How Canada, the EU, and the U.S. Can Work Together to Promote ICT Development and Use

BY NICK WALLACE, ALAN MCQUINN, STEPHEN EZELL, AND DANIEL CASTRO | JUNE 2018

Greater transatlantic cooperation in the development and use of information and communications technology would allow Europe and North America to increase productivity.

Governments in Europe and North America want to harness information and communications technology (ICT) to boost productivity and innovation, but uncoordinated strategies and incompatible regulations make it difficult for them to benefit fully from the mutual gains that would come from greater transatlantic cooperation in the development and use of ICT. This report analyzes key policies shaping ICT innovation in Canada, the European Union, and the United States, and identifies opportunities for policymakers to ensure policies maximize productivity and innovation.

The report describes four policy areas: intellectual property rights (IPR), data protection, the wider regulatory environment, and support for digital innovation.[1]

IPR—including rules on copyright, patents, and trade secrets—fosters much of the research and development that leads to innovation in the digital economy, as well as the creative content that consumers enjoy on digital platforms. Differences in IPR between different jurisdictions can create challenges as companies scale globally.

Data protection laws and regulations set the rules on how organizations can collect, share, and reuse data, and impact important new technologies such as data analytics and artificial intelligence. Data protection laws can be extremely complex, and are interpreted in divergent ways by different courts. Not only does this make it harder for data-driven firms to manage compliance in multiple markets, attempts to apply such laws extraterritorially can force firms to choose between competing legal environments.

The broader regulatory environment determines the legal environment in which businesses must operate. Divergent approaches to questions of anti-trust policy and technical standards threaten to create trade barriers by preventing companies with particular structures or standards from operating effectively across different markets, regardless of how they behave. Furthermore, regional variations within ostensibly single markets—whether they be American states, Canadian provinces, or EU countries—increase complexity and cost.

Government support, such as research grants and support for digital startups, can spur digital innovation. Moreover, cooperative policies, such as issuing joint calls for proposals for research and establishing cross-border research alliances, help deepen ties between the science and technology communities of countries.

To build a strong and competitive shared environment for ICT development and use, Canada, the EU, and the United States need the right combination of policies, including: strong yet flexible IPR laws; interoperable data-protection regimes that enable innovation while also protecting privacy; policies that support digital trade; intergovernmental science and technology cooperation related to digital innovation and research; and robust international cooperation to manage policy differences. This combination will be especially important as all three regions face increasing challenges from ICT competitors in other parts of the world, particularly China.

Policymakers on both sides of the Atlantic should take the following measures:

Intellectual Property

- Protect the free movement of knowledge, such as by allowing companies. participating in pre-competitive research to freely transfer ownership and access rights for IP to affiliates across and among Canada, the EU, and the United States.
- Agree on common protections for trade secrets on both sides of the Atlantic.

Data Protection

- Adopt data protection rules that reduce barriers to collecting and sharing data while also protecting consumers from harm.
- Avoid harmful restrictions on artificial intelligence, such as the so-called "right to explanation". This would impose significant costs while failing to achieve its intended goals.
- Support the free flow of data by enshrining it in international agreements between governments: privacy protection of data does not depend on its physical location.
- Support strong encryption, and do not weaken cybersecurity through mandatory "backdoors."

Wider Regulatory Environment

- Establish institutions and agree on rules for resolving conflicts that arise from policy differences between countries.
- Support free trade in ICT.

Government Support for Digital Innovation

- Help the market develop voluntary ICT standards to support interoperability.
- Establish a tripartite partnership for technology research.
- Revive and revise the Transatlantic Trade and Investment Partnership (TTIP).
- Review major new global technology challenges to prevent unnecessary regulatory divergence.

ICT POLICY IN CANADA, THE EU, AND THE UNITED STATES

Canada, the EU, and the United States each have different approaches to ICT policy. For example, while the United States has largely created a light-touch, sector-specific data-protection regime, the European Union and Canada each have created a single set of general data-protection rules for all industries. These are strict in the EU, somewhat less so in Canada. All have similar and robust laws on copyright protection. This report analyzes the differences between policies on ICT goods and services in four main areas: intellectual property, data protection, the wider regulatory environment, and government support for digital innovation.

Intellectual Property

Intellectual property rights (IPR) safeguard the incentive to innovate, as they guarantee innovators a limited period when they alone can profit from the products of their often substantial investments in R&D. Cooperation on IPR policy forms an important part of international ICT cooperation, as it allows innovators to operate seamlessly across borders and invest in R&D with confidence. However, overzealous IPR laws can inhibit innovation by restricting harmless uses of lawfully-accessed intellectual property, such as text and data mining.

Canada

Patents

Federal patent law in Canada dates back to the British North America Act of 1867.[2] Since that time, Canadian patent law has evolved through numerous iterations into the modern Canadian Patent Act of 1985.[3]

The Canadian Patent Act protects products, compositions, machines, processes, or any new improvement to an existing invention[4]. To receive a patent, the inventor must prove the invention is novel (first of its kind), useful (the invention must work), and inventive (not obvious to the relevant profession). Patents are granted for a maximum of 20 years from the day of the application.[5] Canada has a first-to-file patent system, whereby the patent application filing date is the priority reference for infringement claims.[6]

The Canadian Intellectual Property Office, which issues patents, does not have jurisdiction over patent infringements—this is the job of the courts.[7] Canada also does not have special courts dedicated to patent litigation. Inventors can bring infringement actions before a provincial superior court or the Federal Court of Canada.[8]

Copyright

Parliament passed the Copyright Act in 1921 and amended it substantially in 1988, 1997, and 2012.[9] The 2012 version is frequently referred to as Bill C-11 or the Copyright Modernization Act. It came into force in 2015.

Canadian copyright law protects literary, musical, and other artistic works, including computer programs, performances, and communications signals.[10] A copyright applies if the work was published in Canada regardless of whether the author is a Canadian citizen or resident. Regardless of merit or commercial value, the Copyright Act protects all original creative works and establishes the legal framework to do so.[11]

Many of the updates to Canadian copyright law were prompted by technological developments that challenged previous versions of the law. Portions of the Copyright Modernization Act sought to reduce digital piracy.[12] Like the Digital Millennium Copyright Act (DMCA) in the United States, the Copyright Modernization Act prohibits circumvention of "digital locks", measures installed in digital media to block piracy attempts. That includes removing such locks for personal use, and the law also bans the making, selling or using of technology to circumvent anti-piracy protections.[13]

The law does permit the reproduction of copyrighted works for satire, parody, and educational purposes. There is also an exemption for user-generated content, such as sampling music in order to create a mashup or new musical work.[14] But the Copyright Modernization Act remains controversial in Canada, with critics arguing that it weakens rights the right to personal use, the ability to back-up files, and the ability to convert copyrighted works from one format into another.[15]

Enforcement of copyright law in Canada comes through the courts. The Copyright Act empowers the courts to charge civil penalties of "a sum of not less than $100 or more than $5,000 as the court considers just" for non-commercial infringement, and up to $20,000 for each count of commercial infringement.[16] The court can also impose a criminal penalty of a fine up to $1 million, or a prison sentence of up to two years.

Trademarks

The Trade-marks Act of 1985 provides protections to words, sounds, or designs that are used to distinguish one business's goods or services from others'.[17] Under the Trade-marks Act, there are three types of trademarks: ordinary marks (such as words or sounds that distinguish some goods from others), certification marks (such as markings that show goods or services meet a defined standard), and distinguishing guises (such as the shape or packaging of a good that signifies a specific business or individual).[18] Under Canadian law, a trademark can be registered only if it identifies goods or services, while a "trade name" identifies the name of the business. Once a trademark is registered with the Canadian Intellectual Property Office, it offers protections for 15 years. Trademarks can be renewed every 15 years.

Unlike the U.S. law, Canadian trademark law is solely a federal matter; businesses cannot register trademarks with individual provinces.

European Union

Patents

Each EU member state has its own patent laws. However, there are two important European systems to improve access to patents across borders. One is the European Patent Convention (EPC), which establishes a single procedure for European patent applications, but does not harmonize patent rights: these vary between member states. The other is the unitary patent, which promises harmonized protections, but cannot function until participating countries ratify the agreement.

The European Patent Convention

There is a common application procedure for European patents via the European Patent Office (EPO), the administrative division of the European Patent Organization (EPOrg), which is separate from the EU. It was established in 1977 under the auspices of the European Patent Convention (EPC) of 1973. The EPOrg has 38 member states, including all 28 EU member states, as well as Iceland, Switzerland, Liechtenstein, San Marino, Monaco, Norway, Serbia, Albania, Macedonia, and Turkey. There are two "extension states," Bosnia-Herzegovina and Montenegro, which are not full members of the EPC, but recognize European patents in their national laws. Previous extension states have gone on to become full members. The EPOrg also has bilateral agreements on validating patents with "validation states." Two such agreements are in force with Moldova and Morocco, and the EPOrg has signed an additional two, though they are not in force, with Tunisia and Cambodia.

However, an EPO-issued European patent is not a unitary patent valid across all EPC member states. It is a collection of nationally-issued and nationally-revocable patents that are subject to varying national patent rules and limitations. The EPC is a route of access to national patents: applicants going through the EPC only need to submit one application in one language, but approval does not mean the patent holder has the same rights throughout EPC member states.

Unitary Patents

EU Regulations 1257/2012 and 1260/2012 established a legal basis for unified patents in the European Union, to be issued by the EPO.[19] But to establish the court necessary for unitary patents to work, member states must ratify an intergovernmental agreement, because the EU does not have the supranational authority to establish new courts. The Agreement on a Unified Patent Court (2013/C175/01) has 25 members, including the entire EU except Poland, Spain and Croatia. Poland and Spain decided not to sign the agreement, and Croatia was not an EU member state when participants signed in 2013.[20] As of January 2018, 15 of the 25 participating member states had ratified the agreement: Austria, Belgium, Bulgaria, Denmark, Estonia, Finland, France, Italy, Lithuania, Luxembourg, Latvia, Malta, Netherlands, Portugal, and Sweden. The court is to begin functioning in 2018, provided all participating members have ratified the agreement.

Copyright

European copyright law is partially harmonized at the EU level: there is a set of Directives on copyright, which provide a strong legal framework for copyright protection. Directives are sets of legal requirements that must be upheld in national law, but they are not regulations that apply uniformly throughout the EU. This leaves room for some differences in how member states protect copyright.

Technological change has brought up controversial issues in European copyright law, particularly in relation to text and data mining and ancillary copyright (which relates to snippets of copyrighted works), both of which are the subject of an ongoing review of legislation by the EU as of January 2018. Harmonization of European copyright policy and adaptation to technological change are priorities for the EU's Digital Single Market (DSM) strategy, but progress is slow and controversial.

Technological change has brought up controversial issues in European copyright law, particularly in relation to text and data mining and ancillary copyright.

Key legislation and protections

EU copyright law takes its lead from the Berne Convention of 1886, with which all countries must comply before achieving EU accession.

The Copyright Directive (2001/29/EC) protects the exclusive right to reproduce works.[21] Article 2 protects the rights of authors, performers, phonogram producers, film producers, and broadcasters to "authorize or prohibit direct or indirect, temporary or permanent, reproduction" of their work, 'by any means or in any form, in whole or in part'." (The latter phrase is causing controversy in the debate over ancillary copyright, as explained below.)

The Rental and Lending Rights Directive (2006/115/EC) protects:

1. Under chapter I, the lending/rental rights of authors, performers, phonogram producers and film producers, including the right to fair remuneration for rental and lending.
2. Under chapter II, article 7. the fixation rights of performers and broadcasters.
3. Under chapter II, article 8, the right to broadcast or communicate work to the public.
4. Under chapter II, article 9, distribution rights.[22]

The Computer Programs Directive (2009/24/EC) protects software, granting the authors of computer programs the same IP rights as literary authors.[23]

The Satellite and Cable Directive (93/83/EEC) protects the rights of authors to authorize or prohibit broadcasting of their work by satellite and cable.[24]

The Copyright Term Directive (2006/116/EC), amended by Directive 2011/77/EU, determines the length of protection for copyrighted works:[25]

1. Authors' rights are protected for 75 years from their date of death. For audiovisual works, the same protection exists for the principal director (always considered the author of such a work), the author of the screenplay, the author of the dialogue, and the composer of the music for the audiovisual work.

2. As of September 2011, when the EU adopted Directive 2011/77/, EU recording and performance copyright lasts 70 years from the first distribution or communication of the recording or performance, or 70 years from the date of the recording or performance itself if it was never distributed.[26] This principle covers the rights of performing artists, phonogram producers, film producers, and broadcasting companies. Prior to 2011, the protection under 2006/116/EC lasted 50 years.[27] The 2011 Directive included provisions to extend the length of existing copyright, which suggests the extension applies to works produced after 1961, but not before, although this is not explicit in the Directive.

The Collective Rights Management (CRM) Directive (2014/26/EU) governs the collective management by copyright holders of cross-border licensing for music and regulates how they collect revenue.[28] It authorizes copyright holders to appoint nonprofit entities to manage their collective rights for territories of their choice, anywhere in the EU, and requires member states to ensure each collective management organization has a supervisory function. Ensuring good faith in licensing negotiations is the responsibility of member states.

The Database Directive (96/9/EC) establishes copyright protection for creators of databases for fifteen years from the creation of the database.[29]

Intermediary liability

Section 4 of the E-Commerce Directive (2000/31/EC) protects communication networks and Internet hosts from liability for illegal content, including content that breaches copyright, provided they do not modify the information, do not initiate the transmission, do not select the sender or receiver, and are unaware of its illegality.[30] However, under article 14(b) providers of hosting services must act to "remove or disable access" to the information upon becoming aware of its illegality in order to remain protected from liability.

However, Article 13 of the proposed Directive on Copyright in the Digital Single Market (DSM) would require "information society service providers that store and provide public access to large amounts of works or other subject matter uploaded by their users"—in a word, platforms—to "take measures" to protect copyright that include "content recognition technologies." The proposal would require platforms to proactively remove content without copyright holders having to repeatedly notify platforms of copyright infringements for the same content.[31] In a report published on March 10, 2017, the European Parliament's Legal Affairs Committee (JURI) proposed several amendments to Article 13 that would remove the requirement for active filtering, but as of January 2018, the European Parliament had not yet voted on the JURI amendments.[32]

Text and data mining

Text and data mining of lawfully-accessed copyrighted works without prior permission is a breach of copyright in some EU member states. The European Commission proposed an exemption in the DSM Copyright Directive, whereby text and data mining on copyrighted works for non-commercial research purposes would be legal, but member states would still be able to ban commercial uses.[33] However, commercial uses of text and data mining on lawfully-accessed copyrighted works would not be legal. Amendment 32 of the aforementioned JURI report recommends an amendment to allow all uses of text and data mining on lawfully accessed works.[34]

Ancillary copyright

Ancillary copyright is the right of press publishers to demand remuneration for the small portion of their work that often accompanies links to the complete work, such as previews on news aggregator sites and social media. Germany introduced such measures in 2013, as did Spain in 2014. The Axel Springer group, a major German publisher, lost a significant amount of traffic after the German law came into effect because aggregators were deterred from using such snippets, and the Spanish law prompted Google News to stop displaying Spanish news content entirely.[35]

Ancillary copyright does not exist in EU law, but a complicated provision in the proposed DSM Copyright Directive could introduce it. Article 11 of the proposal would extend Article 2 of the Copyright Directive (2001/29/EC) to press publishers, "for the digital use of their press publications." Article 2 of the Copyright Directive is the exclusive right of authors, performers, phonogram producers, film producers, and broadcasters—but not press publishers—to "authorize or prohibit direct or indirect, temporary or permanent, reproduction [of their work] in any form, in whole or in part." Amendment 52 of the JURI report seeks to remove this from the proposal.[36]

Precisely how much, if any, of a preview accompanying a link might be covered by the proposal is impossible to say, because the 2001 law the proposal references was not designed for this scenario and does not stipulate the size of the extract. Article 5 of the Copyright Directive includes a specific allowance for properly-cited quotations used for the purposes of news reporting, but it is not clear whether this would protect news aggregators, social media users, or other digital platforms when they post a link to a copyrighted work of news reporting.

