]](#footnote-16) These justifications have already been invoked to block widely used websites such as YouTube and Facebook. The new law also codifies government powers that implicate privacy and security, such as obligating individuals to assist with decrypting or otherwise providing assistance to government officials in accessing data. It is unclear how that assistance would be limited or its potential impact of security systems. Provisions that criminalize access or interference with data or systems are broadly written so that they could include the work of security researchers, who protect our rights online.

There is real need to strengthen digital security in the region. Since the bill was first introduced in 2014, civil society organizations, lawyers, legislators and many others in Pakistan have worked toward legislation that better protects user rights. Their efforts led to improvements in the text — despite efforts by supporters of the bill to limit civil society participation.

Although the PECB has passed, the government will now have to work to create regulations to implement the legislation in practice. The government should build in protections to ensure that its vague terms and broad authorizations do not further encroach upon digital rights.

### Access to metadata and users’ communication content:

### Broadband privacy in the EU

#### In the European Union, the e-Privacy Directive is the only legislation protecting users’ right to privacy and confidential communications. It safeguards user privacy when people are browsing the internet, using mobile phones, or using wearable technology and internet-connected devices. The objective of this legislation is to limit the use and collection of communications data — both content and metadata — by establishing clear rules on tracking.

#### But since its adoption in 2002, the e-Privacy Directive has failed to meet its objectives, due partly to the fact that it has not been implemented strongly or uniformly across all EU member states, and lawmakers have failed to anticipate how quickly technology would change. Its authoring legislators did not envision how developments such as smartphone apps, online tracking and marketing, the explosion of social media, or behavioural advertising would impact our privacy and the confidentiality of our communications. Conscious of the need for reform, and the necessity of aligning the e-Privacy Directive with the recently adopted General Data Protection Regulation (GDPR), the EU Commission initiated this much-needed process and is expected to present a proposal for a revised legislation in January 2017.[[17]](#footnote-17)

### U.S. broadband privacy rules

Recently, the U.S. Federal Communications Commission (FCC) voted to approve historic new rules that will require broadband internet service providers to extend privacy and security protections to users.[[18]](#footnote-18)

One of the major benefits of the new rules are its protections for web browsing data. Last summer, we reported that mobile broadband providers have been using “supercookies” to track people’s web browsing habits without their knowledge or consent.[[19]](#footnote-19) In some cases, the tracking took place without even giving users a way to opt-out. Two of the companies tracking people via supercookies, AT&T and Verizon, have pending mergers with other firms that would greatly expand their access to personal information.

Web browsing habits can reveal deeply personal details about your life. For this reason, the new U.S. rules require broadband providers to obtain affirmative consent before using “sensitive” data. The new rules further protect privacy and security by requiring that providers:

* transparently disclose information about their privacy practices to their consumers;
* obtain opt-in consent before using or sharing “sensitive” data — including the content of a user's communications, web browsing data, and app usage history;
* offer the chance to opt-out from sharing and use of other, “non-sensitive” data, such as the user’s tier-level of service;
* take “reasonable measures” to protect security; and
* notify users if there is a data breach that can cause harm.

Receiving more than 275,000 comments on its proposal, the FCC took note and adopted many recommendations to strengthen its final rules, but in some cases, the rulemaking process has resulted in watered down provisions. For example, the original proposed rules did not differentiate between “sensitive” and “nonsensitive” data. That new distinction creates ambiguity in the final rules, and it means different types of data will be treated differently.

Nevertheless, these rules will help protect privacy in the U.S. Broadband service providers have uniquely powerful, privileged access to personal information. They are the companies that transfer everyone’s internet traffic, and they have direct access to every intimate thing we do and say online. This access will only grow as we begin to use devices that are internet-enabled, and the data generated in an “Internet of Things” world will be even more intimate.

**2) Laws, regulations and other measures (including, where applicable, contractual arrangements and extralegal measures) governing/regulating the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and Internet exchange points;**

### Government hacking and unlawful access

The United States government has exploited vulnerabilities in computer systems for decades. The National Security Agency’s (NSA) Office of Tailored Access Operations has been active since the late-1990s.[[20]](#footnote-20) Similarly, the Federal Bureau of Investigation (FBI) has engaged in hacking operations since at least the early 2000s.[[21]](#footnote-21)

A report in Newsweek last year explained: According to the U.S. Intelligence Community’s 2015 “Worldwide Threat Assessment” report, Russia and China are the "most sophisticated nation-state actors” in the new generation of cyberwarfare, and Russian hackers lead in terms of sophistication, programming power and inventiveness.[[22]](#footnote-22)

APT1, a group with ties to the Chinese government, is believed to have engaged in hacking activities since at least 2006.[[23]](#footnote-23) Russia is suspected to have been behind sophisticated attacks against Estonia’s government websites in 2007, shutting down user access to many online services.[[24]](#footnote-24) Australia has broadly authorized government hacking since 1999.[[25]](#footnote-25) The law was amended in 2014 to expand the reach of the government to conduct hacking activity in bulk.[[26]](#footnote-26) In 2016, the Australian Prime Minister explained that his government’s hacking capabilities were “very considerable.”[[27]](#footnote-27)

The German intelligence agency — known as the BND — has reportedly been engaged in government hacking since at least 2009.[[28]](#footnote-28) The German police admitted to hacking in 2011.[[29]](#footnote-29) In the United Kingdom, the Home Office officially acknowledged the use of its authorities in hacking activity, dubbed Equipment Interference, in a 2015 Draft Code of Conduct that was finalized in 2016.[[30]](#footnote-30) Earlier instances of hacking by the UK government have been documented by the press.[[31]](#footnote-31) A news story in 2016 alluded to Italy’s use of malware on a mobile phone to bypass encryption protections.[[32]](#footnote-32) In addition, France passed a law in 2016 that broadly authorizes government hacking.[[33]](#footnote-33)

In 2015, an anonymous activist compromised the servers of Hacking Team, a private company established in 2003 that sells tools and services to facilitate hacking. Emails and other internet documents published by the activists revealed that the company had been contracting with repressive governments since at least 2004.[[34]](#footnote-34) Clients of Hacking Team have included government agencies or agents in Egypt, Italy, Korea, Turkey, Mexico, India, and Colombia, among others. These operations and others like them are particularly dangerous because they operate in the absence of a legal framework for their activities (and likely in violation of domestic law) and interfere with the human rights of innocent people, including political opponents, journalists, and activists.[[35]](#footnote-35)

In at least one instance in 2014, several nations cooperated in an international hacking operation known as Operation Onymous, purportedly to identify individuals suspected of engaging in criminal activity.[[36]](#footnote-36) A hacking program named Warrior Pride, which is operated jointly by the “Five Eyes” countries — the U.S., UK, Canada, Australia, and New Zealand — was revealed in the documents made available by Edward Snowden.[[37]](#footnote-37)

Even when we have information about government hacking processes and procedures, there remains a lack of transparency around their use and effectiveness.

