The Internet and extra-territorial effects of laws

Internet Society Concept Note

September 2018

How to avoid rule-setting and decision-making that will constrain the Internet around the world

The Internet is global, so regulations and court decisions that affect it may have extra-territorial[1] effects. This raises two questions: How mindful are states about avoiding harmful and unnecessary impacts outside their borders, and how can they minimize such negative effects?

The Internet is a network of networks consisting mostly of privately-operated networks; some of those networks cross national boundaries, and many of the organizations themselves cross boundaries, too (for example, international corporations). The value of the Internet comes from its open and global nature. Globalization is a feature of the Internet, not a bug, and legal systems everywhere should recognize this, not try to 'fix' it. Decisions that exert jurisdiction extra-territorially should be made in ways that allow the Internet to evolve as an open, globally-connected, secure and trustworthy technology for everyone.

This Concept Note sets out problems that occur when states exert extra-territorial jurisdiction – i.e. when they make policy or judicial decisions with effect outside the country's territory, either by accident or design. We suggest an approach to avoid or minimize judicial or regulatory decisions that can harm the Internet's global reach and unique characteristics. But, fundamentally, states should not impede the flow of ideas and information the Internet brings, especially to their own citizens.

Executive Summary

- The social and economic progress the Internet brings globally is based on its fundamental properties of openness, innovation, permission-less innovation, interoperability, collaboration and competition (the "Internet Invariants")[2]. If we undermine these properties, we risk all the benefits the Internet brings.
- Right now, decision-makers in many states are imposing rules that spill over onto the Internet elsewhere, hamper innovation, deter investment in their own countries and risk making their people into 'second class citizens' on the Internet.

- Decision-makers can mitigate these problems by encouraging decentralized collaborative approaches, including international norms development processes, to shape Internet-related laws and policies. Such processes and structures can create better outcomes because they have broader participation and are more politically responsive and economically sustainable than some top-down approaches.[3]
- These primary principles will help guide decision-makers and mitigate unintentional extraterritorial harms:

    - **First, do no harm.**
    - **Check what's been done before.**
    - **Collaborate with other stakeholders**
    - **Focus on the activity/behaviour, not the medium**
    - **Be mindful of the properties of the Internet and what they stand for.**

Background

Many national laws are intended to have extra-territorial effect; they apply to people or companies outside the borders of the state that made the laws. This practice long pre-dates the Internet, but its effects are exacerbated both by the cross-border nature of the networks and also the drive by some countries to exert authority over the Internet. Examples include:

- Non-US companies have long been targeted by American laws, including the 1996 Helms Burton Act,[4] on bribery or sanctions relating to third countries.
- EU data protection regulations like the General Data Protection Regulation (GDPR) apply to companies from outside the EU that use the personal data of European citizens.
- Changes made in 2011 to the Criminal Law of the People's Republic of China now include people or companies neither from nor in China who may be guilty of corruption against the Chinese state or its citizens.

Intentional extra-territorial effects of laws aim to ensure that people do not become victims of law-breakers from outside their jurisdictions. While governments have a responsibility to protect their citizens from illegality, the Internet's cross-border nature can create conflicts arising from activities that are legal in one country being illegal in another. In the early 2000s, as the Internet became popular and commercialized, the Yahoo! case highlighted the challenges of Internet regulation. The American search and listings company, Yahoo!, was forced to stop advertising Nazi memorabilia for sale in France, and its executives faced criminal charges[5].

However, many Internet-related laws and international frameworks only regulated where absolutely necessary to promote commerce, and promoted openness and innovation in the development of the networks. For example, the idea of 'mere conduit' - where network operators are not liable for the content of traffic – is found in many laws, including the European E-Commerce Directive of 2000.[6] Governments took a light regulatory touch domestically and coordinated regionally and internationally to allow the Internet to flourish.[7]

Today, government and citizen concerns about privacy, cybersecurity, taxation, competition and electoral integrity have launched a new wave of extra-territorial effects both in regulations and court decisions. Examples include:

- In 2014, a Spanish court created a Europe-wide *Right to Be Forgotten* in Google's search-engine results.[8]
- In 2017, the Supreme Court of Canada upheld orders for Google to "de-index" a website, and asserted the jurisdiction of Canada's courts over Internet intermediaries in other countries. However, the Court provided no insight about how this could be enforced, causing uncertainty and confusion.[9]
- In 2017, a US court ordered the blocking of the academic resource, sci-hub, by a broad range of ISPs and search engines, in addition to the seizure of its domain names (a more typical response to alleged intellectual property rights infringement).[10]
- The European Union's General Data Protection Regulation (GDPR)[11] is explicitly designed to protect European users' personal data, whatever jurisdiction it is processed in.
- The US CLOUD Act coordinated the interests of law enforcement and US tech firms to ensure access to data internationally but has been criticised for minimising other stakeholder interests.
- China is taking steps to increase the extra-territorial reach of its content monitoring and filtering regime.[12]
- The UK and some Middle Eastern countries seem to be moving away from a 'notice and takedown' approach to illegal or unwanted content, and towards a positive obligation for technology platforms to police existing content or even prevent it from being uploaded.[13]

Because of the Internet, decision-making with extra-territorial effect is intensifying, and risks undermining what made the Internet such a powerful and positive force.

What makes the Internet so powerful: The "Internet Invariants"

The Internet has fundamental properties that have made it a global enabler of social and economic progress. We call these properties the *Internet Invariants*[14], because while applications *on* the Internet often change, the underlying source of the Internet's strength does not vary. The sum of these invariants ensures the Internet is an open platform for innovation and creativity.

Supporting the ***Internet Invariants*** will ensure the next generation of innovations develop and that everyone has a chance to enjoy their benefits and rewards:

Global reach and integrity: An 'end to end' Internet where information sent from any point can get to any other.