Trademarks

Trademarks can be registered at the national level or at the EU level (European Trade Mark, EUTM). EUTMs provide protection in all EU member states, and the same trademark can be registered both at national level and at EU level.

The protection of trade secrets, however, varies greatly throughout the European Union. Only Sweden has dedicated legislation addressing the criminal misappropriation of trade secrets; other member states address the issue through a variety of rules in criminal and civil law.[37]

United States

The foundation of U.S. intellectual property law comes from Article 1, Section 8 of the U.S. Constitution, which gives the U.S. Congress authority over granting artists, authors, and inventors the exclusive right to their creations. Intellectual property protections comprise three primary areas: patents, copyrights, and trademarks.

Patents

U.S. patent law gives inventors the exclusive right to use their product or transfer that right to another person. While U.S. patent law officially dates to the 1790s, the modern structure of patent law was created in the Patent Act of 1952, which required patents to be novel and created a definition of infringement (which previously had been left to courts to decide).[38] Indeed, for a technology to be patentable, it must not only be new, but not "obvious" to a person of ordinary skill in that profession as well. Since that time, patent law has been amended several times, including through the Leahy-Smith America Invents Act of 2011.[39] To acquire a patent, inventors file an application with the U.S. Patent and Trademark Office.

Data protection laws should prevent harmful abuses of personal data without unnecessarily limiting companies from collecting and sharing data in ways that enable data-driven products and services.

Copyright

The basic framework for copyright law in the United States comes from the Copyright Act of 1976, which describes what subject matter can be copyrighted, the terms of protection, and the basic rights of copyright holders.[40] Congress has amended this law several times, such as by the Semiconductor Chip Protection Act (SCPA) and the Digital Millennium Copyright Act (DMCA).[41] The Copyright Act allows authors to claim authorship over literary works, musical works and sound recordings, choreographic works and pantomime, graphic, pictorial, and sculptural works, motion pictures, and dramatic works. The Copyright Act grants five exclusive rights to copyright holders: the right to reproduce, distribute copies, perform the work publicly, display the work publicly, or create derivative works. In addition, the act establishes the fair use doctrine, which allows for the use of a copyrighted work without needing to acquire permission under limited circumstances, such as for research, news reporting, or criticism. Authors register copyrights with the U.S. Copyright Office.

The DMCA amended U.S. copyright law for the digital age and implemented the United States' obligations under the World Intellectual Property Organization Copyright Treaty. For example, the DMCA makes it illegal to circumvent technological measures designed to prevent people from copying works or accessing them illegitimately. Another key provision of the DMCA establishes limitations on liability for online service providers for the actions of their users, which has allowed the growth of services such as social networks and cloud computing. Finally, the DMCA established policies to facilitate services such as webcasting, by authorizing ephemeral copies of copyrighted content and establishing a statutory license for online broadcasting.

Trademarks

U.S. trademark law—which provides protections for words, phrases or logos that distinguish companies' goods or services from those of competitors—is primarily laid out in the Lanham Act, also known as the Trademark Act of 1946. The Lanham Act creates the procedure for registering trademarks at the federal level, protects trademarks against infringement, and establishes guidelines and remedies for trademark owners.[42] The purpose of this act is to avoid confusion and deter misleading advertising. Congress has amended the Lanham Act several times since 1946, including in the Trademark Counterfeiting Act of 1984.[43] Businesses only need to use a trademark in order for it to have limited protection, but by registering trademarks with the U.S. Patent and Trademark Office, owners receive additional protections. While federal law provides the most extensive form of trademark protection in the United States, business owners can also register their trademarks with states. To acquire a trademark at the state level, applicants can file the request with an individual state trademark office.[44]

Several U.S. laws provide additional protections for intellectual property. For example, the Economic Espionage Act of 1996 protects businesses from the theft or misappropriation of trade secrets by making it a federal crime.[45] Similarly, patent or trademark holders can choose to file claims of patent infringement with the U.S. International Trade Commission (ITC) instead of the courts for imports that breach copyright, and the ITC can stop these imports.[46]

Data Protection

Data protection laws should prevent harmful abuses of personal data without unnecessarily limiting companies from collecting and sharing data in ways that enable data-driven products and services. In some cases, data protection law is too onerous and restrictive, making it difficult for companies to innovate using personal data. Data protection laws can also be a barrier to international ICT cooperation and trade when they make it more difficult for foreign companies that developed under a different data protection framework to adapt to the requirements of the new market.

Canada

PIPEDA

Canada has two federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). The Privacy Act applies to the public sector and PIPEDA regulates how the private sector handles personal information. PIPEDA became law in 2000, and applies to organizations engaged in commercial activities, as well as to the personal information of employees in federally-regulated industries like banks and broadcasting.[47]

These federally-regulated industries are also subject to additional data privacy provisions specific to them. For instance, the Bank Act regulates use and disclosure standards for personal financial information held by federally regulated financial institutions. PIPEDA does not apply to not-for-profit or charitable groups, nor does it apply to political parties.[48]

PIPEDA applies to all commercial activity that causes personal information to cross provincial or national borders. However, organizations are exempt from PIPEDA if they operate only within a single province with privacy legislation that the Governor in Council deems "substantially similar" to PIPEDA.[49] To be "substantially similar" the provincial law must provide privacy protections consistent with and of equal strength to PIPEDA, offer an independent body empowered to investigate compliance failure, and contain restrictions on the collection, use and disclosure of personal information to ensure the information is not misused.

The Office of the Privacy Commissioner of Canada is responsible for ensuring compliance with the Privacy Act and PIPEDA. The Commissioner acts as a non-partisan ombudsman to investigate claims of institutional non-compliance with federal privacy law, and can audit federal institutions to ensure the appropriate handling and availability of personal information under both the Privacy Act and PIPEDA.[50]

Provinces

All provinces have a commissioner or ombudsman in charge of overseeing provincial privacy legislation and enforcement. In addition, three provinces (Alberta, British Columbia, and Quebec)[51] have created general privacy rules for the public sector that the federal government deems "substantially similar" to PIPEDA.

Provinces also have sector-specific privacy rules for certain types of data. Ontario, New Brunswick, Newfoundland, and Labrador each have health privacy legislation that is "substantially similar" to PIPEDA. In addition, provinces have created privacy rules for consumer credit reporting, credit unions, and other professionals that collect personal data, and many of these rules apply along with PIPEDA. [52]

European Union

The Charter of Fundamental Rights

Article 8 of the EU's Charter for Fundamental Rights includes a right to the protection of personal data.[53] The Charter is not a treaty in itself, but it is primary legislation (analogous to constitutional law in a nation-state) enforced by the Treaty of Lisbon, meaning any change to the Charter would require unanimous agreement among member state governments and ratification in national legislatures.[54] All EU secondary legislation (laws passed by EU institutions) and member-state legislation must comply with the Charter.

Article 8 states:

1. "Everyone has the right to the protection of personal data concerning him or her."
2. "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."
3. "Compliance with these rules shall be subject to control by an independent authority."

The GDPR and the Data Protection Directive

The intention of the General Data Protection Regulation (GDPR), adopted in 2016 and entered into force on May 25, 2018, is to fully harmonize data protection law in the EU, so that the one body of data protection law applies in all member states.[55] The GDPR replaced the Data Protection Directive.[56]

The GDPR includes existing EU privacy provisions such as restrictions on data transfers outside the EU, purpose limitation, and the right to be forgotten (codified for the first time, following the European Court of Justice's establishment of the right in case law). The regulation also includes entirely new measures, such as the right to human review of algorithmic decisions and the right to data portability. The privacy of communications services, such as telephone or Internet browsing, is covered by the privacy Directive, which the EU also plans to replace with the proposed ePrivacy Regulation (see next section).

Data minimization and purpose limitation (Article 5)

Data minimization means collecting no more data than is required to fulfill originally stated purposes. Purpose limitation means not using data for anything other than the originally-stated purpose. If data is anonymized, it falls outside the scope of the GDPR and can be re-purposed. [57] The GDPR relaxes restrictions on repurposing for "pseudonymized" data, which is essentially anonymous until combined with other data. Data minimization and purpose limitation concepts originate in Data Protection Directive, and are implicit in the Charter.

Right to human review of algorithmic decisions

The right to human review of algorithmic decisions is a new concept introduced by article 22 of the GDPR. Individuals (i.e. "data subjects") have a right not to be subject to solely automated decisions that may have legal or other significant effects, and companies can ensure this right by having a human review an algorithmic decision. There is some debate about whether the GDPR also entitles data subjects to an explanation of algorithmic decisions, but it seems likely, because Articles 13-15 explicitly provides for a right to "meaningful information" about an algorithm's rationale, and Recital 71 (recitals are not legally binding, but help judges interpret those parts that are) strongly suggests this information should pertain not only to the algorithm, but to the decision itself. The purpose of these provisions to ensure transparency and accountability in the use of algorithms. However, there is a tradeoff between accuracy and transparency in algorithmic decisions, meaning the rules could, paradoxically, make algorithmic decisions less fair than they might otherwise be.[58] Human review also raises the labor costs of deploying AI, which is designed to carry out tasks that would be costlier, slower, or simply impossible for humans. The GDPR therefore makes AI a much costlier endeavor than it might otherwise be.

Right to erasure and the right be forgotten

Article 17(1) of the GDPR gives data subjects the right to erasure of their personal data. Article 17(2) of the GDPR entitles data subjects to have publicly-available information

removed by online platforms (the right to be forgotten). Article 17(3) provides exceptions to article 17(2), including—in theory—the need to protect freedom of speech. In effect, the free speech exemption means that the right to be forgotten applies to search engines and news aggregators, but not newspapers.

The underlying principle of the right to be forgotten is a May 2014 ruling (C-131/12) by the ECJ, which stipulated that search engines must remove old links to news stories about the data subject.[59] Google has responded by blocking access to relevant articles inside the EU, but not outside it. The French national data protection authority (Commission Nationale de l' Informatique et des Libertés, or CNIL) has taken the right to be forgotten a step further, by demanding that links be removed worldwide, even in territories without a right to be forgotten, and where there are stronger protections for freedom of speech than in the EU.[60]

The right to be forgotten is now codified in Article 17(2) of the GDPR: "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

Right to data portability (Article 20)

Article 20 of the GDPR confers a new right to data portability. Article 20 extends the right of access to one's personal data to a right to receive one's personal data in a structured, machine-readable format. This provision achieves two things. First, it helps to ensure that the right of access remains meaningful as the volume of personal data grows: customers can download large sets of their personal data and analyze them digitally. Second, it allows customers to port their data to other services, opening new opportunities for data-driven services and competition.

International data transfers and adequacy rules (Articles 44-49)

The GDPR imposes a general prohibition on transfers to non-EU or "third" countries except under particular conditions, such as where the European Commission believes the third country's data protection rules are "adequate," or where there are specific safeguards or binding corporate rules that ensure the application of EU law (such as the Privacy Shield framework that governs transfers to the United States). This rule has its origin in Article 25 of the Data Protection Directive (95/46/EC).[61]

ePrivacy

The current ePrivacy Directive (2002/58/EC) is due to be replaced by the ePrivacy Regulation in 2018. the European Commission published the first draft of the proposed regulation in January 2017.[62] As with the transition from the Data Protection Directive to the GDPR, the purpose of replacing the ePrivacy Directive with a regulation is to bring about greater harmonization of European privacy law, in this case with regard to electronic communications data.

The Cookie Law

Both the ePrivacy Directive and the draft ePrivacy Regulation impose rules on the use of cookies. The Directive requires websites to get users' consent before setting cookies, and also requires web publishers to give users information about what cookies are for.

In the years since, national data protection regulators have interpreted and reinterpreted the ePrivacy rules on cookies in a variety of different ways, causing a great deal of confusion. The primary result, however, has been the proliferation of banners and popups supplying information about cookie use.

The draft ePrivacy Regulation is more specific in its rules for using cookies, and puts the responsibility for managing cookies not on the web publishers that issue cookies, as the directive rule does, but on providers of web browser software. Under the draft regulation, browsers would have to ask, on first use, whether users want to accept third-party cookies, block all cookies, or accept all cookies. Third-party cookies support cross-site services such as secure payment portals and social media posting from news websites, as well as targeted advertising. All mainstream browsers already give users the option to block different types of cookies, but they do not force users to change the setting on first use.[63]

The European Parliament has endorsed proposed amendments to the ePrivacy Regulation that would oblige websites that block access by visitors using ad-blockers to offer alternative terms for accessing the content not based on tracking—such as payments, for example.[64]

OTTs

The draft ePrivacy Regulation proposes to extend the rules that apply to traditional communications services, like telephone and Internet providers (which are covered in the Directive), to include so-called "Over the Tops" (OTTs) like WhatsApp, Telegram, Facebook Messenger, Viber, and Skype. Communications services are subject to stricter limitations on analyzing attributes such as call and messaging metadata than on other kinds of personal data, which fall under the Data Protection Directive and the GDPR.

The draft regulation does not distinguish between these types of communications services; they would be subject to the same rules. These include rules such as the requirement to erase or anonymize metadata (Article 7), unless the data is for billing purposes. The data can be retained with consent from the customer, in which case the rules of the GDPR would apply.

United States

The United States does not have a general data protection law. Instead, the U.S. legislative framework for privacy and information security consists of multiple laws that regulate the private sector primarily on a sector-by-sector basis, with multiple regulatory authorities dedicated to oversight. Laws governing data protection exist on both the federal and state levels.

Federal Data Protection Laws for Private Sector

On the federal level, a host of different laws and regulators govern data protection. The primary law for data protection of health information is the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which provides privacy and security provisions for protecting individually-identifiable medical information.[65] HIPAA creates civil and criminal penalties for violations of the privacy rule by covered entities (such as health insurers, health care providers, etc.). The U.S. Department of Health and Human Services oversees enforcement of HIPAA. In addition, the Department of Justice is authorized to criminally prosecute serious HIPAA violations.[66]

The financial services sector is also subject to federal data protection rules. For example, the Gramm-Leach-Bliley Act (GLBA) of 1999 regulates how financial firms—such as companies that offer loans, investment advice, or insurance—can collect, use, and disclose non-public personal financial information.[67] The GLBA requires financial services companies to explain their information-sharing practices with their consumers, allow consumers to choose not to share this data with third parties, and requires companies to have adequate protections in place for this data.[68] Firms that violate the GLBA can be subject to civil and criminal fines. Several federal and state financial services regulators have adopted standards based on the GLBA, including the Federal Trade Commission (FTC) and state insurance regulators.[69]

X the U.S. legislative framework for privacy and information security consists of multiple laws that regulate the private sector primarily on a sector-by-sector basis, with multiple regulatory authorities dedicated to oversight. Laws governing data protection exist on both the federal and state levels.