For example, in 2014 the United States re-invigorated its Vulnerabilities Equities Process, or VEP — a process to determine whether to disclose vulnerabilities so they can be patched — after revelations surfaced suggesting that the NSA had been aware of the Heartbleed vulnerability but kept it secret, leaving it open to be exploited.[[38]](#footnote-38) The VEP, details of which were revealed in a heavily-redacted format as a result of a Freedom of Information Act lawsuit by the Electronic Frontier Foundation, appears to be largely mandatory for newly discovered or purchased vulnerabilities that are not publicly known.[[39]](#footnote-39) However, the FBI was evidently able to sidestep the VEP in 2016, when the agency revealed that when it used an exploit it apparently leased to get data from the iPhone of one of the perpetrators of the San Bernardino attack, while the agency did not submit the vulnerability to the process.[[40]](#footnote-40) The agency appeared to exploit a loophole in the VEP by purchasing the rights to use the exploit, but never actually learning how the vulnerability worked.[[41]](#footnote-41)

Moreover, government hacking operations are expanding. The market for exploits continues to grow, even as governments and companies seek to build legitimate reporting mechanisms.[[42]](#footnote-42) The United Kingdom is currently finalizing a new surveillance law that would explicitly authorize not only hacking, but hacking in “bulk,” despite urgent objections raised by several organizations.[[43]](#footnote-43) The U.S. Supreme Court recently approved controversial updates to the Federal Rules of Criminal Procedure, which remove limits on law enforcement hacking, arguably blessing U.S. hacking operations, including those that target computers en masse located around the world. Under the updated Rule 41 of the FRCP, a single warrant could be used to target not only criminals, but also potentially millions of victims of botnet exploitation.[[44]](#footnote-44) The changes automatically went into effect as U.S. Congress failed to withdraw or amend them before December 2016.

Meanwhile, Kazakhstan recently mandated the installation of software on user devices to provide direct access to communications and services.[[45]](#footnote-45) And, while Hacking Team has suffered a few small setbacks, there are several companies competing to take over as the premier hacking tool supplier to repressive nations around the world.[[46]](#footnote-46)

In the United Kingdom, the Investigatory Powers Act 2016 (IP Act) provides broad authority for the government to order service providers and equipment makers to modify underlying technology in ways that would risk user privacy. The IP Act empowers the Secretary of State to issue “technical capability notices” that would require providers modify underlying technology in order to comply with government orders.[[47]](#footnote-47) Obligation permitted under the IP Act include requiring operators to remove electronic protection (e.g. encryption) applied “by or on behalf of that operator” and modifications relating to the “handling or disclosure of any information”, presumably including personal user information.[[48]](#footnote-48)

Certain laws and bills worldwide addressing “cybercrime” contain similar provisions that require companies to provide “technical assistance” for criminal investigations. Though some of the bills contain requirements that orders be necessary, proportionate, or targeted to a specific investigation, and focused on the goal enabling access to data, if interpreted broadly this legislation may be used to compel technical changes to underlying infrastructure, thereby raising the prospect of undermining the right to freedom of expression.

The Prevention of Electronic Crimes Act in Pakistan, which came into effect this year, requires technical assistance as ordered by law enforcement from anyone in control of information systems.[[49]](#footnote-49) A similar bill in South Africa would require provision of “technical assistance,” including the removal of parts of communications networks or critical infrastructure components.[[50]](#footnote-50)

### Export controls and surveillance technology

Recent attempts to modernize export controls regimes underline an increasing need for authorities to limit the proliferation of HR harming technologies to bad-faith actors. Export controls are not a perfect solution in eliminating government-use malware and mass surveillance systems, but they can lay the groundwork for a constructive and expansive role for regulation in the promotion of human rights and cyber security goals. Current proposals include the issue of brokering and technology transit, but they avoid the issue of import controls - which are an essential component in limiting the global trade (and jurisdiction jumping) of these technologies.

In September 2016, the EU Commission published its draft proposal for an improved export controls regime, seeking to modernise and simplify the existing system in an effort to limit the expansion of “cyber surveillance technologies”.[[51]](#footnote-51) This specific category of technology known under the term “dual-use” has increasingly been used to suppress and violate human rights around the world via unlawful surveillance.

Export controls are not a simple solution. In previous efforts to control dual-use technology, the lack of precision in definitions has appeared to have a chilling effect on digital security research.[[52]](#footnote-52) Computer scientists in particular tend to have a natural aversion to government restrictions on the export of technology as they have in the past encountered restrictions on cryptography which stifled computer security. These legitimate fears have been exacerbated by some of the recent issues around the implementation of the Wassenaar Arrangement.

As governments adopt new rules and consider applications for export licenses, it is incumbent upon export control authorities to ensure that these new regulations are narrowly applied to control equipment, software, and technologies that are substantially designed for surveillance, while not undermining research and work that is fundamental to the promotion of internet security. Moreover, governments should continue to consult with industry and civil society to promote implementation of “know your customer” policies and red flags that will reduce the potential for approved, or otherwise permissible, exports that can be misappropriated for the abuse of human rights. These discussions will also enable more clear technical expectations about how exempted systems should operate in order to achieve legitimate and narrowly-defined objectives, and how to avoid unintended consequences for security research.

More broadly, clarity is needed as to how telcos choose the equipment, such as routers and switches, they install and maintain on their networks and infrastructure. As we frequently learn about vulnerabilities in both hardware and software, we more often see backdoors intentionally installed inside routers.[[53]](#footnote-53) Telecom companies should follow a more transparent approach on how they choose and vet equipment and vendors by employing robust, transparent processes and inviting public oversight and participation, and promoting the use of open-source technologies.

### Cybersecurity

Earlier this year, the European Union finalised its first pan-European cybersecurity rules: the Directive on the Security of Network and Information Systems (NIS).[[54]](#footnote-54) The Directive requires EU member states to develop and implement strict security and notification requirements for “operators of essential services” such as internet exchange points. The notification procedures must abide by the data security rules set out under the General Data Protection Regulation to avoid the possibility of sharing large amounts of users’ personal data when reporting on an incident. If a security incident leads to a breach of personal data that puts user privacy at risk, companies will have to notify the data protection authorities so that users have the opportunity to seek remedy. The Directive does not, however, limit the scope of government power in the handling and use of the data. Oversight of national data protection authorities will therefore be crucial for ensuring compliance with privacy standards. While the legislation sets minimum standards that EU member states must comply with, it remains to be seen how these standards will be implemented in practice. While the text calls for uniform standards to be developed, the vagueness of the Directive, and the discretion given to member states, could lead to the implementation of differing national standards across the EU.

**Transparency**

**3) Laws, regulations and other measures (including, where applicable, contractual arrangements and extralegal measures) on public disclosure of requests made or actions taken to a) suspend or restrict access to websites or Internet and telecommunications networks; and b) to provide or facilitate access to customer data;**

### Transparency reporting and laws on disclosure of government requests

Transparency reporting is one of the strongest ways for technology companies to disclose threats to user privacy and free expression. Such reports educate the public about company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, network disruptions, content removal, and a host of other practices impacting our fundamental rights. More than 60 companies internationally have committed to release regular transparency reports, as listed on Access Now’s regularly-updated Transparency Reporting Index.[[55]](#footnote-55) Transparency reports help investors, board members, civil society groups, and other stakeholders evaluate whether companies are meeting their commitments to be more transparent and accountable.