General purpose: The Internet is not designed for specific purposes or business models, but for general use. There are no built-in limitations on the applications or services that use it.

Permission-less innovation: Anyone can set up a new service on the Internet without having to ask permission, as long as it meets existing technical standards and best practices.[15]

Accessibility: Anyone can use the Internet, not just to consume but to contribute content, put up a server and attach new networks.

Interoperability and mutual agreement: Through open technology standards and mutual agreements between operators of different parts of the Internet.

Collaboration: The best solutions to new issues come from the willing collaboration between stakeholders.

Reusable building blocks: Technologies are often deployed on the Internet for one purpose, only to be used later to do something else. This creativity and problem-solving would be impossible with vertically integrated, closed solutions.

No permanent favourites: Success depends on relevance and utility, not on special status. It must not be 'locked in' by today's winners. Openness and innovation are the life-blood of the Internet.

How might the extra-territorial effects of some national rules and court decisions challenge the premise of the Internet Invariants?

Why extra-territorial jurisdiction can be a problem?

National laws and judicial decisions that exert extra-territorial jurisdiction can have negative and often unintended consequences. For the sake of analogy, let's call them the "extra-territoriality Internet symptoms":

- **Unpredictability** – The unpredictability of how domestic laws might apply and be enforced can stifle innovation because it creates greater risk and uncertainty for new product and services.
- **Inconsistency** – As different organizations try to implement decisions and rules, there can be variance in how rules are implemented. With a proliferation of rules and complexity, only the largest organizations may be able to comply.
- **Power-grabs** – Some states are trying to grab back power over the Internet, and from other countries, seeing it as a threat to their authority. This can intensify the conflict of laws as each country or court races to come out on top, and can even create a wider sense of uncertainty and resentment of interference from abroad. The resulting confusion to users could reduce their trust in the Internet.
- **Uncoordinated action** – Unilateral regulatory actions at a national level displace and undermine collaborative ways of examining issues and impede the development of international norms. While increasing friction between both networks and nation-states, they produce outcomes restricted to the social and economic sensitivities of one jurisdiction or even just one set of stakeholders.
- **Fragmentation** – Applications running in the Internet start to behave differently in different countries,[16] or content is unavailable. The result is an increasing degree of Internet fragmentation, making certain people 'second class citizens', and concentrating the benefits of innovation in some countries, as products and services from abroad are barred or dissuaded from entering their market.

Negative externalities of extra-territorial jurisdiction

A negative externality is when the *benefit* of doing something is enjoyed by some people or organizations, but the *costs* are largely borne by others. A classic example is airborne pollution created in one country that poisons rivers and forests in another. Jurisdictional extra-territoriality can create negative externalities on the networks - by undermining the Internet Invariants - and more broadly on governance and participation in the digital economy.

A. Externalities on the Internet Invariants")

Internet Invariants	Externalities of Extra-Territorial Jurisdiction
Global reach and integrity*:* An 'end to end' Internet where information sent from any point can get to any other in any network around the world. **Accessibility**: Anyone can use the Internet, not just to consume but to contribute content, put up a server and attach new networks.	**Internet fragmentation**: negates and challenges the global reach and integrity of the Internet; creates 'second class citizens' where access to information and communication tools is uneven.
General purpose: The Internet is not designed for specific purposes or business models, but for general use. **Reusable building blocks**: Technologies may be deployed for one purpose, but used later or by others to do something new. **No permanent favourites**: Success depends on relevance and utility, not on special status. It must not be 'locked in' by today's winners. **Permission-less innovation**: Anyone can set up a new service on the Internet without having to ask permission, as long as it meets existing technical standards and best practices.	**Inconsistency** - Different stakeholders try to enact decisions and complicated rules that are often not easily enforceable. With a proliferation of rules and complexity, the largest organizations can most easily comply, creating competition issues for smaller firms and even a **new digital divide** between large and established companies, and smaller, potentially more innovative ones. Vertically integrated solutions driven by the legal and cultural backgrounds of the biggest players and countries are favoured, instead of open, reusable technologies that can be repurposed by new players. Instead of being distributed around the world, the benefits of the Internet are increasingly concentrated in the countries with the most international influence and the companies with the resources to comply, turning certain companies into *permanent favourites*.
Interoperability and mutual agreement: through open technology standards and mutual agreements between operators of different parts of the Internet. **Collaboration**: The best solutions to new issues come from willing collaboration between stakeholders.	**Power-grabs** – States try to grab or reassert power at the international stage, as each races to come out on top, imposing unilateral interests in a top-down, closed way. This intensifies both jurisdictional conflicts and friction between networks. **Uncoordinated action** - Unilateral top-down actions displace and undermine collaborative ways of examining issues. They can negatively affect the development of the network. Because the Internet is a network of networks, if changes are imposed on different networks there is a risk that those networks stop working together. This pulls stakeholders apart instead of bringing them together, resulting in a 'zero-sum game' world where everyone is a loser.

B. Broader externalities

These concern a range of political and economic externalities that affect both governance and how people participate in the digital economy:

- **Fragmentation**: As well as creating a fragmented Internet, extra-territorial jurisdiction drives both governmental and commercial fragmentation,[17] leading to narrow and reduced offerings across various countries.
- **Business model disruption** as businesses try to cope with the compliance burden of possibly conflicting laws. This creates added uncertainty for companies operating globally and weakens the framework of international trade and investment. It can also drive consolidation and competition issues if only the biggest and best-resourced companies can cope with the legal complexity and business risk of compliance.
- The creation of **second class citizens** suffering from new digital divides. As technology advances in certain parts of the world, many countries consider regulation as a means to 'catch up' with such progress. Such regulation risks being narrow in scope and reflecting cultural, economic and social sensitivities incompatible with those in other countries. This limits the range of information and services available, creating new digital divides for users in different countries.
- **International tension** and resentment generated by states imposing their will in other countries. When one state actor is seen as aggressively using domestic law to assert its hegemony globally, we can expect others to react accordingly[18]. Additionally, extraterritoriality undermines international collaboration by diverting attention and resources from developing collaborative frameworks and international norms. Extraterritoriality creates a patchwork of inconsistent rules as different institutions in different countries approach international issues using different laws and procedures.