Similarly, the Fair Credit Reporting Act (FCRA) of 1970 regulates the privacy of personal information gathered by Credit Reporting Agencies (CRAs).[70] The FCRA requires CRAs to follow "reasonable procedures" to protect the accuracy, confidentiality, and relevance of credit information, establishing a framework for protections that limits how information is shared, and allows data subjects to access and correct limits, delete outdated information, and choose to not share information with third parties.[71] The Consumer Financial Protection Bureau is the primary agency that publishes and enforces rules for the FCRA, but the FTC can also bring enforcement actions.[72]

The Communications Act of 1934 promotes privacy of consumer information gathered by telecommunications providers while doing business.[73] This law empowers the Federal Communications Commission (FCC) to create privacy rules for customer proprietary network information (CPNI). The original purpose of CPNI rules was to regulate information regarding basic landline telephone networks—such as phone numbers, consumers' history of purchases, and the frequency, duration, and timing of calls. In 2016, the FCC proposed expanding this definition and asserting new privacy regulations for Internet service providers, but Congress resisted this change in 2017.[74]

The United States also has specific privacy rules for video rentals, video games, and other audio-visual materials (such as video streaming services). The Video Privacy Protection Act (VPPA) of 1988 protects personally identifiable rental information or sales records unless a consumer provides consent for the disclosure in writing.[75] The VPPA also requires law enforcement agencies to seek a warrant to obtain this information and creates civil penalties for violations of this rule. Moreover, U.S. law also specifies privacy rules for automakers

and the use of data gathered from electronic data recorders (EDR)—devices known as "black boxes" that record data in the event of a car accident. In 2015, Congress passed the Driver Privacy Act limiting the use of data gathered from EDRs and specifying that this data is the property of the vehicle owner, regardless of where the vehicle was manufactured.[76]

In addition, the United States has several laws designed to protect the privacy of children. The Children's Online Privacy Protection Act (COPPA) requires websites to obtain parental consent for the collection of personal information on children under 13.[77] The FTC oversees enforcement of COPPA. Similarly, the Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records for children under 18.[78] FERPA requires all schools to receive parental consent prior to sharing a student's educational records, except under limited circumstances.[79] The U.S. Department of Education publishes and enforces this rule.

Besides specific industry and governments rules, U.S. consumer protection law designates the FTC as the primary regulator for general data protection enforcement. The Federal Trade Commission Act of 1914 gives the FTC the power to enforce against "unfair or deceptive acts or practices in or affecting commerce," which the regulator has used to bring enforcement actions against a wide range of entities who have not kept their promises to consumers in stated company privacy policies. The FTC does not have authority over certain industries and entities, such as banks, savings and loan institutions, and common carriers, which are regulated by other federal agencies.

When a company acts unfairly or deceptively, the FTC can bring enforcement actions that result in a consent decree, whereby the company faces penalties for future misconduct. During the span of a consent decree—which can last up to 20 years—the company can be subject to an audit by the FTC, and violations can result in steep fines. For example, in 2011 Google established a consent decree with the FTC under which it committed not to misrepresent privacy assurances.[80] The company then settled with the FTC a year later for violating the terms of the consent decree, resulting in a large fine.[81]

State Data Protection Laws

In addition to federal data protection laws, states have also created numerous specific privacy laws that only apply within their jurisdictions. For example, while there is no federal data breach notification law, 48 states, the District of Columbia, and several territories have enacted legislation that requires private or public organizations to notify individuals in the event of a security breach of their information.[82] California has one of the strongest data breach laws in the United States, which requires any business or state agency to notify a California resident of a data breach within 30 days, except under limited circumstances.[83] With any state-specific privacy or security law, the state's attorney general can punish violations.

Wider Regulatory Environment

Intellectual property and data protection are key regulatory domains for ICT innovation, but the wider regulatory environment can also have a significant impact. Many countries strive to create an environment that attracts businesses and cultivates economic growth, such as by streamlining regulatory requirements imposed on businesses and decreasing barriers to entry into local markets. The World Bank measures this quality in nations—known as the ease of doing business—by assessing 11 different factors in a country's regulatory environment, such as how easy it is to register property, enforce contracts, or start a business.[84]

Canada

Canada's regulatory climate is reasonably business-friendly, ranking 22nd out of 190 countries in the World Bank's "ease of doing business" measurements.[85] Canada is the second-easiest place to start a business in the world due to factors such as the speed and ease of registering a company. Canada also comes in seventh place for both obtaining credit—with its strong legal rights, universal credit bureau coverage of adults, and depth of credit information—as well as the strength of protections for investors. On the other hand, it can take 137 days for a business to get electricity, and Canada also scores quite poorly (112th overall) for enforcing contracts, as resolving claims can be very time-consuming.[86]

In Canada, legislative authority is divided between the federal and provincial governments. At the federal level, an enacted law sets the scope for regulatory power and assigns authority to a ministry to make subordinate regulations. The Statutory Instruments Act governs how ministries create federal regulations.[87] First, the ministry produces a draft regulation, which is reviewed by the Clerk of the Privy Council and the Deputy Minister of Justice before it is published in the Canada Gazette and is made available for public comment.[88] The regulation is then amended based on this feedback, if necessary, registered by the Clerk of the Privy Council, and published in its final form in the Canada Gazette.

Canada's Competition Act is the oldest antitrust legislation in the Western world and applies to all businesses in Canada. The stated purpose of the Act is to maintain competition in Canada, promote efficiency, stop deceptive practices, and ensure equal opportunities for small business. The Competition Act prohibits false or misleading practices by businesses, such as deceptive marketing practices.[89] In addition to criminalizing explicitly anti-competitive business practices, the Act also requires premerger notification and contains noncriminal provisions that allow the Competition Tribunal to review certain business practices (such as tied selling, exclusive dealing, refusal to deal, and abuse of dominance), and to issue orders correcting the conduct to eliminate or reduce its anti-competitive impact. Private parties may also apply to the Tribunal seeking a review of business practices. The consequences of violating the criminal provisions of the Act can be severe, with criminal offenses punishable by fines of up to $10 million and/or imprisonment for periods of up to five years.

The Competition Act also addresses competition outside Canada's borders. International coordination between the Competition Bureau and competition enforcement agencies in

other jurisdictions have become central to Canadian enforcement in cartel matters and merger review. Amendments to the Act introduced in 2002 say Canada may enter competition enforcement cooperation agreements with other countries that permit the exchange of information in criminal and civil competition matters. Canada currently has competition cooperation agreements with several countries, including Brazil, Chile, Japan, Korea, Mexico, New Zealand, members of the European Union, the United Kingdom, and the United States.

Canadian regulators have the authority to punish companies that infringe laws and regulations. For example, in 2015, the Competition Bureau took action against Aviscar and Budgetcar, two of Canada's largest rental car companies (both owned by Avis) for advertising prices that were unavailable to consumers at the time of purchase due to extra fees.[90] Similarly, in 2015 the Canadian Radio-television and Telecommunication Commission announced enforcement proceedings against Compu-Finder for sending commercial messages without recipients' consent and without a functioning "unsubscribe" button (as is required by Canada's anti-spam laws).[91]

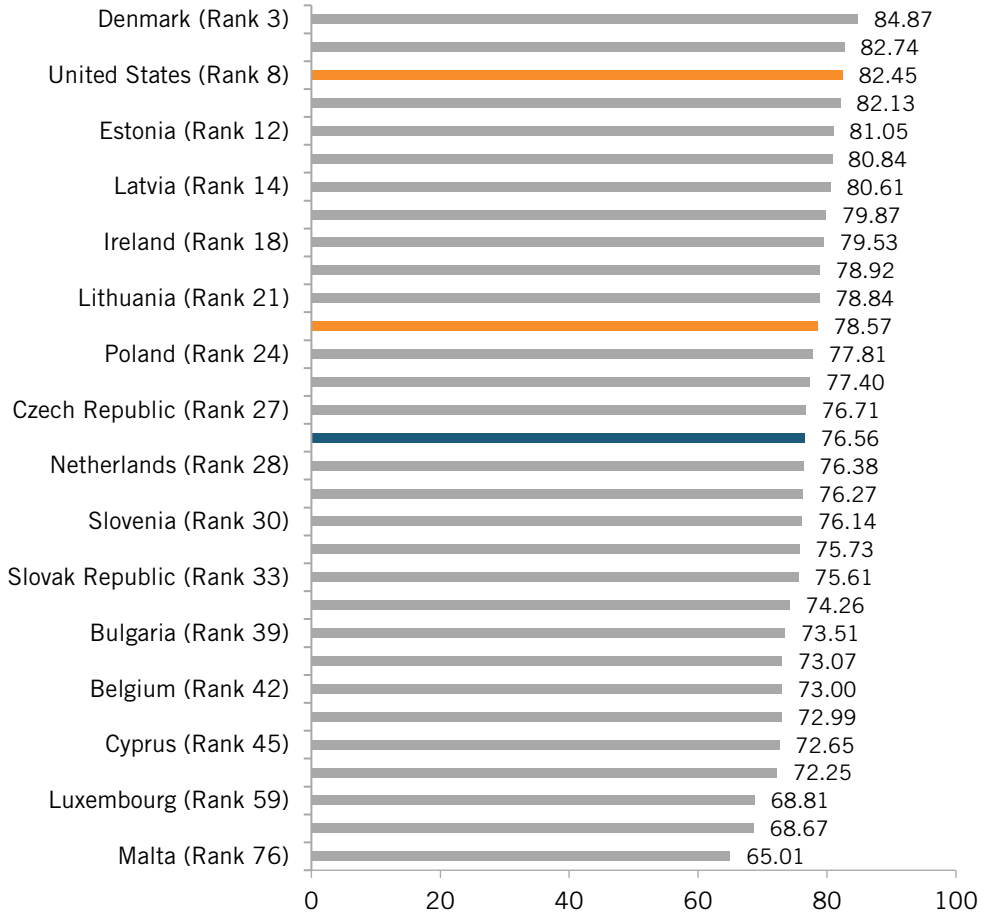
Like the U.S. government, the Canadian government allows industry self-regulation, in which private, market-based institutions govern their own actions through voluntary agreements. For example, in 2013 Canadian advertisers, marketing trade associations, and industry groups formed the Digital Advertising Alliance of Canada and created the self-regulatory program AdChoices for online advertising.[92] The Canadian government supervises these commercial entities to ensure they keep their promises. For example, the Office of the Privacy Commissioner of Canada launched a research project in 2015 to ensure advertisers were complying with Canadian privacy laws and their own commitments.[93]

Canadian Provinces also regulate some areas that the federal government does not, such as credit reporting and contracts, and administer a large portion of Canadian consumer protection law.[94] At the provincial level, each province has its own office for various regulatory affairs, and many of these offices have created rules governing digital goods and services. For example, in March 2017 the Ontario Securities Commission announced that companies using digital currency technology (such as block chain or distributed ledger technology) may be subject to Ontario securities law requirements.[95]

European Union

There is wide variation between EU countries' performance in the World Bank's Ease of Doing Business index.[96] As figure 1 shows, two EU countries ranked higher than the United States and ten ranked higher than Canada.

Figure 1: Ease of doing business in the EU, the United States, and Canada, 2017. Source: World Bank[97]



The wide range of "ease of doing business" scores among EU countries reflects how fragmented is the EU's regulatory environment and "single" market.

The wide range of "ease of doing business" scores among EU countries reflects how fragmented is the EU's regulatory environment and "single" market. To understand this fragmentation, it is necessary to understand how different powers, or competencies, are divided between the EU and its member states.

EU Competencies and the Subsidiarity Principle

The EU's stated competencies are divided into three categories in Articles 3-6 of the Treaty on the Functioning of the European Union (TFEU): exclusive competencies, shared competencies, and supporting competencies. Any policy areas that fall outside these competencies are the sole prerogative of the member states.

Exclusive competencies (Article 3 of the TFEU: only the EU can legislate on these matters)

- The customs union
- The establishment of competition rules necessary for the functioning of the single market
- Monetary policy in the Eurozone (currently ranked 19 out of 28 member states)

- Conservation of marine biological resources under the common fisheries policy
- The common commercial policy
- The conclusion of international agreements when provided for in EU legislative acts, or when necessary to enable the EU to exercise its internal competence, or insofar as an agreement affects common rules or their scope[98]

Shared competencies (Article 4 of the TFEU: member states can legislate on these matters where the EU does not)

- Internal market
- Aspects of social policy defined in the TFEU (Articles 9, 10, 19, 45-48, 145-150 and 151-161)
- Economic, social, and territorial cohesion (regional policy)
- Agriculture and fisheries, excluding the conservation of marine biological resources
- Environment
- Consumer protection
- Transport
- Trans-European networks
- Energy
- Area of freedom, security and justice
- Aspects common safety concerns in public health matters, defined in TEFU Article 168[99]

Supporting competencies (Article 6 of the TFEU: The EU can only act to support, coordinate or complement actions by Member States, it cannot require harmonization of member state law)

- Protection and improvement in human health
- Industry
- Culture
- Tourism
- Education, vocational training, youth, and sport
- Civil protection
- Administrative cooperation[100]

Subsidiarity

A key principle of EU lawmaking is subsidiarity, which in lawmaking means the EU can act outside its exclusive competencies only if the desired objectives cannot be achieved by the member states.[101] In other words, any EU act outside of the exclusive competencies needs a sufficient rationale for not leaving the matter to the member states.

The effect of these competencies and the subsidiarity principle is that regulations vary considerably in different parts of the EU. National regulators are also often responsible for implementing EU-level legislation: the GDPR, for instance, is an EU-wide law, but enforcement will be member states' responsibility.

However, the European Commission does act as a regulator in some instances. In addition to being ultimately responsible for regulation of the member states (initiating action against member states that breach EU law, for example), it also acts as a regulator for issues under the EU's exclusive competences, such as anti-trust in the context of the single market.

United States

In 2017, the United States ranked 8th in the World Bank list for "ease of doing business."[102] At the federal level, Congressional legislation, executive orders, and administrative rules all regulate the actions of firms in the private sector.

U.S. federal agencies, which receive their authority from federal law, have the ability to create administrative rules and regulations. The Administrative Procedure Act of 1946 governs how U.S. agencies may establish regulations.[103] The act requires agencies to inform the public about agency proceedings and rules, sets uniform standards for formal rulemakings and adjudication, requires public participation in the rulemaking process, and defines the scope of judicial review for administrative rules. The act applies to both executive agencies (such as the Department of Transportation) and independent agencies (such as the FCC). As a result of this act, when creating administrative rules, agencies go through an extensive public notice and comment period in which individuals and organizations can submit written comments that the agencies are required to review. In addition, the Office of Information and Regulatory Affairs within the White House Office of Management and Budget conducts cost-benefit reviews of some proposed regulations, particularly those with high expected costs.

The U.S. government also frequently allows industries with no specific guiding laws to self-regulate. Diverse industries, such as higher education, fashion, advertising, mining, nuclear power, and marine fishing all use self-regulatory processes to govern industry practices.[104] Self-regulation is "a regulatory process whereby an industry-level organization (such as a trade association or a professional society), as opposed to a governmental- or firm-level organization, sets and enforces rules and standards relating to the conduct of firms in the industry." [105] This involves private institutions governing their actions through voluntary agreements, peer pressure, and other methods to coordinate behavior without violating anti-trust rules.

Many self-regulatory activities occur through self-regulatory organizations (SROs). SROs are the non-governmental organizations formed by the private sector to set standards, monitor for compliance, and enforce their rules. Some SROs operate with government endorsement. For example, the North American Electric Reliability Corporation (NERC), which is responsible for establishing and enforcing standards for the electric power grid, is certified by the Federal Energy Regulatory Commission. Similarly, the Financial Industry Regulatory Authority (FINRA), which regulates the securities industry in the United States, receives oversight from the Securities and Exchange Commission (SEC).[106] Other examples of SROs include industry bodies that regulate the use of natural resources, such as the Marine Stewardship Council formed to responsibly manage the global fish stocks.[107]

Industry and government jointly administer the self-regulatory process by providing oversight of industry standards or SROs and enforcing penalties for violations. In addition, the United States has other forms of "soft law," such as government-issued recommendations, principles, or codes of conduct that create a nonbinding regulatory framework.[108] The FTC has the authority to enforce voluntary frameworks by penalizing companies that behave unfairly or deceptively. For example, if aerial drone operators adopt the National Telecommunication and Information Administration's (NTIA) voluntary best practices for drone privacy, and then break their commitments, the FTC can take an enforcement action against them.[109] Similarly, if a company mischaracterizes the level of security it provides its customers, then the FTC can bring an enforcement action against that company. Or if a securities company's employees do not follow FINRA's code of conduct, they could be subject to a penalty from the SEC.[110]

The role of U.S. regulators is expanding. ICT goods and services are an area where many U.S. regulators have not traditionally created rules. However, in recent years, regulators have started regulating more ICT goods and services due to the convergence of ICT with other sectors of the economy. For example, the U.S. Department of Transportation (DoT) has always created rules for cars and airplanes, but responding to changing technology, the DoT recently proposed policies for automated vehicles and drones.[111] Similarly, in 2016, the Office of the Comptroller of the Currency, an agency of the U.S. Department of Treasury that oversees banks, announced plans to let fintech companies (i.e. companies focused on using the latest innovations in information technology to improve financial services) apply for special-purpose federal bank charters, allowing them to follow a single set of federal regulations instead of differing state laws.[112]

Government Support for Digital Innovation

Governments that create sensible regulations that enable digital innovation are not responsible for guaranteeing the commercial success of every novel idea. However, governments can help to encourage digital innovation by providing limited financial support to research and development of digital projects that could go on to become commercial successes in their own right and contribute to wider economic competitiveness and productivity.