In a growing trend, governments are also being asked to disclose information and statistics on their requests to access users’ information or restrict content. Public officials and agencies have begun to comply as part of an effort to increase trust among citizens both in and outside their borders. This is a laudable development. However, government agencies sometimes report inconsistent or incomplete data, or refuse to release data even if they are required to do so by law.[[56]](#footnote-56)

Various national laws and regulations bar companies as well as public agencies from improving their transparency. With the support of civil society, U.S. internet firms have pushed back against government restrictions on the release of information about national security requests.[[57]](#footnote-57) Still, many countries — from Australia to the UK, South Africa, and Thailand — appear to bar public disclosure of this type of information altogether through legal prohibitions or extra-legal pressure that prevent companies from meeting their human rights responsibilities via transparency.[[58]](#footnote-58)

**4) Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data; and**

### Remedy and oversight of cross-border data flows

In the European Union, member states can decide whether their telecoms regulatory authority or data protection authority should be tasked with oversight of the rules on telecoms operators’ access to user data, as established by the e-Privacy Directive.[[59]](#footnote-59) This flexibility has lead to unequal enforcement of rights across the EU and fragmentation in the implementation of the rules to protect users’ information. This is why in the context of the review of the e-Privacy Directive, Access Now is requesting that enforcement of the future e-Privacy legislation should be assigned to the data protection authorities (DPAs), who have expertise in this area, and not to telecoms regulators, as is so often the case. This will facilitate uniformity across sectors, as DPAs are already tasked with enforcing the General Data Protection Regulation.

While implementation of a single set of rules across the EU would facilitate harmonised enforcement and help users seek redress of privacy violations, further safeguards for an efficient right to remedy must also be put in place. According to the 2015 EuroBarometer, only 37% of the respondents are aware of the existence of data protection authorities and even those respondents broadly do not know how to seek assistance and redress. To improve users’ access to remedy, consumers and NGOs should be authorised to represent a user or a group of users in claims before supervisory authorities, as in a class action. To ensure meaningful access to remedy, the legislation should also make clear that participation in administrative enforcement mechanisms do not preclude or prevent users from seeking judicial remedy.

Regarding the protection of personal data, the EU is governed by the recently adopted General Data Protection Regulation that establishes a robust and consistent mechanism for remedy. While a good baseline, due to broad "flexibilities" included in the text, users’ rights to remedy might vary from an EU country to another, depending on whether their particular EU country’s government allows collective redress and/or representation by NGOs or consumer groups.[[60]](#footnote-60) Access to remedy is further limited when users’ data is transferred to the United States under international arrangements without regard to users’ remedy rights.

The Privacy Shield - which enables the transfer of commercial and human resources data from the EU to the US since the invalidation of the Safe Harbour deal over privacy violations - aimed at providing an effective right to remedy and oversight mechanism which were lacking under its predecessor.[[61]](#footnote-61) First, the oversight relies heavily on the “multiple oversight layers” that are used to oversee US surveillance operations, including those in the executive branch, Congress, and the Judiciary, despite the fact that these three branches have frequently failed to accomplish their missions effectively. As the Snowden revelations demonstrated, even with most of these mechanisms in place, the US was able to conduct at least one known surveillance programme that, once revealed, was nearly universally believed to have been both unlawful and likely unconstitutional. With regard to remedy from improper government access to data, one of the biggest changes made from the Safe Harbour to the Privacy Shield is the creation of an “Ombudsperson,” to serve as a means for redress for EU citizens. However, the Ombudsperson is given authority only to coordinate responses to complaints filed by users and relevant authorities. The office is not empowered to initiate investigations and there is currently no mechanism for data protection authorities in the EU to transfer citizens’ claims to the Ombudsperson. Further, the lack of independence of the Ombudsperson is particularly problematic. The Ombudsperson will be housed in the US Department of State, which is a central part of the US’s intelligence framework. In fact, the specific individual designated by US Secretary of State John Kerry as Ombudsperson, Catherine A. Novelli, is directly linked to the US intelligence community in her other role as Under Secretary of State.[[62]](#footnote-62) [[63]](#footnote-63) Outside of the Ombudsperson, Privacy Shield offers no new alternative avenues for redress.

For the transfer of data between the EU and the US for law enforcement activities, the Umbrella Agreement — which should not authorise the movement of data but rather define the data protection measures that must apply when such movement takes place — is currently being finalised. The Umbrella Agreement does not fully grant EU citizens a right to remedy for privacy violations, a right that already exists for US citizens in the EU. The Judicial Redress Act of 2015, the adoption of which was linked with the Umbrella Agreement, grants a limited right for EU citizens to pursue civil remedies in cases when their personal information has been misused under certain sections of the US Privacy Act of 1974.[[64]](#footnote-64) [[65]](#footnote-65) This does not, however, protect people from misuse of data collected by federal agencies or in federal programs exempt from these protections.[[66]](#footnote-66) Nor would it allow users to initiate legal claims against companies for privacy breaches that take place in the US.

Overall, remedy has been sorely lacking for users aggrieved by both companies and governments that abuse their digital rights. Even when companies do use their legal arms to push back against government overreach, they often act more to protect their own interests than those of their users.

**5) Other relevant laws, policies or initiatives to promote or enhance Internet accessibility and connectivity, including measures to promote network neutrality.**

### Safeguarding access to the open and secure internet: net neutrality and zero rating

The early 2010s have been the years of ‘Net Neutrality’, the notion that all data on the internet should be treated equally.[[67]](#footnote-67) From the United States, to India and the European Union, landmark legislation and decisions have sought to protect access to an unfettered internet by either promoting Net Neutrality rules or preventing the establishment of ‘zero rating’ programmes. Net Neutrality is central to maintaining the internet’s potential for economic and social development, and for the exercise of internationally recognised human rights such as the right to free expression. Its principles help ensure that anyone, anywhere in the world, can receive and impart information freely over the internet, no matter where they are, what services they use, or what device they operate.

Zero rating is the opposite of Net Neutrality. Zero rating is the practice of offering internet users free access to some, but not all, of the internet, resulting in unequal access. Right now, there are two prominent models of zero rating implementation but all forms of rating amount to price discrimination, and share a negative impact on users' rights. There is the ‘telco model’, implemented by companies like Verizon and AT&T, where the company gives preferential treatment to its own content, over whatever content might be independently created using its network.[[68]](#footnote-68) The second, and much more restrictive, model is one used for sub-Internet offers such as Facebook's Free Basics programme and others, which orchestrate a tightly controlled "walled garden" network.[[69]](#footnote-69) In such an instance, tech companies insert themselves in the middle of all communications in partnership with a telecom carrier, and dictate terms for everything that users can and cannot do on the network.