Principles for dealing with Internet-related decisions and regulation

We are just beginning the conversation on regulation. Some regulators and judges may be dealing with these topics for the first time. These preliminary principles are intended to help decision-makers to achieve their goals while ensuring the Internet still drives social empowerment and economic growth, both at home and abroad:

1. **Weigh Risks and Benefits.**
    - The most limited and targeted decisions will create the least unintended negative consequences. Does the decision *have* to have extra-territorial effect for it to work?
    - Actively consider the role and impact of decisions on other stakeholders, including in other countries.
2. **Check what's been done before.**
    - It's likely other governments or courts have pondered the same challenging questions, Resources to check how others have approached issues may be available from international or regional organizations[19], including regulatory best practices, norms and even suggested legal frameworks.
3. **Be mindful of the properties of the Internet.**
    - The Internet's unique properties – the "Internet Invariants" - can provide an additional benchmark in determining the effectiveness of regulation. We encourage policy makers to add them as evaluators for sound decision making.

4. **Focus on the activity/behaviour, not the medium.**
    - Design laws, rules and decisions to deal with the undesirable or illegal activity or behaviour itself, rather than the medium it occurs in. For example, is fraud that occurs online – e.g. phishing - substantively different from offline fraud? While the Internet adds new dimensions or can change the scale or reach of an activity, it doesn't always require rule-making targeted at the Internet itself.

5. **Seek out collaborations with other stakeholders**
    - Actively seek out opportunities to resolve issues with all relevant stakeholders, including at the regional and international level where cooperation and collaboration on norms can be highly effective.

6. **Apply the principle of proportionality**
    - Has the regulatory measure gone beyond what is required to attain a legitimate goal? Do its claimed benefits exceed the costs?

There is much work to do so the traditional nation-state approach to regulation and the global Internet can continue to evolve. These principles are a starting point. There is a need to both acknowledge and resolve some of the differences identified in the legal systems around the world, and to ensure the Internet remains a source of opportunity and a force for good.

---

1 We recognize that extra-territoriality involves different layers of interpretation and application. However, for the purposes of this concept note, it will refer to the legal ability of a state actor to exercise authority beyond its borders. It does not include Terms of Services imposed by private companies on individual users around the world.

2 "Internet invariants" refers to the fundamental properties that make the Internet unique. They are inherent in the original design of the Internet and, if altered or significantly weakened, would undermine the Internet's open and generative nature. https://www.internetsociety.org/internet-invariants-what-really-matters/

3 https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

4 https://en.wikipedia.org/wiki/Helms%E2%80%93Burton_Act

5 Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1186 (N.D. Cal. 2001)

6 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

7 A similar principle is found in section 512 of the US Digital Millennium Copyright Act (DMCA)

8 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)

9 https://www.osler.com/en/resources/regulations/2017/supreme-court-of-canada-upholds-global-search-engi

10 https://torrentfreak.com/sci-hub-loses-domain-names-but-remains-resilient-171122/

11 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

12 https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

13 https://arstechnica.com/tech-policy/2016/05/uk-ip-enforcement-2020-notice-trackdown-teach-kids/

14 https://www.internetsociety.org/internet-invariants-what-really-matters/

15 The best example of permission-less innovation is the World Wide Web, created by Sir Tim Berners-Lee in Switzerland who made his technology available to everyone.

16 https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542

17 Internet Fragmentation: An Overview, World Economic Forum, http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

18 There is precedent: Kenneth W. Dam, *Extraterritoriality in an Age of Globalization: The Hartford Fire Case*, 1993 SUP. CT. REV. 289, 324; *see also* Thabo Mbeki, Presi- dent of South Africa, Statement to the National Houses of Parliament and the Nation at the Tabling of the Report of the Truth and Reconciliation Commis- sion (Apr. 15, 2003), http://www.anc.org.za/ancdocs/history/mbeki/2003/ tm0415.html ("[W]e consider it completely unacceptable that matters that are central to the future of our country should be adjudicated in foreign courts which bear no responsibility for the well-being of our country.").

ANNEX

Disclaimer: The following is a non-exhaustive list of national laws, dedicated to dealing with Internet issues, that have an extraterritorial effect. The list intentionally excludes some facets of legislation, e.g. tax laws, where, in most cases, extraterritoriality is ingrained in their original design.

Africa				
Country	**Statue Name**	**Year of Adoption**	**Category**	**Description of Extraterritorial Effect**
Kenya	Computer and Cybercrimes Bill	2018	Cybersecurity, Freedom of Expression	This bill introduces 17 offences intended to prevent and control cybercrime, including imposing penalties on individuals circulating "false, misleading or fictitious data," whom share pornographic content, or whom engage in cyber terrorism. Extraterritorial effect: the bill has a broad scope and Section 42 (2) makes it clear that this law applies outside of Kenya if an offence is committed by a Kenyan citizen or someone ordinarily resident in Kenya.
South Africa	Cybercrime and Cybersecurity Bill	2017	Cybersecurity	This legislation criminalises cyber-facilitated offences of fraud, forgery, and extortion. Extraterritorial effect: South Africa's jurisdiction will be expanded to "all offenses which can be committed in cyberspace … to deal with cybercrime which originates from outside our borders" (*extraterritoriality by design*).
	Electronic Communications and Transactions Act	2002	E-Services, Security	This law seeks to enable and facilitate electronic communications and transactions. It also introduced requirements for government agencies to roll out e-services, and criminalises certain cybercrimes like hacking, phishing, and intercepting or interfering with data. Extraterritorial effect: Section 90 of the law states that a court in South Africa has jurisdiction where "the offence has had an effect in the Republic [of South Africa]."
Tanzania	Electronic and Postal Communications (Online Content) Regulations	2018	Media Regulation, National Security	This law introduces a requirement for all blogs that contain information about the Tanzanian government to hold a license to do so. Permits can subsequently be revoked if a website publishes content that "causes annoyance, threatens harm or evil, encourages or incites crimes" or jeopardizes "national security or public health and safety." Bloggers must also remove "prohibited content"