Canada

The Canadian government has several policies that support the development and deployment of ICT, including public R&D support, research organizations, technology transfer offices, tax incentives, and standards development.

Canada encourages innovation in ICT goods and services by supporting scientific research. The Canadian government provides funding for basic scientific research at universities. However, public support for R&D as a share of GDP has fallen substantially over the last few years to its lowest level since before 1996.[113]

The Canadian federal government also funds several government organizations that directly conduct research in numerous scientific disciplines, such as atomic energy, health,

aerospace, and agriculture. For example, the National Research Council of Canada is a government agency that directly funds R&D initiatives to help Canadian industries bring emerging technologies to market.[114] Most Canadian provincial governments also fund labs and institutes that conduct research. For example, Alberta created the Alberta Research Corporation to develop and commercialize technology to help grow innovative businesses in the province.[115]

Canada has created several programs to help encourage technology transfer, such as through dedicated technology transfer offices at various universities and agencies.[116] These offices connect researchers at universities with outside financing and business experts to help turn ideas into commercial viable products. However, according to a 2013 report from the Council of Canadian Academics, while investments in technology transfer may have increased since 2000, the number of patents and licensing agreements has not.[117]

In 2017, the Canadian Government announced Pan-Canadian Artificial Intelligence, a CAD$125 million program to bolster the country's AI research and development.

In addition, Canadian tax law provides numerous incentives for businesses conducting ICT research and development. The Scientific Research and Experimental Development program, a Canadian federal tax incentive program, provides tax credits of up to 35 percent for up to CAD$3 million in research expenditures.[118] This 35 percent is 100 percent refundable. Canadian businesses can also earn a non-refundable credit for research up to 15 percent on all spending after CAD$3 million. A 2014 study found that companies that qualified for a larger tax credit spent more on R&D when compared to firms with similar income whose situation did not change.[119] Nevertheless, the Council of Canadian Academics found in 2013 that the Canadian business sector invests less in R&D than its peers abroad.[120]

The Canadian government also encourages digital innovation by setting standards. The central agency in the Canadian Government that sets standards is the Standards Council of Canada (SCC), which consists of accreditation services, corporate services, and other standards-setting services.[121] The SCC works with various stakeholders to develop standards or accreditation for everything from aerospace to radio interference.[122] For many issues surrounding ICT goods and services—those that are not related to health, safety, or the environment—the Canadian government also allows industries to self-regulate. For example, the Canadian Marketing Association developed a code of ethics and standards of practice, which are compulsory for its members, to create a self-regulatory framework for how marketers can advertise online.[123] This approach allows the government to let industry cooperation and competition, as well as consumer choice, determine appropriate standards, best practices, or codes of ethics.

In addition, the Canadian government is positioning Canada to be a world leader in artificial intelligence (AI). In 2017, the Canadian Government announced Pan-Canadian Artificial Intelligence, a CAD$125 million program to bolster the country's AI research and development.[124] The strategy involves creating national programs that build the AI community, attracting and retaining top AI talent, and increasing the number of Canadian graduate and undergraduate students studying AI. The program will be administered through the Canadian Institute for Advanced Research (CIFAR). Canadian provinces are

also getting involved in AI development. For example, Ontario is contributing CAD$50 million to building the Vector Institute at the University of Toronto, for research into deep learning.[125] (CIFAR's Pan-Canadian Artificial Intelligence Strategy is also contributing between CAD$40 and CAD$50 million to the Vector Institute.)[126]

European Union

Both the EU and its member states provide financial support. The main source of EU funding for digital innovation is currently the Horizon 2020 program, but European Structural Funds—which are primarily for regional development—can also support digital projects, provided those projects are aligned to the goals of the structural funds.[127] The European Commission also plays a role in guiding standards development, such as by coordinating member states' efforts to support the standards development.

EU Initiatives: Horizon 2020 and the EIT

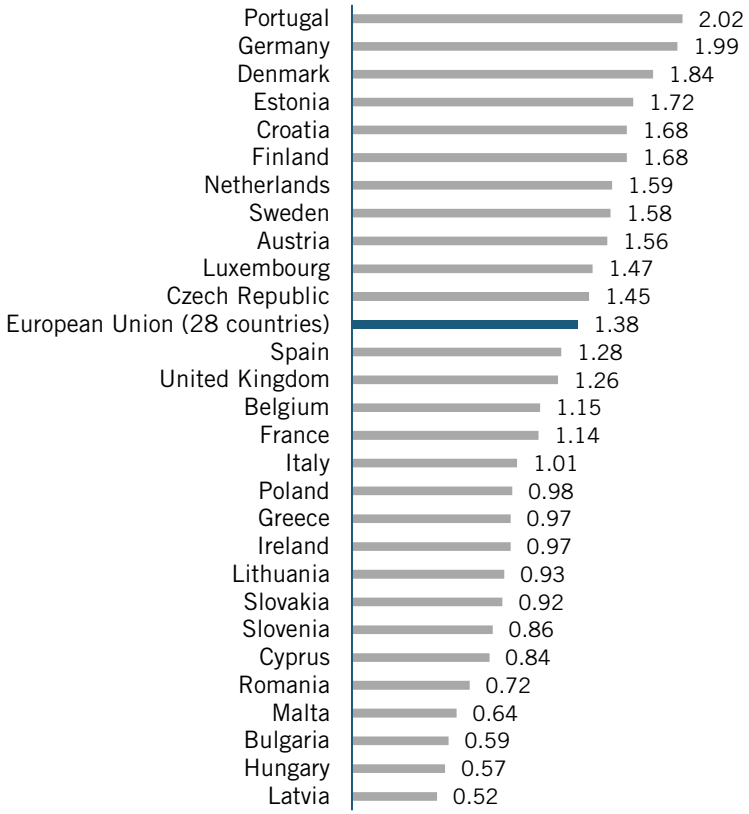
Running from 2014 until 2020, Horizon 2020 is the principal source of EU funding for research and innovation in Europe, including digital innovation. It has a total budget of almost €80 billion, including €2.7 billion for the development of "future and emerging technologies," and €13.6 billion for "leadership in industrial technologies."[128] Furthermore, several other Horizon 2020 top-level provisions not dedicated specifically to technology—including those dedicated to transport, energy, the environment, and sustainability—often help to support digital innovation where it serves relevant goals. For example, some Horizon 2020 funds go to smart-city projects, which use digital technologies to make urban life more efficient and sustainable.

The European Institute for Innovation & Technology (EIT) is an independent organization set up by the EU with the express purpose of supporting technological research and innovation in response to societal challenges. Unlike Horizon 2020, it operates independently of EU institutions.

Member State Support for Digital Innovation

Member state support for digital innovation is varied. Specific policies can include dedicated sources of funding, such as the UK's Innovate UK and the Future Cities Catapult, or tax breaks, such as the French crédit d'impôt recherche (CIR), which supports research in digital innovation. Figure 2 shows EU member state governments' spending on R&D in 2015.

Figure 2: Government R&D spending in the EU as a percentage of overall budget, 2015. Source: Eurostat[129]



United States

The primary form of support the U.S. government provides for digital innovation is investments in ICT research and development (R&D) that have over time laid the groundwork for the development of key digital technologies. From supporting the development of relational databases and integrated circuits to the graphical user interface (GUI) and the Internet itself, federal support for ICT and digital innovation has been vitally important in the United States. In fact, one 1987 study found that the U.S. government financed 18 of the 25 biggest IT innovations (such as magnetic core memory and multiple central processors) between 1946 and 1965.[130] However, unlike the EU, the United States does not have a specific ICT R&D program with a focus on industrial competition.

The U.S. government encourages digital innovation by supporting scientific research. This support has two elements: university funding for basic, curiosity-directed research and federal research labs. Relative to private-sector funding for R&D, however, federal support for R&D has fallen substantially as a share of GDP, from 1.25 percent in 1977 to just 0.75 percent in 2017.[131] The National Science Foundation (NFS) estimated that, while U.S. R&D funding was an all-time high of $499 billion in 2015, the overall federally-sponsored share had fallen to a record-low of 23 percent.[132] In May 2017, the U.S. administration proposed a FY2018 budget that would have compounded these decreases with steep cuts to

federal R&D investment, but Congress rejected most of these cuts.[133] Moreover, fiscal challenges facing the U.S. government suggest that future increases to federal R&D funding will be difficult to achieve and further inflation-adjusted declines are possible.

In addition to funding, the U.S. government supports digital innovation through federal research labs. The United States has a host of collaborative research ventures, including the National Science Foundation (NSF) Science and Technology Centers and Engineering Research Centers as well as the National Institute of Standards and Technology (NIST) Advanced Technology Program. U.S. agencies—such as the Departments of Defense, Energy, and Health—also fund a system of between 80 and 100 government research laboratories. For example, the Department of Energy's National Laboratory system consists of 17 labs that focus on multidisciplinary research for national scientific objectives not advanced by either the private sector or universities.[134] Some of these labs are government operated, while some are private-contractor operated. Most of this research is funded to help agencies better achieve mission goals. In addition, some agencies, like NSF and the National Institutes of Health (NIH), have begun pilot programs to better link their funded research to commercialization.[135] Overall, while there are policies to help spur commercialization, the only federal agency explicitly focused on commercial innovation is NIST.

The Defense Advanced Research Projects Agency (DARPA) and Advanced Research Projects Agency-Energy (ARPA-E) have also played an important role in the development of cutting-edge ICT. While these technologies are initially designed to support agency objectives, such as improved defense or energy efficiency, over time these innovations have yielded substantial technology spinoffs to the global economy (such as lasers). DARPA also hosts open competitions to help develop new technologies or solve technological challenges. For example, in 2004 DARPA hosted a prize competition to develop autonomous vehicles, known as the DARPA grand challenge, and the agency has periodically hosted similar competitions to advance innovation.[136]

Furthermore, the U.S. government helps bolster digital innovation by encouraging voluntary, industry-led standards. No single U.S. government agency sets standards for businesses. In contrast, the U.S. commercial standards system (this does not include standards for health, safety, and the environment) is a voluntary, consensus-based system. The government does not get involved in picking industry standards. For example, when a dispute arose between HD and Blu-ray high-definition video players, the government let cooperation and competition between industry players and consumer choice determine the winning standard.[137] Industry standards are often developed by industry trade associations and by the American National Standards Institute (ANSI), which facilitates the creation of national standards by accrediting the procedures of individual standards-developing organizations.[138] These groups collaborate to develop open voluntary national standards using a consensus-based process.[139] The content of these standards may relate to products, processes, services, systems, or personnel.

The U.S. government may also guide various private-sector stakeholders and interested members of the public in developing guidelines or best practices. For example, the National Telecommunications and Information Administration (NTIA) is the neutral arbiter for several multi-stakeholder processes to develop voluntary best practices or industry codes of conduct for users of particular technologies, such as mobile applications, facial recognition technology, drones, or the Internet of Things.[140] The NTIA leads the discussion between various interested stakeholders but does not actively create or decide the final rules. Similarly, NIST helps develop standards by bringing together various stakeholders, such as other agencies, commercial entities, and ANSI, to help create voluntary technical standards (such as NIST's cryptographic standards) and voluntary frameworks (such as NIST's Cybersecurity framework).[141] NIST is primarily a federal laboratory and its work largely involves measurement, not private-sector standard setting.

The U.S. government has also instituted various federal programs and challenges to promote digital innovation, especially through connected infrastructure technologies. For example, in 2015 the U.S. Department of Transportation launched the Smart City Challenge, a program that offered mid-sized cities across the United States roughly $350 million in public and private funds to develop and deploy smart city and advanced transportation technologies.[142] In addition, the U.S. Department of Transportation allocated $42 million in 2015 for three large-scale pilots of vehicle-to-infrastructure communications technologies in the state of Wyoming, New York City, and Tampa, Florida.[143]

Similarly, in 2014, NIST partnered with US Ignite—a nonprofit dedicated to advancing smart cities—to launch the Global City Teams Challenge.[144] This challenge was designed to bring together stakeholders from diverse sectors of the economy (such as energy, healthcare, manufacturing, etc.), to collaborate and develop standards for smart cities and smart communities.[145]

In addition, the U.S. government has created several programs to promote digital innovation for defense and intelligence. For example, in 2015 the U.S. Department of Defense launched the Defense Innovation Unit-Experimental (DIUx) to bring commercial innovation to the U.S. military.[146] DIUx funds promising technologies through prize competitions, targeted R&D efforts, and incubator partnerships.[147] U.S. intelligence agencies have also created programs to bring the latest technologies to agencies focused on protecting national security. For example, the U.S. Central Intelligence Agency has created a non-profit strategic investing program, known as In-Q-Tel, to invest in the development and deployment of advanced technologies for the U.S. intelligence community.[148]

A key initiative is the National Strategic Computing Initiative (NSCI), which seeks to create a coordinated federal strategy for high-performance computing (HPC) research, development, and deployment. The NSCI defines a multiagency framework for furthering U.S. economic competitiveness and scientific discovery through orchestrated HPC advances. The NSCI represents a whole-of-government effort designed to create a cohesive federal investment strategy, executed in collaboration with industry and academia, to

maximize the benefits of HPC (in terms of both production and adoption) for the United States. In 2016, Congress allocated $325 million to the NSCI effort to bolster U.S. high-performance computing leadership. NITRD has also played an important role in the development of America's *Cybersecurity R&D Strategy*, *Big Data R&D Strategy*, and *Privacy R&D Strategy*.

Moreover, some agencies use contracting methods to support innovation with the private sector.[149] The National Oceanic and Atmospheric Administration (NOAA) partnered with several tech companies—including Amazon Web Services, Google Cloud Platform, IBM, Microsoft Corporation, and the Open Cloud Consortium—to participate in its Big Data Project.[150] NOAA generates tens of terabytes of data from its sensors each day—more data that it could feasibly provide to the public with its current budget—so it invited the private sector to make this data available to the public at no cost in exchange for the opportunity to sell value-added services. Through this partnership, NOAA is able to foster digital innovation without additional expenditure.[151]

Several U.S. states have announced strategic plans to foster a culture of innovation and entrepreneurship. For example, in 2015 Massachusetts announced a plan to attract companies focused on digital health care, the Internet of Things, robotics, cybersecurity, autonomous vehicles, and more.