The Telecom Regulatory Authority of India (TRAI) was one the first regulators to substantially look into the issue of zero rating,passing a comprehensive regulation restricting discriminatory differential pricing.[[70]](#footnote-70) The US Federal Communications Commission adopted in 2015 strong rules to safeguard Net Neutrality, but did not prescribe a general conduct standard for zero rating, leaving it to future enforcement or rule-making.[[71]](#footnote-71) Since then, US operators have launched a number of zero rating plans, which affect millions of people in the US.

The European Union has recently concluded the last stage of establishing harmonised Net Neutrality rules. On August 30, 2016, the Body of European Telecoms Regulators (BEREC) issued the final version of its guidelines for implementing these rules.[[72]](#footnote-72) BEREC addressed several important issues regarding specialised services and traffic management and established a comprehensive set of Net Neutrality rules. On zero rating, the guidelines are close to achieving the highest level of protection possible. They include an outright ban of “sub-internet” zero rating offers like Facebook’s Free Basics. They also ban telcos from offering single services for free outside of data caps, such as a Spotify or YouTube-sponsored deal. But they take a different, more ambiguous approach to other zero rating programmes implemented by telcos. Telcos could still enter into commercial agreements to favor either their own content or that of third parties. For such offers, BEREC has developed criteria for a ‘case by case’ assessment of every agreement. Robust implementation will therefore be crucial to ensure that certain internet users in Europe are not at risk of losing Net Neutrality and suffering network discrimination.

Voice over Internet Protocol (VoIP) services are currently blocked in most countries across the MENA region. The telcos often complain about a drop in long distance calling revenue when users seek VoIP services instead, and therefore they choose to block the services. However, the telcos should be encouraged to shift to business models that maximize bandwidth for data traffic. Greater efforts to establish Net Neutrality regulations in the MENA region are urgently needed in order to facilitate access to information and freedom of expression online. Short of regulations barring this sort of network discrimination, the telecom companies instituting the blocks must be pressured to lift the blocks.

## C) Questionnaire for companies

*information on the policies, practices and processes of* ***Telcos, ISPs and associated businesses*** *identified in the* [*Questionnaire for Business Enterprises*](https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/QuestionnaireBusinessEnterprises.docx)*,[[73]](#footnote-73) and their impact on the right to freedom of opinion and expression. Please identify areas of concern and, where possible, best practices and recommendations for improvement.*

**1) Prevent, mitigate or challenge the human rights impact of State laws or actions requiring your business to:**

**a) suspend or restrict access to websites or telecommunications and Internet networks; and**

### Principles and guidance to prevent infringement: Telco Action Plan

Composed in the aftermath of the Egyptian popular uprising in 2011, the Telco Action Plan[[74]](#footnote-74) contains 10 Principles for Rights-Respecting Telcos and Implementation Guidance for companies to better prevent and mitigate digital rights infringement. The best practices identified in the Principles, such as encouraging corporations to resist orders that conflict with local or international human rights law by demanding written orders signed by the proper authority, remain relevant as more companies look to push back against orders to shutdown and block networks, applications, and services. Transparency and submission to expert third party assessment can ensure long term improvement in corporate practice.

### Internet shutdowns: The risks and opportunities for technology investors

Involvement in internet shutdowns raises financial and reputational concerns for information and communication technology companies and their investors. These disruptions have been found to occur with increasing frequency, with Access Now tracking more than 53 shutdowns in 2016, compared with around 20 in 2015. These events threaten the rights and interests of technology sector investors, companies, and users worldwide. This briefing**[[75]](#footnote-75)** outlines those risks to investors with holdings in companies associated with the shutdown of internet services. It highlights the opportunity for stakeholders to make governance recommendations to companies in order to mitigate exposure to these risks. Implementing the targeted governance measures we identify can significantly improve the investment risk profile of companies involved with shutdowns.

**b) provide access to customer data;**

### Commonwealth of Surveillance States: Russian spy tech

This Access Now paper**[[76]](#footnote-76)** details growing electronic surveillance in post-Soviet Central Asia and the difficulties of regulating its manufacture and distribution. In Kazakhstan, Uzbekistan, Tajikistan, and Turkmenistan, Russian-made technologies and companies dominate the market, and techniques that have limited regulatory efficacy elsewhere — such as export controls and public campaigning — are much less effective. The current discourse on the role of Western companies in electronic surveillance is insufficient, and omits the significant agency of non-Western corporations. The paper provides a detailed analysis on how the presence of Russian technology and companies allows rights violations to continue and presents important potential avenues of redress to mass electronic surveillance in Central Asia, conducted thus far with near-impunity.

Much of the surveillance conducted in the region utilizes the System for Operative-Investigative Activities (SORM), a Russian technical framework developed by the Soviet-era secret police, the KGB.[[77]](#footnote-77) There were three versions of the system in use, at the time of this publication, which allowed for varying levels of surveillance. The increasing availability of these technologies, based on Soviet-era secret policing systems allows governments in Kazakhstan, Tajikistan, Turkmenistan, and Uzbekistan to infringe their citizens’ rights to privacy and free expression. While detailing the challenges involved in enforcing respect for human rights amidst this erosion of political rights, the paper finds a number of possible avenues for addressing these abuses: “naming and shaming” Western investors, campaigns involving the UN Human Rights Council and the Organization for Security and Co-operation in Europe, and direct engagement with individuals to improve conditions.

### Telecom’s legal challenge to data retention

In the absence of guidance from the EU Commission on how to implement the data retention invalidation ruling, some member States implemented surveillance legislation that included data retention provisions. Two data retention cases being heard together, ‘Tele2 Sverige and Davis and Others’, are awaiting decision from the CJEU, expected in 2017.[[78]](#footnote-78) Though slightly different in scope and tone, both of these cases concern the validity and extent of national data retention laws in Sweden and the UK with respect to EU law.[[79]](#footnote-79) While the issues in each case are slightly different, both cases seek to clarify to what extent national data retention is subject to the aforementioned CJEU ruling and to what extent national data retention can be governed by EU law and the EU Charter of Fundamental Rights. In the Swedish case, the ISP Tele2 has launched the case against the national data retention law on the basis of the disproportionate costs its represents for a company and raised concerns about the necessity and proportionality of the measures given their impact on user rights. The Advocate General’s opinion from July 2016 reaffirms the need to establish some of the safeguards defined under the 2014 Data Retention ruling, but it fails to clarify to what precise extent, which both cases are seeking to determine.

**3) Promote transparency about company policies and actions that impact freedom of expression; and**

Disclosure of third party requests and corporate responses impacting user rights are essential to respecting digital rights, and has become a norm of doing business in the digital age. Companies should continue to raise the floor of reporting, and innovate to overcome legal barriers to disclosure of major events like direct access, full take, and shutdown orders.