				within 12 hours or face fines of not less than five million Tanzanian shillings or a year in prison. Extraterritorial effect: any blog posting information about Tanzania, regardless of where it is hosted in the world or the nationality of the author or publisher, is prior to publication required to obtain a license from the Tanzanian government.
Uganda	Over the Top Services Tax	2018	Internet Freedom	Uganda has imposed a levy of 200 Ugandan shillings per day on citizens who use social media platforms like Facebook, Skype, Twitter, and WhatsApp. Extraterritorial effect: the law applies to all Ugandan citizens, everywhere in the world (at present it is only being implemented on a national level, with the country's major telecom companies developing special mobile money menus through which users can pay the tax.) Note: this law is still alive as of the date of publication: http://www.theeastafrican.co.ke/business/Ugandans-raise-volume-on-social-media-tax-protests/2560-4680280-i4ipp0/index.html
Zambia	Cybersecurity & Cybercrimes Bill	2018	Cybersecurity	The bill was adopted to "promote an increased cybersecurity posture, facilitate intelligence gathering, investigation, prosecution and judicial processes in respect of preventing and addressing cybercrimes, cyber terrorism and cyber warfare." Extraterritorial effect: Part XI of the law is extraterritorial, noting that it applies to "any person, irrespective of the nationality or citizenship of the person" who engages in a cybercrime, "directed against equipment, software, or data located in Zambia regardless of the location of the person."
Asia-Pacific				
Country	Statue Name	Year of Adoption	Category	Description of Extraterritorial Effect
Australia	Interactive Gambling Amendment Bill	2017	Gambling	This law requires any website which provides or advertises online gambling services, regardless of whether or not the vendor has assets in Australia, to obtain a license from a designated agency if it makes its services available to Australian users. Extraterritorial effect: the law states "this Act extends to acts, omissions, matters and things

				outside Australia" for the purposes of applying civil non-compliance provisions.
	Privacy Enhancement (Enhancing Privacy Protection) Act	2014	Data Protection	This law introduces a set of privacy principles that are intended to see personal data be handled and stored in a more secure manner throughout its lifecycle. Extraterritorial effect: an organization "carrying on business" in Australia must comply with this law even if domiciled in a foreign jurisdiction. This will necessarily include foreign organizations with an online presence, even if that entity has no physical presence in Australia, if it has customers located in Australia.
	Spam Act	2013	Advertising	This law regulates the distribution of unsolicited electronic communications. Extraterritorial effect: Section 14 of the Act applies where an Australian computer network has received a spam message.
	Therapeutic Goods Advertising Code	2018	Advertising	This regulation introduces new required warning statements that must be displayed or communicated to consumers before medicines can be sold, and clarifies that no advertisement may target a person under 12 years of age. Extraterritorial effect: Section 6 states that the law applies "in Australia and a place outside Australia," if it involves "the promotion of therapeutic goods online" by either an Australian business targeting consumers abroad, or a foreign business targeting Australian consumers.
China	Anti-Terrorism Law	2015	National Security	This law requires both Chinese and foreign technology companies to create 'cyber police stations' which provide Chinese law enforcement with surveillance access to any and all data concerning Chinese users. ISPs and platforms are also obliged to block terrorism-related content if asked to do so by designated law enforcement. Extraterritorial effect: the law applies to any data concerning a Chinese national, regardless of where in the world he or she may live.
	Cybersecurity Law	2017	National Security	This law applies to all enterprises that employ networks or information systems in their operations and sets forth significant cybersecurity obligations.

				It also introduces penalties for individuals and entities who commit cybercrimes. Extraterritorial effect: Article 75 makes it an offense for anyone "outside of China" to cause damage to the critical information infrastructure of China. In the case of a breach of this provision, the law empowers Chinese authorities to freeze the property of or take "any other necessary sanction" against the offender.
India	Information Technology Act	2000	Cybersecurity	This law criminalises the failure to assist law enforcement in decrypting information; gaining unauthorised access into a private computer system; publishing obscene information; disseminating child pornography; and other cybercrimes. Extraterritorial effect: the law "confers extraterritorial jurisdiction on Indian courts and empowers them to take cognisance of offences committed outside India even by foreign nationals provided that such offence involves a computer, computer system, or computer network located in India."
	Copyright Act	2012	Intellectual Property	This statute provides moral rights, neighbouring rights, and transferrable economic rights to the creators of literary, dramatic, musical, and artistic works and the producers of films and sound recordings. Extraterritorial effect: this law states that Indian courts have jurisdiction to adjudicate upon disputes arising within the territories of India. As a result, a website based outside of India that facilitates the infringement of copyright by providing infringing copies of a work to users in India will confer jurisdiction on the courts in India to adjudicate the matter.
Indonesia	Law on Information and Electronic Transactions	2016	Cybersecurity, Freedom of Expression, Data Protection	Article 26 of the law introduces a right to be de-indexed, Article 40 enhances the government's ability to block or filter content to prevent the dissemination of illicit content, and other provisions seek to increase the privacy rights of Indonesians. Extraterritorial effect: the law imposes data processing obligations on any entity which handles the data of Indonesian citizens, including foreign owned and foreign operated platforms and services,