U.S. states also have created initiatives to support digital innovation. Several U.S. states have announced strategic plans to foster a culture of innovation and entrepreneurship. For example, in 2015 Massachusetts announced a plan to attract companies focused on digital health care, the Internet of Things, robotics, cybersecurity, autonomous vehicles, and more.[152] U.S. states have also invested heavily in R&D funding for digital innovation. States like Indiana and Maryland have poured millions of dollars into research and technology transfer for a variety of different innovative disciplines, such as biotechnology and aerospace.[153] Much of this funding is directed to public universities within the state. For example, in 2017 the Michigan Strategic Fund awarded the University of Michigan and Michigan Technological University $2.2 million in tech transfer grants.[154]

Furthermore, U.S. taxes also affect ICT goods and services. U.S. tax policy towards ICT can be interventionist, sometimes for good policy reasons (such as tax credits for R&D) and other times due to pressures from special interests.[155] However, most U.S. policymakers generally strive for a tax code that does not favor particular industries over others, even if this means that some traded sectors exposed to international competition pay more than some nontraded sectors.[156] Moreover, the U.S. federal corporate tax rate was high at 35 percent (excluding state taxes), but at the end of 2017, Congress cut this to 21 percent.[157] This compares to averages in 2016 of 30.21 percent in the G7, 18.88 percent in Europe and 22.5 percent globally.[158] In addition, the U.S. R&D tax credit is relatively anemic compared to other nations, ranking 25th in the OECD in 2012 for R&D tax generosity.[159] And unlike all EU countries and Canada, the United States does not use a border-adjustable value-added tax (VAT).[160]

COMPARATIVE ANALYSIS OF TRANSATLANTIC ICT POLICY AND COOPERATION

What effect the policy measures described above have within their respective jurisdictions is a separate question from how the contrasts between them shape the transatlantic ICT market, and how Canada, EU, and the United States cooperate on ICT. This section

analyzes how the above contrasts play out at the transatlantic level, and what efforts the three entities have made to support transatlantic ICT cooperation.

Intellectual Property

While IPR rules differ between Canada, the EU, and the United States, there are basic common protections in all three markets established by a variety of international agreements. The EU and the United States both support research into the importance of intellectual property to their respective economies. For example, the report published by the European Patent Office (EPO) and the EU Intellectual Property Office (EUIPO) found that IPR-intensive industries generated 27.8 percent of jobs in the EU during 2011-2013, and accounted for 42 percent of GDP.[161] The U.S. Economics and Statistics Administration (ESA) and the U.S. Patent and Trademark Office (USPTO), meanwhile, found that IPR-intensive industries accounted for 30 percent of U.S. employment, 30 percent of U.S. growth, and 38.2 percent of overall GDP in 2014.[162]

The oldest of the relevant trade agreements are the Paris Convention of 1883 and the Berne Convention of 1886, both of which remain in force, subject to amendments (the most recent being 1979 and 1971, respectively) and which establish the basic principles for subsequent intellectual property agreements. These, along with 24 other subsequent treaties on intellectual property, are today administered by the World Intellectual Property Organization (WIPO).[163]

These treaties establish principles such as the common recognition of the date on which a rights holder initially filed an intellectual property application in a signatory country, and minimum rights for all literary, scientific, and artistic productions. However, WIPO-administered agreements lack strong international enforcement mechanisms, and therefore are to a large extent dependent on member states adhering to their international commitments and respecting the rule of law.[164]

The World Trade Organization (WTO), however, has stronger enforcement procedures, and as members of the WTO, Canada, the EU, and the United States all have ratified the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). TRIPS includes requirements such as a minimum copyright term of 50 years, and the automatic entitlement to copyright, without the need for registration (thus strengthening an important provision of the Berne Convention by bringing it under the authority of WTO courts).[165]

The most recent transatlantic agreement that deals with intellectual property is the Canada-EU Comprehensive Economic Trade Agreement (CETA), which both parties signed in 2014 and ratified in February 2017. CETA brings Canadian intellectual property protections into line with the stricter protections of EU member states, such as by extending copyright terms from 50 years to 70 years.[166]. CETA includes ICT-specific measures for intellectual property, such as legal protection for anti-piracy technology measures and for rights management information in digital content.[167] CETA also limits the extent to which internet platforms (intermediaries) can be held liable for copyright-

infringing content uploaded by their users, in line with existing EU law.[168] CETA also includes measures for the protection of data related to plant-production products under its intellectual property provisions.[169]

Data Protection

Canada, the EU, and the United States have very different data protection regimes, yet data flows, and the regulation thereof, are an increasingly important topic for transatlantic trade. The EU and the United States are each other's largest export markets for digitally-deliverable services, and the United States' underwater cable Internet connections to Europe are its fastest.[170] However, there are barriers to the free flow of data internationally, particularly as a result of data protection concerns. Efforts to establish freer data flows have been limited, in large part because the EU does not negotiate data protection matters in trade agreements.[171]

The EU's Data Protection Directive and the General Data Protection Regulation (GDPR), which will replace the Directive on May 25, 2018, prohibit transfers of personal data outside the EU unless the European Commission has ruled the data protection laws of the destination country to be adequate, or unless there is an international agreement or binding corporate rules to protect the data.[172] The United States has also resisted international efforts to abolish rules restricting data transfers for financial data, as part of its negotiations with Canada and Pacific countries for the Trans-Pacific Partnership (TPP, from which it has now withdrawn completely), due in part to pressure from U.S. financial regulators concerned about their ability to access data.[173]

The European Commission has regarded Canadian data protection law as "adequate" since 2001.[174] The Commission does not view United States privacy law as adequate, but does permit data transfers to the United States under the terms of the Privacy Shield Agreement between the EU and the United States, which provides a legally-enforceable framework for the treatment of European personal data in the United States.[175] Privacy Shield replaced the Safe Harbor decision, which operated from 2000 until 2015, allowing data transfers by American companies that agreed to EU requirements and received certification.[176] The European Court of Justice terminated Safe Harbor in 2015, in light of Edward Snowden's revelations about NSA surveillance.[177] The ensuing crisis led to Privacy Shield.

It is notable that Canada, despite being a part of the "Five Eyes" intelligence sharing alliance, along with the United States, Australia, New Zealand, and the outgoing EU member state UK, retains its EU adequacy for data transfers. The UK is not currently subject to adequacy requirements because it is still an EU member state, and a bill to transpose the GDPR into British law is currently making its way through the UK Parliament. However, the European Court of Justice has ruled that the UK's sweeping new surveillance law is in breach of EU law. It remains to be seen whether UK surveillance law or any of the complex difficulties associated with the impending British withdrawal from the EU will impede data flows across the English Channel in the long term.

Furthermore, although Canada's EU adequacy means data flows from the EU are unrestricted, this does not mean there are no major differences in data protection policy. For example, the incoming GDPR will introduce restrictions on algorithmic decision-making that do not exist in Canada, such as the right to explanation.[178]

Regulatory Environment

There is little transatlantic regulatory coordination with specific regard to ICT, but the importance of ICT to transatlantic trade nevertheless makes it a major factor in trade policy. The High-Level Regulatory Cooperation Forum is intended to establish cooperation between the EU and the United States on developing "better and more compatible" rules, but it has not published any reports of meetings since 2014, amid negotiations for the Transatlantic Trade and Investment Partnership (TTIP), a proposed trade agreement between the EU and the United States.[179] Those negotiations have themselves stalled due to political resistance on both sides of the Atlantic. Meanwhile, the Transatlantic Economic Council (TEC), which has not met at ministerial level since the start of TTIP negotiations (nor since those negotiations stopped) but continues to meet at the technical level, includes in its mission statement the reduction of regulatory barriers between the EU and the United States, including with regard to ICT.[180]

The EU, the United States, and Canada are all party to the WTO's Information Technology Agreement (ITA), which commits them to abolish tariffs on ICT products. However, some ICT tariffs and taxes nevertheless persist in the three markets, although they are far lower than in countries that have not signed the ITA.[181] The more recent CETA further eliminates most other tariffs between the EU and Canada. Tariffs aside, the differences in intellectual property and data protection rules between the three markets add up to very different regulatory environments for ICT.

Moreover, political pressures in the EU and the United States threaten to create a regulatory environment that is less conducive to transatlantic ICT cooperation than the one in place today. For example, senior European policymakers such as Günther Oettinger and Sigmar Gabriel have called for European "digital sovereignty" or "digital independence" from U.S. "digital imperialism," and have expressed a desire to replace U.S. Internet platforms—such as for search and social media—with European ones.[182] Such protectionist sentiments are not only, by definition, unconducive to transatlantic ICT cooperation, they also threaten to inhibit genuine competition and innovation, by encouraging European firms to merely emulate the international firms they would be protected from, rather than compete with them by doing something new. The new U.S. administration led by President Donald Trump, meanwhile, is far less enthusiastic about international trade agreements than its predecessors, and has brought forward protectionist policies such as "Buy American, Hire American."[183] This type of political pressure further limits the feasibility of improved transatlantic cooperation in ICT during the next few years.

Government Support for Digital Innovation

Canada-EU cooperation on science and technology is institutionalized via the Agreement for Scientific and Technological Cooperation between the EU and Canada, which was signed in 1996 and remains in force.[184] The agreement committed both parties to funding science and technology, and established the Joint Science and Technology Cooperation Committee (JSTCC), which is responsible for making recommendations to Canada and the EU with regard to supporting, among other things, information technologies, communications technologies and medical and health research. Canadian organizations can also participate in Horizon 2020, the EU's current flagship funding resource for research and innovation. As of October 2016, Canadian participants had received €2.7 million through Horizon 2020, and contributed €11.1 million.[185]

The European Union and the United States later signed similar agreements. They signed the Agreement for Scientific and Technological Cooperation in 1998, and extended it in 2009 and 2014.[186] In October 2016, the European Commission and the United States signed an agreement that would allow U.S. organizations to participate in Horizon 2020 as well.[187] The EU and the United States also have a memorandum of understanding (MOU) committing them to cooperation on development of e-health systems, and have published a joint "roadmap" for development of e-health technologies, skills, and services on both sides of the Atlantic.[188]

Canada and the United States, along with the European G8 country members (France, Germany, Italy, and the UK), are signers to the G8 Open Data Charter, the first global commitment to open data.

Canada, the EU, and the United States have a number of collaborative initiatives on data. With regards to open data, Canada and the United States, along with the European G8 country members (France, Germany, Italy, and the UK), are signers to the G8 Open Data Charter, the first global commitment to open data.[189]

Canada and the United States are also part of the Open Government Partnership (OGP), an international forum for creating more open and accountable governments, including through the use of ICT. The EU is not a direct participant in the OGP, but many EU member states participate.[190] The EU and the United States also cooperate on the development of common, interoperable standards for open data. This collaboration includes the development of a shared open data library, which establishes relationships between relevant European and American datasets and allows researchers to browse and combine them, in order to support transparency, research, and innovation on both sides of the Atlantic.[191]

In addition, the Research Data Alliance is a program jointly funded by the European Commission, the U.S. National Science Foundation and National Institute of Standards and Technology, and the Australian Department of Innovation. The purpose of the program is to improve how research data is shared across disciplines by establishing common data infrastructures and other methods for solving data complexity.

IMPACT OF ICT POLICY ON TRANSATLANTIC RESEARCH AND INNOVATION

Technology has changed the ways that companies of all sizes innovate. Innovation is now commonly a cross-border, round-the-clock process, with product design and development

offices spread across multiple time zones, all working on developing new products and services. At the same time, innovation is moving from an in-house, intra-company model to a global, collaborative "open innovation" model based on partnerships with other companies, universities, and research institutions.[192] Companies are finding this new, collaborative approach to innovation to be the fastest, most productive way to accelerate the development of new products and services across markets.[193] This means data, design files, project management systems, video conferencing, and more, need to flow seamlessly across borders to support the innovation process itself.

Data Flows

Data is increasingly the source of innovation. The ability to extract actionable, real-time insight from data (such as through data analytics, data mining, and artificial intelligence) is driving value creation across the global economy. The McKinsey Global Institute finds that, over the past decade, added value created by global data flows increased world GDP by at least 10 percent.[194] The global value of international data flows exceeded the value of global merchandise trade for the first time in 2015. TEKES, Finland's Technology and Innovation Agency, estimates that by 2025, half of all value generated in the global economy will be created digitally. Twenty-two percent of global economic output can already be attributed directly to the digital economy, and the continued application of emerging digital technologies—such as cloud computing, data analytics, and the Internet of Things—is expected to increase global GDP by another $2 trillion by 2020. Three-quarters of the value created by data moving across the Internet accrues to traditional industries.[195]

Organizations use data to create better insights, which, in turn, lead to innovation. Businesses use data to enhance research and development, develop new products and services, create new production or delivery processes, improve marketing, and establish new organizational and management approaches.[196] Countries that erect barriers to data flows make it harder and more expensive for their companies to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative new goods and services that rely on data. Barriers to data flows mean delays and higher costs in the development of new and innovative goods, as companies may be unable to use their preferred research partners or are forced to use second-choice research partners (if they do so at all). Local data storage requirements—also known as data localization—undermine the ability of companies, such as Procter & Gamble (P&G), that use global "open innovation" platforms to facilitate collaboration among firms, universities, and other research organizations to drive innovation.[197]

Smart Manufacturing

Canada, the EU, and the United States all are investing in smart manufacturing (also known as "Industry 4.0" in Europe), which refers to the application of information and communications technologies to modern manufacturing processes.[198] The digitalization of manufacturing will transform how products are designed, manufactured, used, and serviced post-sale as much as it will transform the operations, processes, and energy footprint of

factories and the management of supply chains. ICT-enabled smart manufacturing is expected to increase global manufacturing productivity by up to 25 percent, producing $1.8 trillion in global economic value by 2025. Europe is investing heavily in smart manufacturing. The EU's Horizon 2020 program plans to allocate €17 billion for "leadership in deploying six key enabling and industrial technologies," such as advanced manufacturing, by 2020, including a total of €7 billion for a "Factories of the Future" public-private partnership to develop the blueprints for smarter manufacturing.[199] The United States is investing in smart manufacturing through its Manufacturing USA network as well as through its National Institute of Standards and Technology (NIST). Canada's Advanced Manufacturing Fund provides CAD$200-million to help Canadian manufacturers adopt smart manufacturing techniques, and it is supported by Canadian Manufactures & Exporters (CME) SMART Programs that have provided direct funding to over 1,400 smart manufacturing projects in Canada.[200]

Challenges in International Research Grants

A number of U.S. institutions that have been successful in applying for Horizon 2020 grants have nevertheless turned them down and refused to sign the grant agreement. For some of these institutions, the main reason was the administrative burden required to abide by the current Horizon 2020 grant regulations. One major example is the financial reporting rules, which require line-by-line data entry of individual expenses for each grant in a specific online portal. For a U.S. institution that is accustomed to U.S. federal financial reporting, which generally accepts a standard invoice, the Horizon 2020 financial reporting regulation seems unnecessarily and expensively burdensome.

While Horizon 2020 has a whole set of fellowships and grants, such as Maria-Skłodowska Curie Awards and the prestigious European Research Council (ERC) grants, that encourage Europeans to engage in research in different countries' institutions, including the United States, there is no equivalent set of fellowships and grants among U.S. federal agencies, and certainly nothing that is considered a "flagship" mobility scheme that encourages U.S. researchers to have an equivalent experience in a different country. Creating a fellowship scheme like this among U.S. federal agencies, or better yet, a joint fellowship scheme to be shared among all U.S. federal agencies, would do much to encourage U.S. researchers to engage in research activities in partnership with European researchers.

Finally, whereas many European research institutions and agencies recognize that transnational research partnerships are far more successful at generating results and publications that are more widely cited, this is still relatively unknown among U.S. and even some Canadian institutions. As such, few U.S. institutions incentivize their researchers to engage in international research partnerships. In contrast, European, some Canadian, and Asian institutions have financial incentives for their researchers to do just that.

Distinctions in data protection regimes and their impact on innovation

A key difference between Canada, the EU, and the United States is how each ensures data protection and privacy. U.S. law does not generally limit where personal data is transferred, but stipulates that the company transferring the data protect the data according to U.S. law, wherever it is stored. U.S. data protection policy focuses on giving consumers control of their privacy settings in order to leave open greater space for business model experimentation. On the other hand, the sectoral approach of U.S. privacy law means enterprises that compete in multiple sectors have to understand and respond to multiple different directives, and this can also make it more difficult for companies from other nations to understand the variety and complexity of America's sector-based privacy laws. By contrast, Canadian and European data protection law apply generally, to data processing in all business sectors. The GDPR will give the EU by far the most restrictive data protection regime of the three markets.

To support cross-border research and development, companies participating in pre-competitive research should be able to freely transfer ownership and access rights for IP to affiliates across and between the EU, the United States, and Canada.