### Robust and uniform transparency and disclosures

Civil society groups are showing tech and telecom companies how they can improve their disclosures about the policy and practices they use to safeguard digital rights. In this campaign of letters to companies in Ranking Digital Rights 2015 Corporate Accountability Index,**[[80]](#footnote-80)** Access Now partnered with Ranking Digital Rights (RDR) and the Business and Human Rights Research Centre (BHRRC) to give companies targeted advice to help bring their practices in line with international human rights standards. Access Now sent letters to the Chair of the Board and Chief Executive Officer of 16 companies the practices of which had been evaluated by Ranking Digital Rights. The letters explained that fundamental rights are under attack — online as well as offline — and that companies must play a role in protecting them. Access Now informed these companies how to make necessary and important changes to their practices to respect human rights. Access Now specified objectives that are well within reach for each company — “low-hanging fruit”, such as adopting a policy opposed to internet shutdowns — and provided other best practice recommendations. Twelve of the 16 companies responded substantively to the letters. This represents a net positive, but also shows the need for greater engagement by corporate executives on the most pressing human rights issues facing their users.

### Regulatory action in response to unlawful tracking

In 2016, the Federal Communications Commission enforced a penalty[[81]](#footnote-81) against Verizon Wireless for its use of so-called ‘supercookies,’ a technology to track mobile http requests, without user consent or disclosure. According to the order, the company “failed to disclose to consumers that it was inserting Unique Identifier Headers (UIDH) into consumers’ Internet traffic over its wireless network. Verizon Wireless’s targeted advertising programs (Verizon Selects and Relevant Mobile Advertising (RMA)) associate UIDH with Verizon Wireless customer proprietary information as well as other customer demographic and interest information to create profiles in order to serve targeted advertisements.” This effective regulatory action followed extensive research by civil society[[82]](#footnote-82) and technologists showing the use of headers without transparency or notice. Researchers detailed the extensive, unlawful tracking they enable by both advertisers and unaffiliated third parties.

**4) Remediate undue restrictions on access to your company’s telecommunications and Internet services and networks, or undue access to your customers’ data.**

### Mitigating and remedying abuses: Telco Remedy Plan

Many companies and governments have publicly committed to uphold the UN Guiding Principles on Business and Human Rights. Yet the third pillar of the Guiding Principles, which establishes that companies and governments should jointly provide access effective remedy for human rights abuses, has not been developed or implemented widely.

The goal of remedy is to counteract and make good any human rights harms that have occurred. Companies and the state have shared responsibility to provide access to remedy, which can take a variety of procedural and substantive forms. To help telcos address these human rights concerns, Access Now developed the Telco Remedy Plan,**[[83]](#footnote-83)** a companion to the Access Telco Action Plan. It assists companies to implement both the procedural aspects of remedy, such as safe and accessible grievance mechanisms, and the substantive aspects, which may be as simple as an explanation and commitment to non-repetition. By approaching the question of remedy holistically, throughout the entire human rights due diligence process, telcos will be prepared to address those affected in a more timely and cost-effective way.

The Telco Remedy Plan’s ten clear steps include three procedural aspects:

1. Incorporate the question of remedy into due diligence.

2. Implement accessible and secure grievance mechanisms.

3. Respond quickly and effectively to complaints.

In addition, seven options for substantive remedy are outlined. Every step is not applicable to every claim, but these offer a path to escalate the company's response depending on the context:

4. Investigate and make policy changes to cease the rights-infringing activity.

5. Interview staff and review relevant policies, retraining and revising as needed.

6. With an eye toward assisting those affected, preserve evidence.

7. After external consultations, acknowledge and apologize where appropriate.

8. Repeated, systemic infringement should lead to independent or ongoing oversight.

9. Participate in regional or sector-wide entities to increase the telco’s leverage.

10. Those affected should be compensated where necessary to make good any human rights harms.

We recommend that companies take a holistic view and account for the question of remedy during the entire business cycle, from due diligence before securing licenses to reporting, auditing and grievance mechanisms during operations. Working with civil society organizations, submitting to third party audits, and participating in industry-wide multistakeholder organizations will allow ICT firms to craft the best human rights policies and practices, fulfill their obligations UN Guiding Principles, and reduce the long-term costs associated with unaddressed human rights complaints. We encourage stakeholders from civil society, government, and the private sector to devote greater attention to the Third Pillar of the Guiding Principles in order to help ICT companies maximize the positive role they play in modern society.

Recently, we have seen joint action by internet companies to address the issue of terrorist content on their platforms in a collaborative fashion through a central database. This type of sector-wide approach shows the potential for similar action in favor of user rights, such as via:

* a unified tracking database mapping disruptions to networks, applications, and services in real time, worldwide;
* a uniform set of transparency reports and terms of service, giving broad notice and information to users on how to control their data and understand third party access to it across platforms; and
* a centralized complaints system enabling the right to meaningful remedy.

## D) Internet governance and relevant standards

*Please share information concerning the role of relevant standards and Internet governance bodies in protecting and promoting freedom of expression, and how that role may be improved.*

### Fake Domain Attacks

While the field of internet governance and the standards bodies certainly impact human rights, we will limit our submission at this time to a specific, emerging threat to civil society. Dubbed “fake domain” attacks,[[84]](#footnote-84) these are defined as incidents in which an adversary creates a similar-looking website or social media profile to the targeted website. This may be done with the intent to draw readership from the original website and display alternative content, create confusion amongst a targeted community, or serve malware to compromise the target audience of the original website.

Fake domain attacks go beyond the phishing attacks for banking information or commercial gain traditionally understood to involve fake domains — they represent a significant front some state-aligned actors are waging against independent media and civil society organizations.

We have observed these attacks on the eves of elections and other important political events, including during critical social and political periods. Such attacks in Iran and Belarus attempted to minimize the spread of information and disrupt potential civil unrest during political elections and anniversaries. As news organizations and citizen media increasingly rely on digital means to present their work, state-level adversaries are relying on novel ways of diminishing their impact and targeting their readers.

Other attacks in Belarus and Kazakhstan utilized the privileged position internet service providers (ISPs) have in a user’s interaction with websites to redirect them away from targeted websites to the fake websites. In addition, many fake domains took advantage of procuring similarly-named URLs as the targeted website in order to provide a sense of trust to the unwary user.

All top-level-domains (TLDs) are covered by ICANN’s Uniform Domain-Name Dispute-Resolution Policy (UDRP) as a potential means of a targeted website to pursue legal action against fake domains.

The UDRP process is begun when the complaint alleges an abusive registration of a domain, in our case a fake domain targeting an existing website. Such a complaint requires (in part) that the “domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights,” probably not a difficult threshold for the fake domains with mirrored layouts, logo, designs, or content.

However, submission to the UDRP dispute process is only voluntary for country-code top-level domain names (ccTLDs). Because of this, some ccTLDs (including .uk, .de, .us, .cn, .in, and .ru) lie outside the UDRP and require disputes to be pursued through their own dispute resolution services or national civil courts. Many fake domains are registered under national registries as opposed to international registries. Situations where the dispute arbitrator is a national body related to the perpetrator of the fake domain attack could result in a difficult appeals process and leave meaningful remedy out of reach.