				though how enforceable this law is remains questionable.
	Regulation on Personal Data Protection in Information Systems	2016	Data Protection	This regulation introduces new rules on when personal information can be collected and processed, and administrative sanctions for the misuse of personal data. Extraterritorial effect: the regulation has a broad scope and applies to individuals and entities domiciled in Indonesia or overseas which are conducting actions that have a legal effect in Indonesia and/or which harm the interests of Indonesia.
Japan	Amended Act on the Protection of Personal Information	2017	Data Protection	This decade-old privacy law was amended to adapt to various changes in the information technology landscape. Extraterritorial effect: Article 75 of the law states that it is applicable to entities that are domiciled outside of Japan which obtain and/or process the personal information of Japanese residents. This extraterritorial effect was intentional, and while largely intended to reign in financial institutions, the language applies to all data controllers.
Malaysia	Anti-Fake News Act	2018	Freedom of Expression	The Act covers "news, information, data and reports which is or are wholly or partly false" and applies only to digital publications and social media platforms. Extraterritorial effect: the law applies to offenders outside of Malaysia, including foreigners, if Malaysia or a Malaysian citizen are affected.
	Sedition Bill	2015	Freedom of Expression	This existing law was amended in order to empower the Sessions Court of Malaysia to order the removal of "seditious publications" from the global Internet. Extraterritorial effect: a separate piece of legislation, the Extra-Territorial Offences Act, creates a schedule of Malaysian laws that may be enforced "beyond the limits of Malaysia." There are currently two items in its schedule; the Official Secrets Act, and the Sedition Bill.
New Zealand	Harmful Digital Communications Act	2015	Freedom of Expression	This law provides for fines, and potentially imprisonment, for people who post "harmful" speech online. Extraterritorial effect: the law creates criminal offences which are subject to the Crimes Act 1961. Section 7 of the Crimes Act provides for

				circumstances where prosecutions may happen extraterritorially. Where an offence is committed by someone who is either a New Zealand citizen or ordinarily resident in New Zealand, and they have targeted their harmful speech at a New Zealand citizen or resident, even if the act was committed outside of New Zealand, then there is the provision for extraterritorial enforcement.
Pakistan	Prevention of Electronic Crimes Bill	2016	Cybersecurity	This legislation is intended to combat terrorism, harassment, the sharing of child pornography, spamming, encryption, and other perceived forms of cybercrime. The law also grants Pakistani law enforcement agencies broad powers to access personal data and to remove content from social media platforms without judicial oversight. Extraterritorial effect: the bill specifically notes that it applies to all Pakistani citizens outside of the country's territory.
Philippines	Republic Act No. 10175 "Cybercrime Prevention Act"	2012	Cybersecurity	This law has a number of provisions regarding libel and improper online behaviour. Extraterritorial effect: the law assumes jurisdiction "over any violation of the provisions of this Act including any violation committed by a Filipino national regardless of the place of commission."
	Republic Act No. 10173 "Data Privacy Act"	2016	Data Protection	This law, passed in 2012 but only coming into effect in 2016, protects Filipinos from the unauthorized processing of their personal and/or identifiable information. Extraterritorial effect: Chapter 1, Section 6 of the law says it has extraterritorial application if a data controller enters into a contract in the Philippines. As an example, a foreign owned and operated website which allowed the registration of a data subject resident in the Philippines would be entering into a contract with them.
Singapore	Computer Misuse and Cybersecurity Act	2017	Cybersecurity, National Security, Data Protection	This law seeks to put an end to cybercrimes that cause, or could cause, "serious harm" to Singaporean computer networks. Extraterritorial effect: Section 11 of the law states, "the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore."

	Personal Data Protection Act	2012	Data Protection	This law sets forward a minimum set of protections and obligations that data controllers must provide Singaporean data subjects. Extraterritorial effect: the law casts a wide net and applies to any entity which holds or the processes the personal data of any living or deceased individual who is ordinarily resident in Singapore.
South Korea	Personal Information Protection Act	2011	Data Protection	This law regulates all sectors that collect and/or process personal information, with the exception of public institutions collecting information under the Statistics Act. Extraterritorial effect: the law's reach is not limited to local data processors and, accordingly, extraterritorial application is possible with respect to matters that affect South Korean data subjects.
Taiwan	Personal Information Protection Act	2012	Data Protection	This law brings to Taiwan a number of core data collection and processing principles that were contained within the European Union's 1995 data protection directive. It applies to both the public and private sectors and mandates data minimalization, fair and lawful processing, the deletion of unnecessary data, and special protections for sensitive data. Contraventions of the Act, where damage is caused to another person, can be punished by imprisonment up to two years or substantial fines. Extraterritorial effect: Article 51 of the law is explicitly extraterritorial, stating it "applies to [the] collection, processing, or use outside of the territory of the Republic of China by a public agency or non-public agency of personal data of nationals of the Republic of China."
Thailand	Computer-Related Crime Act	2016	Cybersecurity	This Act states that any person "who enter[s] into a computer system, publicise[s] or share[s] false information that "could" cause damage to [Thailand's] national security, public safety, economic security, public services and infrastructure or provoke public panic will be subject to five years' imprisonment." Extraterritorial effect: the Act applies to anyone who is engaging in such activities aimed at Thailand, a Thai citizen, or a Thai resident.
Turkey	Law on the Establishment	2018	Freedom of Expression	Turkey amended its existing radio and television legislation to empower the Radio and Television