The highly complex GDPR may require the assignment of 75,000 or more data protection officers for businesses to comply with the regulation's myriad requirements.[201] The GDPR will add significant costs that may actually harm digital innovators operating in the EU. One study from the University of Milan Biocca, Ca' Foscari University Venice, and the Denver-based Analysis Group estimated that if the data protection officer provisions of the EU regulation are implemented as written, it would cost each effected European small and medium-sized enterprise as much as €7,200 in additional compliance costs per year.[202] The Lisbon Council argues GDPR compliance costs "would suppress jobs in some sectors, reducing employment by as much as 0.6% in particularly heavy hit industry."[203] On the other hand, as noted earlier in this report, Article 20 of the GDPR confers a new right to data portability. There's no equivalent rule in the United States or Canada, but provided the legal guidance is clear, data portability could boost competition between firms by making it easier for companies to get their hands on pre-existing customer data. On the other hand, complex data portability requests could incur large costs.[204]

RECOMMENDATIONS

The objective for improving transatlantic ICT cooperation should not be to eliminate policy differences—not least because that is politically impossible. The goal should be to develop measures that acknowledge differences and establish as much common ground as possible for cooperation that maximizes the economic benefits of ICT innovation for Canada, the EU, and the United States.

Intellectual Property

Support the free movement of knowledge

To support cross-border research and development, companies participating in pre-competitive research should be able to freely transfer ownership and access rights for IP to affiliates across and between the EU, the United States, and Canada. There should also be more flexible transfers of IP among joint venture partners on either side of the Atlantic.[205] This will encourage European, Canadian and American firms to invest in innovation across the Atlantic and will support transatlantic collaboration in R&D programs.

Protect trade secrets on both sides of the Atlantic

Large differences in the protection of trade secrets are a barrier for transatlantic trade in ICT. In the EU, member states offer varying protection in a mixture of civil and criminal laws. This makes it complicated and expensive for firms to take action when their secrets are stolen, which can deter investment.[206] In the United States, the Uniform Trade Secrets Act (UTSA), which states are free to enact as they see fit, facilitates the harmonization of state law on trade secrets. As of 2013, 47 of 50 U.S. states have adopted UTSA, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.[207]

The transatlantic partners should agree to establish a common definition for trade secrets: any information that has economic value (actual or potential), is not generally known to the public, and that the owner has taken reasonable measures to keep private. They should also commit to strong legal safeguards that deter malicious misappropriation of trade secrets, particularly when done to aid a foreign government.[208]

Data Protection

Keep data protection rules simple

Complex data-protection laws create pointless work, destroy productive jobs, stifle innovation, raise consumer costs, and create a difficult regulatory environment for international trade in data-driven services. For example, the GDPR creates complex data handling requirements which will require companies to hire more workers to handle. In addition, they will likely divert money away from investments that would create more productive jobs and benefit customers through lower prices and better product features—including privacy-enhancing ones.[209]

Overly restrictive data protection rules also limit the ability of enterprises to improve productivity.[210] For example, less effective advertising reduces available revenue for websites and can cripple the growth of useful services. All countries should attempt to make privacy legislation straightforward, so that Canadian, European, U.S. firms know what they must do in order to comply with the law in each market. In addition, Canada, the EU, and the United States should prevent their respective provinces, member states, and states, and from obstructing the development of a digital single marketplace with additional regulations, especially more complex data protection regulations that go beyond supposedly common sets of rules, as these drastically complicate the cross-border regulatory environment.[211]

Do not impose needless restrictions on artificial intelligence

The GDPR's right to explanation will impose significant costs on companies using AI and algorithmic decision making, as explaining an individual decision requires considerable work by expert auditors. Furthermore, this kind of auditing may not even be sufficient to determine whether inappropriate characteristics—such as ethnicity or religion—were the basis of any given decision, because the markers for such things can be extremely subtle, and subject to regional nuances: just because an algorithm picks up on them does not mean the auditors attempting to explain the decision will. Oversight of the outcomes of

algorithmic decisions in aggregate is a more effective means of identifying such biases because this allows auditors to identify correlations with protected characteristics, even if the precise markers for them are unknown.[212]

Support the free flow of data

Requiring data to be stored in a particular location does not enhance data protection, but it does inhibit competition between service providers in different countries, which stifles innovation and raises costs in data-driven services. Proper encryption of data, combined with legal accountability for multinational firms in the markets where they operate, is a far more effective means of protecting data in the global economy.[213]

EU data protection law imposes a general prohibition on foreign transfers of EU personal data, except under pre-defined circumstances that ensure equal protection abroad. But in any case, businesses that operate in the EU (whether EU-based or foreign) remain responsible under EU law for what they do with data collected in the EU, regardless of where they actually store it. U.S. companies in Europe cannot dodge their legal obligations simply by storing EU personal data outside the EU. Moreover, storing it in the EU does not protect it from adversaries abroad: that is a question of proper security.[214]

Canada, the EU, and the United States should propose a "Data Services Agreement" to WTO member states, to protect cross-border data flows and prevent signatory countries from creating barriers to them.[215]

Support strong encryption

The key to strong international data protection is proper encryption, not data localization. But policymakers on both sides of the Atlantic have proposed weakening encryption in order to ensure access for law enforcement and intelligence agencies. This undermines cybersecurity for law-abiding citizens and businesses, exposing them to cyber threats, without taking strong encryption out of the hands of criminals and terrorists. It would also undermine trust between countries trading data-driven services, damaging the transatlantic data economy. Canada, the EU, the United States should agree not to pass laws that weaken, undermine, restrict or control the ability of businesses and individuals to use the strongest possible encryption available.[216]

Establish A "Geneva Convention on the Status of Data"

Canada, the EU, and the United States, along with their trading partners, should work together on developing multilateral legal standards for surveillance and government access to data, for transparency in the treatment of international data, and for resolving questions of jurisdiction and conflicting laws—a "Geneva Convention on the Status of Data," so to speak. This would help to build trust in the international data economy while simultaneously allowing countries to find ways to address law enforcement challenges, such as slowness of accessing vital evidence via Mutual Legal Assistance Treaties (MLATs).[217]

Regulatory Environment

Establish a framework to resolve conflicting digital regulations

Different regulatory attitudes to the global internet can lead to legal conflicts between countries. There should be a framework for addressing such conflicts when they arise, because they can put companies in a position where complying with the law in one country means breaking the law in another. For example, the French authorities' extraterritorial interpretation of the EU's "right to be forgotten" overlooks the fact that the "right to be forgotten" could conflict with other legal protections in other countries, particularly those for freedom of speech.[218]

The transatlantic partners should agree on a framework that balances mutual respect for sovereignty with respect for the global nature of the internet, taking into account what, who, or where the intended targets of any proposed policy are, relevant international organizations (such as ICANN), existing international agreements, and the possibility for new ones. In the absence of cross-border consensus on a particular policy—such as the "right to be forgotten"—countries determined to implement digital regulations should ensure they do not impact people outside their jurisdiction.

Stop protectionist ICT procurement policies

Canada, the EU, and the United States, should agree to regulations against protectionism in ICT procurement (such as data localization, not just in general law, but also in procurement rules and guidelines), including at the level of their respective member states, states, and provinces, and each should encourage bids for tenders from firms based in the other two markets.

Government Support for Digital Innovation

Collaborate on voluntary, transparent, consensus-based, market-led standards

Standards development is an important area for transatlantic cooperation. For example, European policymakers are working towards European standards for new ICT, including the Internet of Things.[219] But rather than particular standards for each market, the EU, Canada, and the United States should work together to support interoperable standards that work across all three markets. While supporting research into voluntary standards is worthwhile in itself, policymakers should be wary of creating national or regional standards that diverge from international equivalents.

To demonstrate why, the power grid and television serve as a case in point. North America, mainland Europe, and the UK & Ireland, operate three different standards for electrical outlets and two different standards for power output, A/C frequency, and "standard definition" television. Consumers and manufacturers incur additional costs to overcome these differences, such as converter plugs, transformer circuits, and PAL-NTSC switches. If possible, it would be better to avoid replicating such unnecessary costs in new technologies.

Public-sector deployments of the Internet of Things should have common standards to be interoperable, and these standards should form part of national strategies for investment in

the Internet of Things.[220] However, the development of common standards should not occur within isolated national or regional environments, like the EU, the United States, or Canada. They should be developed internationally, in order to ease transatlantic trade and cooperation in the Internet of Things. The three parties should publish joint impact assessments for proposed regulations and standards.

Establish a tripartite partnership for science and technology research

With EU-U.S. and Canada-EU ICT cooperation already established, the three entities should pull bilateral institutions together to establish a tripartite partnership for science and technology research and innovation. Such multilateral R&D cooperation could draw on the different strengths and knowledge bases of universities and research institutions in Canada, the EU, and the United States.[221]

For example, the three partners could establish a platform for sharing information from research projects funded by Horizon 2020, or the U.S. National Science Foundation and National Institutes of Health. Canada, the EU, and the United States should also each set a target of ten percent of government-funded research programs involving partners from the other two, in order to boost cooperation between research organizations and companies in the three markets.[222]

Boost cooperation between regional bodies

Transatlantic ICT cooperation should go beyond policymakers in Brussels, Ottawa, and Washington: There should also be cooperation involving Canadian provinces, European countries, and U.S. states, not to mention German states, Spanish autonomous communities, and Bulgarian oblasts. For example, the development of smart cities will be significantly improved if similar cities in all three regions collaborate and share best practices so they can learn from one another.

Regulators operating at the middle or lower tiers of the administrative divisions of the EU, the United States, and Canada should look for opportunities to build coalitions with their transatlantic counterparts, independently of top-tier initiatives.

Create a common position on text and data mining's place in copyright law

Text and data mining is an exciting new research tool that supports the knowledge economy. The use of text and data mining technologies on lawfully accessed content, provided it does not result in any unauthorized redistribution of copyright-protected materials, should always fall within the definition of "fair use" or "fair dealing." Canada, the European Union, and the United States should agree on a common position on this matter in order to give all researchers, whether non-profit or commercial, the confidence to use text and data mining across borders without fear of legal repercussions.[223]

Help start-ups grow

Start-up businesses do not want to remain start-ups forever, and they should be encouraged to grow and compete. Besides grant schemes that help get them off the ground, tech start-ups need access to longer-term private finance and a regulatory environment that allows them not just to start, but to grow. Policymakers in the three transatlantic partners, at all

administrative tiers, should share their experiences in order to assemble a transatlantic policy framework for opening the way for growing start-ups, and include the most effective measures from across Europe and North America.

Promote tech literacy among legislators

MPs, MEPs, representatives, and senators, will have a better chance of drawing up good regulations if they understand properly what they are regulating. Legislators in Canada, the EU, and the United States, should work with experts in academia, industry, and civil society to enhance their understanding of ICT and the impact of regulations upon it.

Review major policy issues together

Growing the digital economy and increasing competitiveness is often as much about reviewing existing policies as it is about creating new ones. The transatlantic partners should review what policies they have on the books, compare them with one another, and work together to overhaul transatlantic policy to support the most mutually beneficial outcomes. Canada, the EU, and the United States should also work together on emerging and future issues, such as tech-driven economic phenomena in the labor market.

Growing the digital economy and increasing competitiveness is often as much about reviewing existing policies as it is about creating new ones.

Revive and revise the Transatlantic Trade and Investment Partnership (TTIP)

The EU and the United States should work to revive TTIP negotiations, which were halted in September 2016, when regulators could not overcome political sensitivities. But the success of CETA emphasizes that political shifts on either side of the Atlantic do not undermine the fundamental case for lasting trade agreements that build on and improve transatlantic cooperation, including in the realm of ICT. Transatlantic trade is to the benefit of Europe and North America regardless of political sensitivities, and it is the responsibility of those who hold office to explain these benefits to the electorate, and to be transparent in how they pursue them.

To do this, TTIP needs to address modern trade issues such as data flows and digital trade, which has proven hard for the European Union to recognize and protect within the scope of its trade negotiations. As with the Trans Pacific Partnership, TTIP negotiators should look to create an interoperable digital space for goods, services, and data, including provisions that explicitly prohibit unnecessary and restrictive measures that force companies to store data locally or use local computing facilities. These provisions are needed to protect the distributed nature of the Internet and the essential role that data flows play in today's modern economy.

However, the European Union has struggled to present a united position on this due to internal disagreement among its members (some of which, such as France and Germany, are prone to supporting data localization policies).[224] Whether a revived TTIP results in a revised agenda, the critical role of data in the trade relationship means that any TTIP agreement needs to address these types of digital trade issues for it to be of value to ICT sectors on both sides of the Atlantic.

ENDNOTES

1. These four topics were chosen by the DISCOVERY Transatlantic ICT Forum following its workshop in Brussels in October 2016.

2. British North America Act, 1867 - Enactment No. 1, (Government of Canada, Last Updated January 7, 2017), http://canada.justice.gc.ca/eng/rp-pr/csj-sjc/constitution/lawreg-loireg/p1t13.html.

3. Patent Act, R.S.C., 1985, c. P-4, http://www.laws-lois.justice.gc.ca/PDF/P-4.pdf.

4. Government of Canada "A Guide to Patents: Patents Defined," https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr03652.html#patentsDefined.

5. "A Guide to Patents: Patents Defined," (Government of Canada, last updated June 30, 2017), accessed January 6, 2018, https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr03652.html#patentsDefined.

6. Keith Bird, "Significant Differences Between Canadian and American Patent Law," *InBrief,* Summer 2008, McMillan, http://www.mcmillan.ca/Significant-Differences-Between-Canadian-and-American-Patent-Law.

7. Florence E Legere, "Patent litigation in Canada: overview" *Thomson Reuters Practical Law*, February 1, 2017, https://content.next.westlaw.com/5-621-1843?transitionType=Default&contextData=(sc.Default)&__lrTS=20170508195415737&firstPage=true.

8. Ibid.

9. "History of Copyright in Canada," (Government of Canada, Last Modified October 26, 2016), http://canada.pch.gc.ca/eng/1454685408763.

10. "A Guide to Copyright," (Government of Canada, Last Updated November 15, 2016), https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr02281.html.

11. Ibid.

12. P Schabas, I Fischer, and C. DiMatteo, "Canada's Copyright Modernization Act: A Delicate Rebalancing of Interests", *Media Law Resource Center,* 2013, Issue 2, http://www.medialaw.org/component/k2/item/1820-canada%E2%80%99s-copyright-modernization-act-a-delicate-rebalancing-of-interests.

13. G Robertson, "Unlocking Bill C-11: What are digital locks, and why should you care?", *The Fulcrum*, February 8, 2012, http://thefulcrum.ca/news/unlocking-bill-c-11-what-are-digital-locks-and-why-should-you-care/.

14. Copyright Modernization Act, S.C. 2012, c. 20., 41st Canadian Parliament.

15. G Robertson, "Unlocking Bill C-11: What are digital locks, and why should you care?", *The Fulcrum*, February 8, 2012, http://thefulcrum.ca/news/unlocking-bill-c-11-what-are-digital-locks-and-why-should-you-care/.

16. Copyright Modernization Act, S.C. 2012, c. 20., 41st Canadian Parliament (2012).

17. Trade Marks Act (R.S.C., 1985, c. T-13) (consolidated version, status as at January 15, 2011) http://www.wipo.int/wipolex/en/details.jsp?id=8561.

18. "A guide to trademarks," (Government of Canada), http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr02360.html?Open&wt_src=cipo-tm-main&wt_cxt=learn.

19. REGULATION (EU) No 1257/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:361:0001:0008:EN:PDF.

    COUNCIL REGULATION (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:361:0089:0092:EN:PDF.

20. Agreement on a Unified Patent Court (UPC) Signed 19/02/2013: Brussels, OJEU reference: C 175 (20/06/2013), http://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=OJ:C:2013:175:FULL&from=EN.