\*\*\*



*Access Now (*[*www.accessnow.org*](http://www.accessnow.org)*) is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.*

*For more information, contact:*

**Peter Micek | Global Policy & Legal Counsel |** **peter@accessnow.org**

*Thanks to the Access Now Policy team and Alyse Rankin for their research, writing, and editing to create this document.*

1. Access Now, [https://www.accessnow.org](https://www.accessnow.org/). [↑](#footnote-ref-1)
2. OCHCR, “Questionnaire for States” (August 2016), available at http://www.ohchr.org/Documents/Issues/Expression/Telecommunications/QuestionnaireStates.docx. [↑](#footnote-ref-2)
3. For more information on the CMS programme, see: Scroll.in, “Congress minister who put surveillance system in place warns against its ‘lawful but malicious’ use” (28 May 2015), available at http://scroll.in/article/729701/congress-minister-who-put-surveillance-system-in-place-warns-against-its-lawful-but-malicious-use; Medianama, “Govt’s Central Monitoring System already live in Delhi and Mumbai” (11 May 2016), available at http://www.medianama.com/2016/05/223-india-central-monitoring-system-live-in-delhi-mumbai/; The Economic Times, “Government setting up centralised monitoring system for lawful interception: Ravi Shankar Prasad” (4 May 2016), available at http://economictimes.indiatimes.com/news/economy/policy/government-setting-up-centralised-monitoring-system-for-lawful-interception-ravi-shankar-prasad/articleshow/52111222.cms;

Takshashila Institution, “India’s Central Monitoring System” (July 2013), available at http://takshashila.org.in/wp-content/uploads/2013/07/India%E2%80%99s-Central-Monitoring-System-Rohan-Joshi.pdf. [↑](#footnote-ref-3)
4. The Economic Times, “Government setting up centralised monitoring system for lawful interception: Ravi Shankar Prasad” (4 May 2016), available at http://economictimes.indiatimes.com/articleshow/52111222.cms. [↑](#footnote-ref-4)
5. See: The Economic Times, “Prepare yourself to be snooped in the interest of national security” (27 December 2013), available at http://articles.economictimes.indiatimes.com/2013-12-27/news/45626736\_1\_indian-telegraph-act-national-security-telecom-department; Indian Journal of Law and Technology, “The Central Monitoring System and Privacy: Analysing What We Know So Far” (2014), available at http://ijlt.in/wp-content/uploads/2015/08/IJLT-Volume-10.41-62.pdf. [↑](#footnote-ref-5)
6. Acccess Now, “Data retention in Peru: a poor copy of a bad idea” (17 August 2015), available at https://www.accessnow.org/data-retention-in-peru-a-poor-copy-of-a-bad-idea/. [↑](#footnote-ref-6)
7. Presidency of the Republic of Brazil, Civil House Legal Affairs Subsection, “Principles, guarantees, rights and obligations for the use of Internet in Brazil: Articles 13 and 15” (23 April 2014), available at https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf. [↑](#footnote-ref-7)
8. Government of Colombia Ministry of Information Technologies and Communications, “Presidential Decree Nº 1704” (15 August 2012), available at http://www.mintic.gov.co/portal/604/articles-3559\_documento.pdf. [↑](#footnote-ref-8)
9. Congress of the Republic of Colombia, “Law 1621/2013” (17 April 2013), available at: http://web.archive.org/web/20140826121112/http://200.75.47.49/senado/basedoc/ley/2013/ley\_1621\_2013\_pr001.html. [↑](#footnote-ref-9)
10. European Court of Justice Grand Chamber, “Judgment of the Court in Joined Cases C-293/12 and C-594/12” (8 April 2014), available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30db64b73b07787a4f539fdea33356c73fe9.e34KaxiLc3qMb40Rch0SaxuNaN50?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=467902. [↑](#footnote-ref-10)
11. European Parliament and Council, “Directive 2006/24/EC on the retention of data generated or processed in conncetion wtih the provision of publicly availably electronic communications services of of public communications networks and amending Directive 2002/58/EC” (15 March 2006), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. [↑](#footnote-ref-11)
12. European Parliament and Council, “Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)” (12 July 2002), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML. [↑](#footnote-ref-12)
13. European Parliament and Council, “Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)” (27 April 2016), available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. [↑](#footnote-ref-13)
14. Parliament of United Kingdom, “Investigatory Powers Act 2016” (29 November 2016), available at http://services.parliament.uk/bills/2015-16/investigatorypowers.html. [↑](#footnote-ref-14)
15. National Assembly of Pakistan, “Prevention of Electronic Crimes Act” (11 August 2016), available at http://www.na.gov.pk/uploads/documents/1472635250\_246.pdf. [↑](#footnote-ref-15)
16. Ibid., § 37. [↑](#footnote-ref-16)
17. For more information, see: Access Now, “Review of the e-Privacy Directive” (July 2016), available at https://www.accessnow.org/cms/assets/uploads/2016/07/ePrivacy-Review-Policy-Paper-1.pdf. [↑](#footnote-ref-17)
18. Access Now, “U.S. broadband privacy rules grant users control, meaningful rights protections” (7 November 2016), available at https://www.accessnow.org/u-s-broadband-privacy-rules-grant-users-control-meaningful-rights-protections/. [↑](#footnote-ref-18)
19. Access Now, “The Rise of Mobile Tracking Headers” (August 2015), available at https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf. [↑](#footnote-ref-19)
20. Wired, “NSA Hacker Chief Explains How to Keep Him Out of Your System” (28 January 2016), available at https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/; see also: Enigma, “Disrupting Nation State Hackers” (27 January 2016), available at https://www.usenix.org/node/194636. [↑](#footnote-ref-20)
21. Wired, “Everything We Know About How the FBI Hacks People” (16 May 2016), available at https://www.wired.com/2016/05/history-fbis-hacking/; see also: Federal Bureau of Investigation, “Operational Technology Division” (undated), available at https://www2.fbi.gov/hq/otd/otd.htm. [↑](#footnote-ref-21)
22. Newsweek, “Russia’s Greatest Weapon may be its Hackers” (7 May 2015), available at http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html. [↑](#footnote-ref-22)
23. Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units” (2013), available at https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. [↑](#footnote-ref-23)
24. The Guardian, “Russia Accused of Unleashing Cyberwar to Disable Estonia”