	of Radio and Television Enterprises and Their Media Services			Supreme Council to monitor the Internet for radio, television, and on-demand broadcast content that has been uploaded by Turkish publishers. It does not apply to content uploaded by individuals on to social media. The law requires Turkish publishers to obtain a license from the Council, and empowers the Council to block access to content uploaded by 'illegal' publishers. Extraterritorial effect: the law applies to foreign media service providers and platform operators who are targeting audiences in Turkey, regardless of whether they provide their service and broadcasts in the Turkish language or have a local office.[18]
Vietnam	Cybersecurity Law	2018	Data Localisation, Data Protection, Freedom of Expression	This law imposes requirements on the processing of personal data that is captured in Vietnam. The law applies to all entities which offer services in Vietnam. Extraterritorial effect: the language of this law is broad and captures almost all varieties of online business activities. The scope is that it applies to any entity which, "provide[s] services on the telecommunication network, internet, and other value-added services on the internet in Vietnam."[18] If a foreign bank's website was accessed by a foreign national on vacation in Vietnam, for example, it would be captured by the language of this law, even if that seems highly unlikely to have been the law's intent, based upon public statements by Vietnamese lawmakers.
Europe				
Country	Statue Name	Year of Adoption	Category	Description of Extraterritorial Effect
European Union	Consumer Protection Regulation	2017	Freedom of Expression	This regulation gives consumer protection agencies within the European Union the authority to order ISPs, web hosts, and domain registries to block or delete websites without judicial oversight. Extraterritorial effect: websites that can be blocked or deleted are not limited to European ones, so it is in theory possible that a website not hosted in the EU could be permanently deleted at the request of a consumer protection agency.
	Directive on Attacks	2013	Cybersecurity	This directive criminalises "attacks on information systems" and introduces new criminal offences for

	Against Information Systems			obtaining illegal access to an information system and/or interfering with its systems and/or data. Extraterritorial effect: this directive says that a criminal act occurs where an offence against an information system occurs on its territory, irrespective of whether the offender is physically present or not in its territory or a national of the member state. However, where the offender is a national of the impacted member state, and committed the offence outside of the member state's territory, the directive has "extraterritorial jurisdiction based on the restrictive active nationality principle."
	General Data Protection Regulation	2014	Privacy	With a few exceptions, any organisation – no matter where in the world it is – that processes the personal data of persons ordinarily resident in the European Union will fall under the scope of the GDPR. Extraterritorial effect: the territorial scope of the GDPR is broad and explicit that it is intended to apply to data controllers outside of the EU.
	Privacy and Electronic Communications Directive	2002	Cybersecurity	This directive was intended to focus on the security of electronic communications and to eliminate spam, but has come to be known as the 'cookie law' for mandating that websites disclose if they place a cookie on a European user's hard drive. Extraterritorial effect: the directive is tied to the EU's Data Protection Directive 1995 (subsequently superseded by the GDPR) in that it requires that the personal data of EU residents can only be transferred to non-EU countries if that country has an adequate level of personal data protection. As a result, the directive extends to apply to organizations located outside of the EU that process electronic communications data in connection with providing electronic communication services to EU end-users.
	Payment Services Directive 2	2015	Financial Services	This directive regulates payment services and payment service providers throughout the European Union and the European Economic Area. The directive's purpose is to increase pan-European competition and participation in the payments industry, and to harmonise consumer protection rights and obligations across the member states.

				Extraterritorial effect: The original directive, adopted in 2007, had a limited scope, but it was amended in 2015 to have a broader, extraterritorial scope to cover "one leg transactions." This makes it explicit that a payment service provider outside of the European Economic Area, but whom is processing a payment for an EU consumer at a non-EU website, must comply with the directive's requirements.
Finland	Information Society Code	2015	Privacy, Cybersecurity, Ecommerce	This regulation consolidated 10 existing laws regulating ecommerce, privacy, data security, the communications sector, and the information society into one. Extraterritorial effect: The territorial scope of the regulation was broadened to adopt the same language as was in the GDPR at the time it was being drafted in 2014. This regulation is therefore intended to apply to entities which are established outside of the EU but which maintain or use devices for the transmission of communications in Finland or which provide services online, provided that the user of such services is in Finland. (Whether the extraterritorial nature of this provision can be enforced remains to be seen.)
Germany	Copyright and Related Rights Act	2017	Intellectual Property	This statue grants moral and exploitation rights to the producers of eligible digital and non-digital works of literature, art, and science. Extraterritorial effect: the statue is applicable to foreign-owned or foreign-operated websites that infringe copyright, provided that the website's content is available in Germany and "intentionally addressed" to German users. A common indication for the intention to address German users is the language of content being in German. Such an interpretation has been upheld by the German Supreme Court.
	Network Enforcement Act (NetzDG)	2017	Freedom of Expression	Netzwerkdurchsetzungsgesetz (Network Enforcement Act) requires online platforms with more than two million users to remove "obviously illegal" posts within 24 hours or risk fines of up to €50 million. Extraterritorial effect: the law applies to any platform, regardless of whether it would ordinarily fall within German jurisdiction, where hate speech

				may be uploaded or viewed by a German citizen or resident. Implementation has been challenging.
Russia	Code of Administrative Offenses	2018	Freedom of Expression	This amendment to an existing bill introduces fines for search engines that link to websites that are unlawful within Russia. The law requires that search engines cross-check their results against a central database of banned domain names, and not include in their Russian language search results any content that would link to a domain name on this list. Extraterritorial effect: The law is extraterritorial in that it applies to any search engine that can be accessed within Russia, regardless of whether the search engine targets Russian users or has a local presence inside of the Russian Federation.
	Law on Information, Information Technologies, and Information Protection	2017	Freedom of Expression	This law requires Russian users of online messaging apps, including WhatsApp and Telegram, to be registered to a local cellphone number. Extraterritorial effect: the law applies to non-Russian users who are not resident in Russia if they use a platform or app that is Russian owned, like VKontakte.
Serbia	Personal Data Protection Act	2008	Data Protection	This law sets out a basic framework for the protection of personal information. Extraterritorial effect: this law has a broad jurisdictional scope that applies to all users and processors of personal information who collect or process personal information in the territory of the Republic of Serbia, regardless of where they are domiciled.
Switzerland	Federal Data Protection Act	1992	Data Protection	This law governs the processing of personal information by private parties and federal bodies. The processing of personal information by cantonal authorities is subject to separate state legislation. Extraterritorial effect: enforcement of this law is possible against an entity domiciled outside of Switzerland where "the result of the violation of privacy occurs in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland)."
The Netherlands	Cybercrime III	2016	Cybersecurity	This law permits the Dutch police to hack into computers located in foreign jurisdictions in limited circumstances. Ordinarily, the law requires that the police first seek assistance through mutual legal