21. DIRECTIVE 2001/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN.

22. DIRECTIVE 2006/115/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0115&from=EN.

23. DIRECTIVE 2009/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2009 on the legal protection of computer programs (Codified version), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF.

24. COUNCIL DIRECTIVE 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0083:EN:PDF.

25. DIRECTIVE 2006/116/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2006 on the term of protection of copyright and certain related rights (codified version), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:372:0012:0018:EN:PDF;

    DIRECTIVE 2011/77/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:265:0001:0005:EN:PDF.

26. Directive 2011/77/EU.

27. Directive 2006/116/EC.

28. DIRECTIVE 2014/26/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0026&from=EN.

29. DIRECTIVE 96/191/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 1996 on the legal protection of databases, http://eur-lex.europa.eu/lexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:PDF.

30. DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN.

31. Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, (European Commission (September 9, 2016), https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market.

32. DRAFT REPORT on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, (Committee on Legal Affairs, March 10, 2017), http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.094&format=PDF&language=EN&secondRef=01; "Legislative Train Schedule—Modernisation of European Copyright Rules: Directive on Copyright in the Digital Single Market," (European Commission, last updated December 20, 2017), accessed January 9 2017, http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-directive-on-copyright-in-the-digital-single-market.

33. European Commission (2016, September 9) Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market.

34. DRAFT REPORT on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, (Committee on Legal Affairs, March 10, 2017), http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.094&format=PDF&language=EN&secondRef=01.

35. "A digital agreement," (El País March 24, 2017), http://elpais.com/elpais/2017/03/24/inenglish/1490355715_551697.html.

    Elsa García de Blas, "Google News to start excluding all Spanish media from service," *El País,* December 11, 2014, http://elpais.com/elpais/2014/12/11/inenglish/1418289854_162105.html.

36. DRAFT REPORT on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, (Committee on Legal Affairs, March 10, 2017),

http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.094&format=PDF&language=EN&secondRef=01.

37. "Public Consultation on the Protection Against Misappropriation of Trade Secrets and Confidential Business Information: Summary of Responses," (European Commission, July 1, 2013), http://ec.europa.eu/DocsRoom/documents/14900.

38. U.S. Patent Act 1952, https://www.law.cornell.edu/patent/patent.overview.html.

39. U.S. Code: Title 35-Patents, *http://uscode.house.gov/browse/prelim@title35&edition=prelim.*

40. U.S. Code: Title 17-Copyrights, Chapter 1-8 and 10-12, http://uscode.house.gov/browse/prelim@title17&edition=prelim.

41. U.S. Code: Title 17-Copyrights, Chapter 9, http://uscode.house.gov/browse/prelim@title17&edition=prelim; U.S. Copyright Office (1998, December) The Digital Millennium Copyright Act 1998: U.S. Copyright Office Summary, https://www.copyright.gov/legislation/dmca.pdf.

42. U.S. Code: Title 15-Commerce and Trade §1051 et seq, http://uscode.house.gov/browse/prelim@title15/chapter22&edition=prelim.

43. H.R. 6071: Trademark Counterfeiting Act of 1984, https://www.govtrack.us/congress/bills/98/hr6071.

44. "State Trademark Information Links," (UPTO, February 10, 2010) Last updated January 10, 2017, https://www.uspto.gov/trademarks-getting-started/process-overview/state-trademark-information-links.

45. U.S. Code: Title 18, chapter 90, § 1831–1839, http://uscode.house.gov/browse/prelim@title18/part1/chapter90&edition=prelim.

46. "Intellectual Property" (United States International Trade Commission, Last updated January 3, 2018), accessed January 4, 2018, https://www.usitc.gov/intellectual_property.htm.

47. Personal Information Protection and Electronic Documents Act, S.C., c. 5, 36th Canadian Parliament (2000).

48. Ibid.

49. Ibid.

50. "What We Do," (Office of the Privacy Commissioner of Canada, Last Updated May 2014), https://www.priv.gc.ca/en/about-the-opc/what-we-do/.

51. "Overview of privacy legislation in Canada," (Office of the privacy Commissioner of Canada, Last Updated May 2014), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

52. Ibid.

53. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2012/C 326/02) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

54. TREATY OF LISBON Amending the Treaty of European Union and the Treaty Establishing the European Community (2007/C 306/01) http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC_19.

55. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 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) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

56. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:PDF.

57. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI," (Center for Data Innovation, 2018), http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

58. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI," (Center for Data Innovation, 2018), http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

59. JUDGMENT OF THE COURT (Grand Chamber) 13 May 2014, Google Spain SL,

Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5b6c0ef0cfcc34664af65824af1275c09.e34KaxiLc3eQc40LaxqMbN4OaNmNe0?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=433471.

60. Daniel Castro, and Alan McQuinn, "France, you do not own the internet" *Computerworld,* January 11, 2017, http://www.computerworld.com/article/3156296/internet/france-you-do-not-own-the-internet.html.

61. EU-US Privacy Shield agreement, full text published by IAPP: https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_full_text.pdf.pdf.

62. DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:PDF; Proposal for a Regulation on Privacy and Electronic Communications, (European Commission, January 10, 2017), https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

63. Nick Wallace, "New EU Cookie Law Hurts Ad-Supported Industries (Like Journalism) Without Offering More Privacy," (Center for Data Innovation, March 20, 2017) https://www.datainnovation.org/2017/03/eu-policymakers-should-overcome-their-fear-of-cookies/.

64. Nick Wallace and Daniel Castro, "e-Privacy law would penalise sites who block ad-blockers," *EUobserver,* December 22, 2017, accessed January 9, 2018, https://euobserver.com/digital/140397.

65. U.S. Department of Health, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

66. Former Hospital Employee Indicted for HIPAA Violations, (U.S. Department of Justice, July 3, 2014), https://www.justice.gov/usao-edtx/pr/former-hospital-employee-indicted-criminal-hipaa-violations.

67. Gramm-Leach-Bliley Act 113 Stat. 1338 Public Law 106-102-Nov. 12, 1999, https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf.

68. "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," (Federal Trade Commission, 2002) https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.

69. "State Insurance Regulation," (NAIC), http://www.naic.org/documents/consumer_state_reg_brief.pdf; https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

70. U.S. Code: Title 15-Commerce and Trade § 1681, http://uscode.house.gov/browse/prelim@title15/chapter22&edition=prelim.

71. "FCRA Summary of Rights," (Equifax, 2017), https://www.equifax.com/privacy/fcra.

72. Tricolor Auto Acceptance LLC, FTC Matter no. 142 3037 September 17, 2015, https://www.ftc.gov/enforcement/cases-proceedings/142-3073/tricolor-auto-acceptance-llc; https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/fair-credit-reporting-regulation-v/.

73. 47 U.S.C. § 222 (1943), https://www.law.cornell.edu/uscode/text/47/222.

74. Brian Naylor, "Congress Overturns Internet Privacy Regulation," *NPR*, March 28, 2017, https://www.npr.org/2017/03/28/521831393/congress-overturns-internet-privacy-regulation.

75. 18 U.S.C. § 2710 (2002), http://uscode.house.gov/browse/prelim@title18/part1&edition=prelim.

76. Fixing America's Surface Transportation Act, Public Law 114-94 (2015), 114th Cong. (2015). The DPA was included as part of the FAST Act, which was signed into law in December 2015.

77. Children's Online Privacy Protection Rule ("COPPA") 15 U.S.C. §6501-6505, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

78. Family and Education Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn.

79. Ibid.

80. Google, Inc., In the Matter Of FTC Matter No. 102 3136, https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.

81. Federal Trade Commission, "Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser," (Federal Trade Commission, August 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

82. "Security Breach Notification Laws," (National Conference of State Legislators, December 4, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

83. K.D. Harris, "California Data Breach Report" (California Department of Justice, February 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

84. *Doing Business 2017,* (World Bank, October 25, 2016) http://www.doingbusiness.org/reports/global-reports/doing-business-2017.

85. Ibid.

86. Ibid.

87. Statutory Instruments Act, http://laws-lois.justice.gc.ca/eng/acts/S-22/.

88. "The nature of regulations," *The Canadian Legal Research and Writing Guide*, accessed May 17, 2017, http://legalresearch.org/statutory/federal-statutes/regulations/.

89. "Ensuring Truth in Advertising," (Competition Bureau, November 5, 2015), accessed May 17, 2017, http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00529.html.

90. "Competition Bureau takes action against alleged false or misleading car rental advertising," (Competition Bureau, March 11, 2015), http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03885.html.

91. "Archived - CRTC Chief Compliance and Enforcement Officer issues $1.1 million penalty to Compu-Finder for spamming Canadians," (Canadian Radio-television and Telecommunication Commission, March 5, 2015), http://news.gc.ca/web/article-en.do?nid=944159.

92. "About the DAAC," (Digital Advertising Alliance of Canada), Accessed May 17, 2017, http://youradchoices.ca/about-the-daac/.

93. "Canadian Privacy Regulators Launch Research to Examine Advertising Compliance," (TRUSTe, January 16, 2015), http://www.truste.com/blog/2015/01/16/canadian-privacy-regulators-launch-research-advertising-compliance/.

94. "Consumer protection legislation in Canada" (Government of Canada), accessed May 17, 2017, https://www.ic.gc.ca/eic/site/icgc.nsf/eng/07554.html.

95. "OSC Highlights Potential Securities Law Requirements for Businesses Using Distributed Ledger Technologies," (Ontario Securities Commission, March 8, 2017), http://www.osc.gov.on.ca/en/NewsEvents_nr_20170308_osc-highlights-potential-securities-law-requirements.htm.

96. "Regional Profile 2017: European Union," *Doing Business 2017*, (World Bank, October 25, 2017) *http://www.doingbusiness.org/reports/~/media/WBG/DoingBusiness/Documents/Profiles/Regional/DB2017/EU.pdf* .

97. *Doing Business 2017,* (World Bank, October 25, 2016) http://www.doingbusiness.org/reports/global-reports/doing-business-2017.

98. *CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION - PART ONE - PRINCIPLES - TITLE I - CATEGORIES AND AREAS OF UNION COMPETENCE - Article 3 (C 236/1)* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E003.

99. *CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION - PART ONE - PRINCIPLES - TITLE I - CATEGORIES AND AREAS OF UNION COMPETENCE - Article 4* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E004.

100. *CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION - PART ONE - PRINCIPLES - TITLE I - CATEGORIES AND AREAS OF UNION COMPETENCE - Article 6* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E006.

101. *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union* (2012/C 326/01) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2012:326:FULL&from=EN.

102. *Doing Business 2017,* (World Bank, October 25, 2016) http://www.doingbusiness.org/reports/global-reports/doing-business-2017.

103. 5 U.S. Code Chapter 5 – Administrative Procedure. https://www.law.cornell.edu/uscode/text/5/part-I/chapter-5.

104. Gunningham, N and Rees, J (1997, October) "Industry Self-Regulation: An Institutional Perspective," *Law & Policy* Vol. 19, No. 4.

105. Anil K. Gupta and Lawrence J. Lad (1983), "Industry Self-Regulation: An Economic, Organizational, and Political Analysis," *The Academy of Management Review* 8, no. 3, p 417.

106. "About NERC," (North American Electric Reliability Corporation), accessed April 26, 2017, http://www.nerc.com/AboutNERC/Pages/default.aspx.

107. "About us," (Marine Stewardship Council), https://www.msc.org/about-us.

108. Christopher Marsden (2011), *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace,* Cambridge: Cambridge University Press.

109. *Voluntary Best Practices for UAS Privacy, Transparency and Accountability,* (NTIA, May 18, 2016) https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

110. *Investment and Securities Account Restrictions Under FINRA's Code of Conduct,* (Financial Industry Regulatory Authority), http://www.finra.org/sites/default/files/Corporate/p123543.pdf.

111. *Federal Automated Vehicles Policy,* (Department of Transportation, September 2016) https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016 ; *Unmanned Aircraft Systems,* (Dept. Transportation, updated March 31, 2017), https://www.faa.gov/uas/.

112. "OCC Issues Draft Licensing Manual Supplement for Evaluating Charter Applications From Financial Technology Companies," (Office of the Controller of the Currency, March 15, 2017), https://www.occ.treas.gov/news-issuances/news-releases/2017/nr-occ-2017-31.html

113. "Research and Development Expenditure 1996 - 2014 (% of GDP)," (World Bank), accessed May 4, 2017, http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=CA.

114. "About NRC," (National Research Council, May 1, 2017), accessed May 4, 2017, http://www.nrc-cnrc.gc.ca/eng/about/index.html.

115. "Alberta Research Council," (Innovation Alberta, May 5, 2017), http://www.innovationalberta.com/theme.php?themeid=13.

116. For example, see the University of Manitoba Technology Transfer Office: accessed May 4, 2017, http://www.ic.gc.ca/app/ccc/srch/nvgt.do;jsessionid=0001oPE92dZkdVmO9zLxmuinb0O:-99CCU?lang=eng&prtl =1&sbPrtl=&estblmntNo=234567005688&profile=cmpltPrfl&profileId=1921&app=sold&searchNav=F.

117. "The State of Industrial R&D in Canada," (Council of Canadian Academics, 2013), http://www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/research%20and%20develop/ird_fullreporten.pdf.

118. "Claiming SR&ED tax incentives," (Canada Revenue Agency, April 25, 2015), accessed May 5, 2017, http://www.cra-arc.gc.ca/txcrdt/sred-rsde/clmng/clmngsrd-eng.html.

119. Ajay Agrawal, Carlos Rosell, Timothy S. Simcoe, "Do Tax Credits Affect R&D Expenditures by Small Firms? Evidence from Canada," (The National Bureau of Economic Research, October, 2014), accessed May 5, 2017, http://www.nber.org/papers/w20615.

120. "The State of Industrial R&D in Canada," (Council of Canadian Academics 2013), http://www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/research%20and%20develop/ird_fullreporten.pdf.

121. "About the Standards Council of Canada," (Standards Council of Canada), accessed May 5, 2017, https://www.scc.ca/en/about-scc.

122. "Participate in committee work—Electronics, information technology and telecommunications," (Standards Council of Canada), accessed May 5, 2017, https://www.scc.ca/standards/get-involved-in-standardization/committees?field_sector_value_i18n=4 ; 122 Standards Council of Canada, "Participate in committee work—Engineering technologies," accessed May 5, 2017, https://www.scc.ca/standards/get-involved-in-standardization/committees?field_sector_value_i18n=3.

123. "CMA Code of Ethics & Standards of Practice," (Canadian Marketing Association), accessed May 5, 2017, https://www.the-cma.org/regulatory/code-of-ethics.

124. "Government announces CIFAR Pan-Canadian Artificial Intelligence Strategy," (Canadian Institute for Advanced Research, March 30, 2017), accessed May 4, 2017, https://www.cifar.ca/assets/government-announces-cifar-pan-canadian-artificial-intelligence-strategy/.

125. Jennifer Robinson, "Aims to produce the world's largest number of deep learning graduates," *University of Toronto News,* March 30, 2017, https://www.utoronto.ca/news/toronto-s-vector-institute-officially-launched.

126. Ibid.

127. *Overview of EU Funds for research and innovation*, (European Commission), http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568327/EPRS_BRI(2015)568327_EN.pdf

128. *Factsheet: Horizon 2020 Budget*, (European Commission) http://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_horizon2020_budget.pdf.

129. "Total GBAORD as a % of total general government expenditure," (Eurostat, gba_nabste).

130. Kenneth Flamm, *Targeting the Computer: Government Support and International Competition*, Washington, DC: Brookings Institution, 1987.

131. "Federal R&D as a Percent of GDP, 1976-2017," *R&D Budget and Policy Program,* (AAAS, 2017), https://www.aaas.org/page/historical-trends-federal-rd; Robert D. Atkinson, *Understanding the U.S. National Innovation* System, (ITIF, June 2014), http://www2.itif.org/2014-understanding-us-innovation-system.pdf.