(16 May 2007), available at https://www.theguardian.com/world/2007/may/17/topstories3.russia. [↑](#footnote-ref-24)
25. Parliament of Australia, “Australian Security Intelligence Organisation Legislation Amendment Act 1999 (No. 161)” (1999), available at http://www.austlii.edu.au/au/legis/cth/num\_act/asiolaa1999664/sch1.html, amending: Parliament of Australia, “Australian Security Intelligence Organisation Act § 25A”, (1979), available at http://www.austlii.edu.au/au/legis/cth/consol\_act/asioa1979472/s25a.html. [↑](#footnote-ref-25)
26. Parliament of Australia, “National Security Legislation Amendment Bill (No. 1)” (2014), available at http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query%3DId%3A%22legislation%2Fbillhome%2Fs969%22;rec=0; see also: ABC News, “Five Questions About Our New National Security Laws” (1 October 2014), available at http://www.abc.net.au/news/2014-10-01/bradley-five-national-security-questions/5783142. [↑](#footnote-ref-26)
27. PhysOrg, “Australia Admits Government Hack Attacks, Boosts Cyber Security” (21 April 2016), available at http://phys.org/news/2016-04-australia-hack-boosts-cyber.html. [↑](#footnote-ref-27)
28. Security Affairs, “Trojan & Co, the New Frontiers of Espionage” (13 November 2011), available at http://securityaffairs.co/wordpress/166/cyber-crime/trojan-co-the-new-frontiers-of-espionage.html. [↑](#footnote-ref-28)
29. Ibid. [↑](#footnote-ref-29)
30. Access Now, “Joint Representations by Access, the Center for Democracy & Technology, the Electronic Frontier Foundation, and New America’s Open Technology Institute on ‘Interception of communications and equipment interference: draft codes of practice’” (20 March 2015), available at <https://www.accessnow.org/cms/assets/uploads/archive/Joint%20GCHQ%20Representation.pdf>; see also: United Kingdom Home Office, “Equipment Interference Code of Practice: Draft for public consultation” (February 2015), available at https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/401863/Draft\_Equipment\_Interference\_Code\_of\_Practice.pdf; United Kingdom Home Office, “Equipment Interference Code of Practice” (January 2016), available at https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/496069/53693\_CoP\_Equipment\_Interference\_Accessible.pdf. [↑](#footnote-ref-30)
31. Wired, “Anonymous and LulzSec Targeted by GCHQ DDoS Attacks”, (5 February 2014), available at [http://www.wired.co.uk/news/archive/2014-02/05/gchq-ddos-attack-anonymous.](http://www.wired.co.uk/news/archive/2014-02/05/gchq-ddos-attack-anonymous) [↑](#footnote-ref-31)
32. Propublica, “ISIS via WhatsApp: ‘Blow Yourself Up, O Lion’” (11 July 2016), available at https://www.propublica.org/article/isis-via-whatsapp-blow-yourself-up-o-lion. [↑](#footnote-ref-32)
33. Republic of France, “Loi n 2016-731: Law strengthening the fight against organised crime, terrorism and their financing, and improving the efficiency and guarantees of criminal procedure” (3 June 2016), available at https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=FE4569C44829C0F79D4BF17709AAA7EF.tpdila18v\_1?cidTexte=JORFTEXT000032627231&categorieLien=id. [↑](#footnote-ref-33)
34. PCWorld, “Former hacking team developer reportedly in contact with a terrorist group”, (31 July 2015), available at http://www.pcworld.com/article/2955592/former-hacking-team-developer-reportedly-in-contact-with-a-terrorist-group.html. [↑](#footnote-ref-34)
35. See: The Citizen Lab, “Hacking Team and the Targeting of Ethipian Journalists” (12 February 2014), available at https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/. [↑](#footnote-ref-35)
36. Wired, “Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains” (7 November 2014), available at https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/. [↑](#footnote-ref-36)
37. Spiegel Online, “The Digital Arms Race: NSA Preps America for Future Battle” (17 January 2015), available at http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html. [↑](#footnote-ref-37)
38. The White House, “Heartbleed: Understanding When We Disclose Cyber Vulnerabilities” (28 April 2014), available at http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities. [↑](#footnote-ref-38)
39. Vulnerabilities Equities Process, *supra* fn. 4; see also: Electronic Frontier Foundation, “Complaint for Injunctive Relief for Violation of the Freedom of Information Act, 5 U.S.C. § 552 in Electronic Frontier Foundation v. National Security Agency, Office of the Director of National Intelligence” (1 July 2014), available at https://www.eff.org/document/eff-v-nsa-odni-complaint. [↑](#footnote-ref-39)
40. The Verge, “The FBI Bought an iPhone Hack, But Not the Right to Tell Anyone How it Works” (27 April 2016), available at http://www.theverge.com/2016/4/27/11518754/fbi-apple-iphone-hack-vulnerability-disclosure-vep. [↑](#footnote-ref-40)
41. See: The Washington Post, “Comey Defends FBI’s Purchase of iPhone Hacking Tool” (11 May 2016), available at https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a\_story.html. [↑](#footnote-ref-41)
42. Ars Technica, “The First Rule of Zero-Days is No One Talks About Zero-Days (So We’ll Explain)” (20 October 2015), available at <http://arstechnica.com/security/2015/10/the-rise-of-the-zero-day-market/>; National Telecommunications & Information Administration, “Multistakeholder Process: Cybersecurity Vulnerabilities” (8 April 2016), available at <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>; Motherboard, ”As Hackers Continue to Target Porn Sites, Pornhub Launches Bug Bounty Program” (10 May 2016), available at https://motherboard.vice.com/read/pornhub-bug-bounty. [↑](#footnote-ref-42)
43. Parliament of the United Kingdom, ”Written Evidence Submitted by Access Now: Investigatory Powers Bill” (28 April 2016), available at http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm (last visited July 29, 2016). [↑](#footnote-ref-43)
44. Slate, “This Arcane Rule Change Would Give U.S. Law Enforcement New Power to Hack People Worldwide” (11 May 2016), available at http://www.slate.com/blogs/future\_tense/2016/05/11/the\_rule\_41\_change\_would\_give\_u\_s\_law\_enforcement\_power\_to\_hack\_people\_worldwide.html. [↑](#footnote-ref-44)
45. TechDirt, “Kazakhstan Decides to Break the Internet, Wage All Out War on Encryption” (9 December 2015), available at https://www.techdirt.com/articles/20151204/07412332986/kazakhstan-decides-to-break-internet-wage-all-out-war-encryption.shtml. [↑](#footnote-ref-45)
46. Ars Technica, “Massive Leak Reveals Hacking Team’s Most Private Moments in Messy Detail” (6 July 2015), available at http://arstechnica.com/security/2015/07/massive-leak-reveals-hacking-teams-most-private-moments-in-messy-detail/. [↑](#footnote-ref-46)
47. Parliament of United Kingdom, “Investigatory Powers Act 2016 § 253” (29 November 2016), available at http://services.parliament.uk/bills/2015-16/investigatorypowers.html. [↑](#footnote-ref-47)
48. Parliament of United Kingdom, “Investigatory Powers Act 2016, § 253(5)(c) and § 253(5)(e)” (29 November 2016), available at http://services.parliament.uk/bills/2015-16/investigatorypowers.html. [↑](#footnote-ref-48)
49. National Assembly of Pakistan, “Prevention of Electronic Crimes Act, § 35(f)” (11 August 2016), available at http://www.na.gov.pk/uploads/documents/1472635250\_246.pdf. [↑](#footnote-ref-49)
50. Republic of South Africa, “Cybercrimes and Cybersecurity Bill, § 33” (2015), available at http://www.justice.gov.za/legislation/invitations/cybercrimesbill2015.pdf. [↑](#footnote-ref-50)
51. European Commission, Commission proposes to modernise and strengthen controls on exports of dual use items” (28 September 2016), available at http://europa.eu/rapid/press-release\_IP-16-3190\_en.htm. [↑](#footnote-ref-51)
52. For more information, see: Access Now, “Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies” (undated), available at https://www.accessnow.org/cms/assets/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf. [↑](#footnote-ref-52)
53. Schneier on Security, “D-Link Router Backdoor” (18 October 2013), available at https://www.schneier.com/blog/archives/2013/10/d-link\_router\_b.html. [↑](#footnote-ref-53)
54. European Parliament and Council, “Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union” (6 July 2016), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. [↑](#footnote-ref-54)
55. See: Access Now, “Transparency Reporting Index” (undated), available at https://www.accessnow.org/transparency-reporting-index. [↑](#footnote-ref-55)
56. For more information, see: Access Now, “Don’t take their word for it: scrutinizing government transparency reports”, available at https://www.accessnow.org/dont-take-word-scrutinizing-government-transparency-reports. [↑](#footnote-ref-56)
57. See: Freedom of the Press Foundation, “Brief for Amicus Curiae in support of the Plaintiff’s opposition to defendant’s partial motion to dismiss” (17 February 2015), available at http://www.clearinghouse.net/chDocs/public/NS-CA-0013-0003.pdf. [↑](#footnote-ref-57)
58. See: Access Now, “Spotlighting Surveillance: where states can lead on transparency reporting” (17 September 2014), available at https://www.accessnow.org/spotlight-on-transparency-where-states-can-lead-on-transparency-reporting. [↑](#footnote-ref-58)
59. European Parliament and Council, “Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)” (12 July 2002), available at