				assistance treaties (MLAT). However, if the location of a computer cannot be determined (for instance, because an anonymizer like TOR has been used) and it is therefore unknown as to whether an MLAT exists, the police may hack into the foreign computer for the purposes of gathering evidence. Extraterritorial effect: this law permits Dutch law enforcement to perform searches and to install location-tracking malware on computers physically located in a foreign territory by unilaterally applying Dutch criminal procedural rules to foreigners.
Turkey	No. 6698 "Law on Personal Data Protection"	2016	Data Protection	This law is Turkey's first dedicated privacy and data protection statute, and was modelled after the European Union's 1995 Data Protection Directive. Extraterritorial effect: this law is not explicitly extraterritorial. However, the law must be read in conjunction with the Criminal Code of Turkey. Article 8 of the Criminal Code states, "Turkish law is applied to the offences that are committed in Turkey. Where the act constituting an offence is … felt in Turkey, the offence is presumed to have occurred in Turkey."
United Kingdom	Computer Misuse Act	1990	Cybersecurity	This information security law has been amended numerous times since being adopted. The law permits the prosecution of British nationals for cybercrimes that happen outside of the UK and which do not hurt the UK, where the offence committed is also an offence in the jurisdiction where it took place. Extraterritorial effect: In 2015, the Act's jurisdiction was amended to become extraterritorial where a cybercrime is committed by a British national.
	Digital Economy Act	2017	Content Regulation	This Act introduces a requirement for websites that distribute pornography to install controls to verify the age of their users. Extraterritorial effect: the age-check requirement is extraterritorial as it applies to any website or other online platform that provides pornography "on a commercial basis" to people in the UK, regardless of where the website itself is based.
	Investigatory Powers Bill	2016	National Security	This legislation consolidates together into one law existing investigatory powers that are available to British law enforcement and security and

				intelligence agencies which are enshrined in several other regulations. Extraterritorial effect: the bill permits authorized parties to demand or intercept data from foreign-based companies that have, or may have, British users.
	The Gambling (Licencing and Advertising) Act	2014	Gambling	This law changed the way in which gambling was regulated in the UK from a point-of-supply to a point-of-consumption basis. Section 1(2) of the Act says it is applicable where equipment is located within the UK, or where "no such equipment is situated in Great Britain but the facilities are used there." This means that remote gambling operators now require a licence from the British government if their gambling facilities are used in Britain, even if no equipment is located here. Extraterritorial effect: a license attracts a remote gaming duty of 15% on all profits generated from British citizens, no matter where in the world the operator is situated or from where the customer accesses the facility.
Latin America and the Caribbean				
Country	Statue Name	Year of Adoption	Category	Description of Extraterritorial Effect
Brazil	Law 12,737 "Dieckmann law"	2013	Cybersecurity	This law, named after a celebrity who fell victim to cybercrime, aims to tackle Brazilian nationals who are committing cybercrimes both inside and, expressly, outside of Brazilian jurisdiction. Extraterritorial effect: any Brazilian citizen, regardless of where in the world they are, can be charged under this law if they engage in phishing, unlawfully extracting credit card numbers, extortion, or other fraudulent activities.
	Law 12,965 "Marco Civil da Internet"	2014	Civil Rights Framework	This law sets forth that access to the Internet is a requisite to the exercise of civic rights in Brazil, and imposes a number of obligations on service providers in order to guarantee the rights of Brazilians online. Extraterritorial effect: the law applies to Internet businesses that have at least one Brazilian user, regardless of whether or not they have Brazilian servers or a local office. Failure to comply with the

				law can result in fines of up to ten percent of revenue originating from Brazil.
	Law 13,709 "General Data Privacy Law"	2018	Data Protection	This statue, modelled after the European Union's General Data Protection Regulation, creates a new legal framework for the collection and processing of personal information in Brazil in both the public and private sectors. Extraterritorial effect: this statue applies to any processing: (1) "carried out in the national territory (e.g., in Brazil); (2) associated with the offering of goods or services in the national territory or involving the personal data of individuals located in the national territory; or (3) of personal data collected in the national territory." Processing activities conducted wholly outside of Brazil, but which impact Brazilian citizens, would therefore fall within this provision.
Colombia	Law 1581 "Provisions for the Protection of Personal Data"	2012	Data Protection	This statue sets forward a legal framework for the management of personal and sensitive information. Extraterritorial effect: the law itself does not define its scope. However, in a 2016 circular, the Colombian data protection authority issued interpretation guidance on the law. According to an analysis by Privacy International, its scope should be seen as extraterritorial. They note, "the processing of personal data is carried out in Colombian territory not only when the data collector is domiciled in Colombia, but also when, in order to undertake the collection, use, circulation or storage of the personal data, it uses "means" that are located in the Colombian territory."
Mexico	Law Regulating Financial Technology Institutions	2018	Fintech	This law regulates (1) crowdfunding platforms that connect entrepreneurs with investors, and (2) e-money companies which deliver electronic payment services through cryptocurrencies. Such firms must now obtain a license to operate. Extraterritorial effect: foreign businesses with no presence in Mexico are not required to obtain a license from the Central Bank of Mexico, however they must notify any Mexican consumers that their activities are not supervised by the Mexican authorities. Furthermore, foreign providers of these services are still obliged to comply with Mexican anti-money laundering requirements, including