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML. [↑](#footnote-ref-59)
60. For more information, see: EDRi, “Proceed with Caution: Flexibility in the General Data Protection Regulation” (undated), available at https://edri.org/files/GDPR\_analysis/EDRi\_analysis\_gdpr\_flexibilities.pdf. [↑](#footnote-ref-60)
61. European Commission, “Commission implementing decision (EU) 2016/1250 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield” (12 July 2016), available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN. [↑](#footnote-ref-61)
62. European Commission, “Annex III: EU-US Privacy Shield Ombudsperson mechanism regarding signals intelligence” (22 February 2016), available at http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3\_en.pdf. [↑](#footnote-ref-62)
63. See: Office of the Director of National Intelligence, “Intelligence Community” (undated), available at https://www.dni.gov/index.php. [↑](#footnote-ref-63)
64. United States Congress, “Judicial Redress Act of 2015” (24 February 2016), available at https://www.congress.gov/bill/114th-congress/house-bill/1428. [↑](#footnote-ref-64)
65. United States Department of Justice, “Privacy Act of 1974” (17 July 2015), available at https://www.justice.gov/opcl/privacy-act-1974. [↑](#footnote-ref-65)
66. United States Department of Justice, “Overview of the Privacy Act of 1974: Ten Exemptions” (16 July 2015), available at https://www.justice.gov/opcl/ten-exemptions. [↑](#footnote-ref-66)
67. Journal of Telecommunications and High Technology Law, “Network Neutrality, Broadband Discrimination” (2003), available at http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=388863. [↑](#footnote-ref-67)
68. Ars Technica, “Sprint now zero-rating some video, joining AT&T, Verizon, and T-Mobile” (23 May 2016), available at http://arstechnica.com/business/2016/05/sprint-now-zero-rating-some-video-joining-att-verizon-and-t-mobile/. [↑](#footnote-ref-68)
69. Internet.org by Facebook, “Where we’ve launched” (undated), available at https://info.internet.org/en/story/where-weve-launched/. [↑](#footnote-ref-69)
70. Telecoms Regulatory Authority of India, “Prohibition of discriminatory tariffs for data services regulations (No.2 of 2016)” (8 February 2016), available at http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation\_Data\_Service.pdf. [↑](#footnote-ref-70)
71. United States Federal Communications Commission, “Protecting and Promoting the Open Internet” (12 March 2015), available at https://apps.fcc.gov/edocs\_public/attachmatch/FCC-15-24A1.pdf.. [↑](#footnote-ref-71)
72. Body of European Regulators of Electronic Communications (BEREC), “BEREC Guidelines on implementation by National Regulators of European net neutrality Rules” (30 August 2016), available at http://berec.europa.eu/eng/document\_register/subject\_matter/berec/regulatory\_best\_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules. [↑](#footnote-ref-72)
73. Office of the High Commissioner for Human Rights, “Questionnaire for Business Enterprises” (August 2016), available at http://www.ohchr.org/Documents/Issues/Expression/Telecommunications/QuestionnaireBusinessEnterprises.docx. [↑](#footnote-ref-73)
74. Access Now, “Telco Action Plan: Respecting Human Rights: Ten Steps and Implementation Objectives for Telecommunications Companies” (March 2012), available at https://www.accessnow.org/cms/assets/uploads/archive/docs/Telco\_Action\_Plan.pdf. [↑](#footnote-ref-74)
75. Access Now & ShareAction, “Investor Briefing: Internet shutdowns: The risks and opportunities for technology sector investors” (September 2016), available at https://shareaction.org/wp-content/uploads/2016/08/InvestorBriefing-InternetShutdowns.pdf. [↑](#footnote-ref-75)
76. Access Now, “Commonwealth of Surveillance States: on the export and resale of Russian surveillance technology to post-Soviet Central Asia” (undated), available at https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046\_8sm6ivg69.pdf. [↑](#footnote-ref-76)
77. Access Now, “Commonwealth of Surveillance States: the dangers of Russian made surveillance technology” (29 June 2013), available at https://www.accessnow.org/commonwealth-of-surveillance-states-the-dangers-of-russian-made-surveillanc/. [↑](#footnote-ref-77)
78. European Court of Justice, “Opinion of the Advocate General in Joined cases C-203/15 and C-698/15” (19 July 2016), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=112824. [↑](#footnote-ref-78)
79. European Court of Justice, “Opinion of the Advocate General in Joined cases C-203/15 and C-698/15” (19 July 2016), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=112824. [↑](#footnote-ref-79)
80. Business & Human Rights Resource Centre, “Access Now sends digital rights demands to tech and telco firms” (15 April 2016), available at https://business-humanrights.org/en/access-now-sends-digital-rights-demands-to-tech-and-telco-firms. [↑](#footnote-ref-80)
81. Federal Communications Commission, "In the Matter of Cellco Partnership, d/b/a Verizon Wireless," Order by Chief, Enforcement Bureau, adopted March 7, 2016. File No.: EB-TCD-14-00017601. [↑](#footnote-ref-81)
82. See Access Now report, “The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy,” (August 2015) at https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf; see also AmIBeingTracked at http://amibeingtracked.com for more information on the Access Now campaign against supercookies. [↑](#footnote-ref-82)
83. Access Now, “Forgotten Pillar: The Telco Remedy Plan” (May 2013), available at https://www.accessnow.org/cms/assets/uploads/archive/docs/Telco\_Remedy\_Plan.pdf. [↑](#footnote-ref-83)
84. Access Now, “One of these things is not like the other: report on fake domains attacks on civil society released” (1 August 2013), available at https://www.accessnow.org/one-of-these-things-is-not-like-the-other-report-on-fake-domains-attacks-on/. [↑](#footnote-ref-84)