				reviewing customer names against a Ministry of Finance blacklist.
	Federal Law for the Protection of Personal Data Held by Private Parties	2011	Data Protection	This statue regulates the collection, processing, publication, and sharing of personal information by data controllers, granting privacy rights to individuals which are not waivable under any covenant or agreement between parties. Extraterritorial effect: while the 2011 law itself does not specify a scope, its accompanying regulations published in 2013 and 2014 are clear that the law is intended to have an extraterritorial effect. The regulations note that the law is applicable to any entity not established under Mexican law that is executing a contract under Mexican law; for instance, with a data subject who is resident in Mexico.
Peru	Law 29,733 "Law on the Protection of Personal Data"	2011	Data Protection	This law offers a framework intended to ensure that the fundamental right to privacy is afforded to Peruvian citizens. Extraterritorial effect: the law applies to all personal information processing activities that are conducted on Peruvian territory, even when conducted by entities located abroad. As the definition of data "processing" is very broad, it would apply, theoretically, to any website or database containing the data of a Peruvian citizen that can be accessed from within Peru.
Venezuela	Special Law Against Computer Crimes	2001	Intellectual Property	This statue criminalizes five categories of offences, including the unauthorized dissemination of copyrighted material, the use of the Internet to access child abuse imagery, and the use of computer systems to steal records or commit espionage. Extraterritorial effect: Article 3 of the law states, "Extraterritoriality. When any of the offences provided in this Law are committed outside the territory of the Republic, the perpetrator will only be subject to its provisions if the offence has an effect within the territory of the Republic and the person responsible has not been judged for said offence, or has evaded prosecution or conviction by foreign courts."

North America				
Country	Statue Name	Year of Adoption	Category	Description of Extraterritorial Effect
Canada	Canadian Anti-Spam Law	2014	Advertising	This law regulates the distribution of unsolicited electronic communications. Extraterritorial effect: the law's broad, extraterritorial reach "applies where a computer system located in Canada is used to send or access an electronic message."
	Personal Information Protection and Electronic Documents Act	2000	Privacy	This law governs how private sector organisations may collect, use, and disclose personal information in the course of their business. Extraterritorial effect: there can be no cross-border movement of personal data belonging to Canadian residents unless the target country has enacted legislation establishing substantially equivalent data protection norms.
United States of America	Allow States and Victims to Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act	2018	National Security, Freedom of Expression	These bills make intermediaries liable for "knowingly assisting, supporting, or facilitating a sex trafficking violation," and are the first-ever federal legal precedents that permit the government to go after and prosecute websites for content that their users post. Extraterritorial effect: the laws apply to US citizens who engage in human trafficking, even if they do so in jurisdictions where this practice is not banned or use non-American platforms outside of the US in order to engage in this crime.
	California Consumer Privacy Act	2018	Privacy	This state privacy bill codifies privacy and consumer protections into law, and introduces new penalties for the misuse of personal data. Extraterritorial effect: this bill has potential extra-territorial application; subject to certain thresholds, it applies to businesses, no matter where in the world they are located, that collect information from California residents.
	Clarifying Lawful Overseas Use of Data (CLOUD) Act	2018	Data Localisation, National Security	This law empowers federal US law enforcement agencies to compel US-based technology companies via warrant or subpoena to provide requested data stored on their servers, regardless of whether the data is stored in the US or on foreign soil.

				Extraterritorial effect: in Section 3(1), the law states that it applies to any data held by an American "provider of electronic communication service[s] or remote computing service[s] … within or outside of the United States."
	Digital Millennium Copyright Act	1998	Intellectual Property	This law introduced penalties for copyright infringement on the Internet, and criminalises the production and dissemination of technology, devices, or services intended to circumvent measures that control lawful access to copyrighted works. Extraterritorial effect: the law's extraterritorial reach has been the subject of much litigation and even more debate, but it is generally accepted now that it has a binding extraterritorial reach on American companies operating abroad whose foreign subsidiaries violate its clauses.
Middle East and Adjoining Countries				
Country	**Statue Name**	**Year of Adoption**	**Category**	**Description of Extraterritorial Effect**
Egypt	Anti-Cyber and Information Technology Crimes Law	2018	Cybersecurity	This law introduces criminal penalties for cybercriminal activities such as circulating disinformation or using the Internet for purposes which "violate public morals." Article 7 of the law grants the competent authority in charge of investigating cybercrime the right to shut down websites that spread 'fake news' against the Egyptian state or threaten "national security." Extraterritorial effect: the law authorizes the competent authority to shut down (not block) foreign websites, though it is unclear how this would happen in practice.
Oman	Royal Decree No 12/2011 Issuing the Cyber Crime Law	2011	Cybersecurity	This legislation introduces into the Omani Penal Code criminal offences for the unauthorized access to a computer system, and interference with a computer system or data, among others. Extraterritorial effect: Chapter 1 Article 2 states it shall apply "even if committed wholly or partially out of the Sultanate whenever damage to its interests is ensued, or if the criminal result is ascertained within its territories or being intended to be ascertained therein even though not yet ascertained."

United Arab Emirates	Federal Law on Combatting Cybercrimes	2012	Cybersecurity	This law criminalises the use of the Internet to commit a wide range of offences, punishable by a fine and/or imprisonment. The key offences include: defamation; publishing "illegal content"; hacking and phishing; money laundering, credit card fraud, identity theft; inciting criminal and terrorist acts; and threatening state security. Extraterritorial effect: Article 47 of the law states that it has extraterritorial application, however it still remains to be seen how the authorities will enforce the law outside of UAE jurisdiction.

[19] https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/