132. "US R&D Spending at All-Time High, Federal share Reaches Record Low," (American Institute of Physics, November 8, 2016), https://www.aip.org/fyi/2016/us-rd-spending-all-time-high-federal-share-reaches-record-low.

133. Adams Nager, "Trump's Cuts to Federal Science Funding Will Mean Less Industry R&D, Not More," *The Information Technology and Innovation Foundation*, March 17, 2017, https://itif.org/publications/2017/03/17/trumps-cuts-federal-science-funding-will-mean-less-industry-rd-not-more; "FY 2018 R&D Appropriations Dashboard," *American Association for the Advancement of Science,* https://www.aaas.org/news/week-appropriations-house-clears-omnibus-spending-bill, (accessed January 19, 2017).

134. Matt Stepp et al, "Reimaging the National Labs in the 21st Century Innovation Economy," (Information Technology and Innovation Foundation, Center for American Progress, and the Heritage Foundation, June 2013), http://www2.itif.org/2013-turning-the-page.pdf.

135. National Institutes of Health (2014, June 18) "NIH and NSF collaborate to accelerate biomedical research innovations into the marketplace" https://www.nih.gov/news-events/news-releases/nih-nsf-collaborate-accelerate-biomedical-research-innovations-into-marketplace.

136. "Grand Challenge Overview," (DARPA, 2014), http://archive.darpa.mil/grandchallenge04/overview.htm; "The DARPA Grand Challenge: Ten Years Later," (DARPA, March 13, 2014), http://www.darpa.mil/news-events/2014-03-13.

137. Ben Drawbaugh, "Two years of battle between HD DVD and Blu-ray: a retrospective," *Engadget*, February 2, 2008, accessed May 18, 2017, https://www.engadget.com/2008/02/20/two-years-of-battle-between-hd-dvd-and-blu-ray-a-retrospective/.

138. "About ANSI," (American National Standards Institute), accessed May 18, 2017, https://www.ansi.org/about_ansi/overview/overview?menuid=1.

139. Robert D. Atkinson, *Understanding the U.S. National Innovation* System, (ITIF, June 2014), http://www2.itif.org/2014-understanding-us-innovation-system.pdf.

140. "Multistakeholder Process; Internet of Thins (IoT) Security Upgradability and Patching," (National Telecommunications and Information Administration, April 26, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

141. *Framework for Improving Critical Infrastructure Cybersecurity*, (National Institute of Standards and Technology, 2014, February 12), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf; "NIST Cryptographic Standards and Guidelines Developments Process" http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf.

142. "Smart City Challenge," (Department of Transportation, last updated January 20, 2017), https://www.transportation.gov/smartcity.

143. U.S. Department of Transportation, "U.S. Department of Transportation Announces up to $42 Million in Next Generation Connected Vehicle Technologies," press release, September 16, 2015, https://www.transportation.gov/briefing-room/us-department-transportation-announces-42-millionnext-generation-connected-vehicle, (accessed January 1, 2018).

144. "Global City Teams Challenge," (US Ignite), https://www.us-ignite.org/programs/global-city-teams-challenge/.

145. "Global City Teams Challenge," (NIST), https://www.nist.gov/el/cyber-physical-systems/smart-americaglobal-cities.

146. Cheryl Pellerin, "DoD's Silicon Valley Innovation Experiment Begins," *U.S. Department of Defense*, October 29, 2015, https://www.defense.gov/News/Article/Article/626602/dods-silicon-valley-innovation-experiment-begins/.

147. Ash Carter, "The "X" is for Experimental," *U.S. Department of Defense*, Medium, May 11, 2016, https://medium.com/@SecDef/the-x-is-for-experimental-3c9438e76214.

148. "Our process," *In-Q-Tel*, accessed May 18, 2017, https://www.iqt.org/about-iqt/process/.

149. Alex Kostura and Daniel Castro, "Three Types of Public-Private Partnerships That Enable Data Innovation," (Center for Data Innovation, August 1, 2016), https://www.datainnovation.org/2016/08/three-types-of-public-private-partnerships-that-enable-data-innovation/.

150. "U.S. Secretary of Commerce Penny Pritzker Announces New Collaboration to Unleash the Power of NOAA's Data," (Department of Commerce, April 4, 2015), https://www.commerce.gov/news/press-releases/2015/04/us-secretary-commerce-penny-pritzker-announces-new-collaboration-unleash.

151. "Big Data Project," (National Oceanic and Atmospheric Administration), http://www.noaa.gov/big-data-project.

152. "Opportunities for All – the Baker-Polito Strategy and Plan for Making Massachusetts Great Everywhere," (Commonwealth of Massachusetts (December 23, 2015), http://www.mass.gov/hed/docs/eohed/edplan2015.pdf.

153. "IN, MD continue funding innovation," (SSTI, May 4, 2017), accessed May 17, 2017, http://ssti.org/blog/md-continue-funding-innovation.

154. Kurt Nagl, "UM, Michigan Tech Receive $2.2 million in tech transfer grants," *Crain's Detroit Business*, March 2, 2017, accessed May 17, 3017, http://www.crainsdetroit.com/article/20170302/NEWS/170309967/um-michigan-tech-receive-2-2-million-in-tech-transfer-grants.

155. Robert D. Atkinson, *U.S. Corporate Tax Reform: Groupthink or Rational Debate?*, (ITIF, July 2011), http://www.itif.org/files/2011-corporate-tax-reform.pdf.

156. Robert Atkinson *Incentives for Capital Investment and Manufacturing: Hearing on Tax Reform Options Before the Senate Finance Committee*, written testimony, (ITIF, 2012) http://www2.itif.org/2012-senate-finance-manufacturing.pdf.

157. Joe Kennedy, "Assessing U.S. Corporate Tax Reform in an Age of Global Competition," (ITIF, March 2014), http://www2.itif.org/2014-corporate-tax-reform-global-competition.pdf; "Preliminary Details and Analysis of the Tax Cuts and Jobs Act" (Tax Foundation, December 18, 2017), accessed February 14, 2018, https://taxfoundation.org/final-tax-cuts-and-jobs-act-details-analysis/.

158. Kyle Pomerlau and Emily Potovsky, "Corporate Income Tax Rates Around the World, 2016," (Tax Foundation, August 18, 2016), accessed February 14, 2018, https://taxfoundation.org/corporate-income-tax-rates-around-world-2016/.

159. Joe Kennedy and Robert D. Atkinson, "Why Expanding the R&D Tax Credit is Key to Successful Corporate Tax Reform," (Information Technology and Innovation Foundation, July 2017), http://www2.itif.org/2017-rd-tax-credit.pdf?_ga=2.160367229.136445465.1519991855-2011989933.1510846480.

160. "Value Added Tax (VAT) In Canada," *Economy Watch,* June 29, 2010, http://www.economywatch.com/business-and-economy/canada.html; "What is VAT?" (European Commission, Last updated May 3, 2017), http://ec.europa.eu/taxation_customs/business/vat/what-is-vat_en.

161. "Intellectual property rights intensive industries and economic performance in the European Union," (EPO and EUIPO, October 2016), https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/performance_in_the_European_Union/performance_in_the_European_Union_full.pdf.

162. "Intellectual Property and the U.S. Economy: 2016 Update," (ESA and USPTO, September 2016), https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

163. Carmen-Cristina Cîrlig, "Overcoming Transatlantic differences on intellectual property: IPR and the TTIP negotiations," *European Parliament Members Research Service*, July 2014, 140760REV1, page 7, http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140760/LDM_BRI(2014)140760_REV1_EN.pdf.

164. Ibid, page 8.

165. *AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS* (as amended on January 23, 2017), https://www.wto.org/english/docs_e/legal_e/31bis_trips_e.pdf.

166. "THE EU'S FREE TRADE AGREEMENT WITH CANADA AND ITS INTELLECTUAL PROPERTY RIGHTS PROVISIONS." (European Commission, October 18, 2013), http://trade.ec.europa.eu/doclib/docs/2012/august/tradoc_149866.pdf.

COMPREHENSIVE ECONOMIC AND TRADE AGREEMENT (CETA), http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf.

167. *COMPREHENSIVE ECONOMIC AND TRADE AGREEMENT (CETA),* http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf, Articles 20.9-20.10.

168. Ibid, Article 20.11.

169. Ibid, Article 20.30.

170. Joshua P. Meltzer, "The Importance of The Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment" Brookings Institution, Global Economy and Development, Working Paper 79, October 2014, https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm.

171. Alberto Mucci, Laurens Cerulus, and Hans von der Bouchard, "Data fight emerges as last big hurdle to EU-Japan trade deal" *Politico*, December 8, 2016, updated December 9, 2016, http://www.politico.eu/article/eu-japan-trade-deal-caught-up-in-data-flow-row-cecilia-malmstrom/.

172. Directive 95/46/EC (Data Protection Directive); Regulation (EU) 2016/679 (General Data Protection Directive), Articles 45-46, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

173. Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements," (ITIF, April 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf.

174. *COMMISSION DECISION of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act,* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=EN.

175. *COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 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, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN.

176. *COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce* 2000/520/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=EN.

177. *JUDGMENT OF THE COURT (Grand Chamber) 6 October 2015 In Case C-362/14*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN.

JUDGMENT OF THE COURT (Grand Chamber) 6 October 2015 In Case C-362/14, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN.

179. "EU - US Cooperation," (European Commission, last updated April 28, 2017), https://ec.europa.eu/growth/industry/international-aspects/cooperation-governments/eu-us_en.

"EC-US High-Level Regulatory Cooperation Forum," document list, (European Commission), http://ec.europa.eu/DocsRoom/documents?locale=en&tags=EC-US%20High-Level%20Regulatory%20Cooperation%20Forum.

180. *Framework for Advancing Transatlantic Economic Integration between the United States of America and the European Union,* Ref. Ares(2014)3748022, November 11, 2014, http://ec.europa.eu/DocsRoom/documents/7496?locale=en

181. Ben Miller and Robert D. Atkinson, "Digital Drag: Ranking 125 Nations by Taxes and Tarrifs on ICT Goods and Services," (ITIF, October 2014), http://www2.itif.org/2014-ict-taxes-tariffs.pdf?_ga=1.167471038.1045463480.1471968194.

182. Guillaume Xavier-Bender (Editor), Robert Atkinson, Andrea Renda, "Seeing the Forest for the Trees: Why the Digital Single Market Matters for Transatlantic Relations" (German Marshall Fund of the United States, January 2016), http://www.gmfus.org/publications/seeing-forest-trees.

183. David Smith, "Trump withdraws from Trans-Pacific Partnership amid flurry of orders," *The Guardian,* January 23, 2017, https://www.theguardian.com/us-news/2017/jan/23/donald-trump-first-orders-trans-pacific-partnership-tpp.

Simon Marks and Hans Von Der Bouchard, "Europe to Trump: Don't give up on free trade," *Politico*, November 9, 2016, Updated November 14, 2016, http://www.politico.eu/article/europe-to-donald-trump-dont-give-up-on-free-trade-ttip-ceta-us-eu/.

Shawn Donan, "Trump moves towards imposing tariffs on steel imports," *Financial Times,* April 20, 2017, https://www.ft.com/content/d8413fe8-25e6-11e7-8691-d5f7e0cd0a16.

Glenn Thrush, Nick Wingfield, and Vindu Goel, "Trump Signs Order That Could Lead to Curbs on Foreign Workers," *The New York Times,* April 18, 2017, https://www.nytimes.com/2017/04/18/us/politics/executive-order-hire-buy-american-h1b-visa-trump.html.

184. *Agreement for Scientific and Technological Cooperation between the European Community and Canada,* March 22, 1996, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:21996A0322(01)&from=EN.

185. "Roadmap for EU-Canada S&T Cooperation," (European Commission 2016, October, 2016), http://ec.europa.eu/research/iscp/pdf/policy/roadmaps_ca-2016.pdf

186. "Roadmap for EU-USA S&T cooperation," (European Commission 2016, October, 2016), http://ec.europa.eu/research/iscp/pdf/policy/roadmaps_usa-2016.pdf#view=fit&pagemode=none ; "Scientific and technological cooperation with the United States," September 23, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:ri0009&from=EN.

187. "EU-US agreement offers new opportunities for research cooperation," (European Commission, October 17,2016), http://ec.europa.eu/research/iscp/index.cfm?pg=usa.

188. *Memorandum of Understanding EU-US on eHealth*, October 17, 2010, https://ec.europa.eu/digital-single-market/en/news/memorandum-understanding-eu-us-ehealth; *Transatlantic eHealth/Health IT Cooperation Roadmap*, July 2016, http://ec.europa.eu/information_society/newsroom/image/document/2016-30/eu_us_roadmap_16674.pdf.

189. Open Data Charter and Technical Index, http://opendatacharter.net/resource/g8-open-data-charter/.

190. Open Gov Partnership, "Participating Countries" https://www.opengovpartnership.org/countries.

191. Roberto Viola, "EU-US cooperation for better usability of open data," (European Commission, October 7, 2016), https://ec.europa.eu/digital-single-market/en/blog/eu-us-cooperation-better-usability-open-data; Luca Gramaglia, "EU-US Open Data R library: Mix and match EU-US data more easily," (European Commission, November 8, 2016), https://ec.europa.eu/eurostat/cros/content/eu-us-open-data-r-library-mix-and-match-eu-us-data-more-easily_en.

192. "Accelerating the Transatlantic Innovation Economy," (Transatlantic Business Dialogue, November 2011), http://trade.ec.europa.eu/doclib/docs/2012/july/tradoc_149711.pdf.

193. Ibid.

194. *Digital Globalization: The New Era of Global Flows*, (McKinsey Global Institute, March 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

195. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," (ITIF, February 24, 2015), https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries.

196. Christian Reimsbach-Kounatze and Brendan Van Alsenoy, "Exploring Data-Driven Innovation as a New Source of Growth," (Organization for Economic Co-operation and Development, June 2013), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En.

197. "Digital Trade in the U.S. and Global Economies, Part 2," (U.S. International Trade Commission, 2014, August), https://www.usitc.gov/publications/332/pub4485.pdf.

198. Stephen J. Ezell, "A Policymaker's Guide to Smart Manufacturing," (ITIF, November 30, 2016), https://itif.org/publications/2016/11/30/policymakers-guide-smart-manufacturing.

199. "Factories of the Future: Multi-annual roadmap for the contractual PPP under Horizon 2020," 14, (European Commission, 2013), http://www.effra.eu/attachments/article/129/Factories%20of%20the%20Future%202020%20Roadmap.pdf.

200. "Advanced Manufacturing Fund," (FedDevOntario, last updated February 10, 2015,) accessed January 9, 2018, "CME Smart Program," (Canadian Manufacturers & Exporters), accessed January 9, 2018, http://www.feddevontario.gc.ca/eic/site/723.nsf/eng/h_01855.html; http://www.cme-smart.ca/home-en.

201. Rita Heimes and Sam Pfeifle, "Study: GDPR's global reach to require at least 75,000 DPOs worldwide," (IAPP, November 9, 2016), https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

202. L. Christensen, et al., "The Impact of the Data Protection Regulation in the E.U." (University of Milan Bicocca and Analysis Group, February 13, 2013), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf.

203. *Uncovering the Hidden Value of Digital Trade*, (Lisbon Council and Progressive Policy Institute, February 2015), http://www.lisboncouncil.net/publication/publication/127-uncovering-the-hidden-value-of-digital-trade-towards-a-21st-century-agenda-of-transatlantic-prosperity.html.

204. Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI," (Center for Data Innovation, 2018), http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

205. Michelle Wein and Stephen J Ezell, *How to Craft an Innovation Maximizing T-TIP Agreement,* (ITIF, October 2013), http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf?_ga=1.133188494.1045463480.1471968194.

206. European Commission, "Study on Trade Secrets and Confidential Business Information in the Internal Market," (European Commission, April 2013), http://ec.europa.eu/internal_market/iprenforcement/docs/20130711/final-study_en.pdf.

207. "Legislative Facts Sheet – Trade Secrets Act," (Uniforma Law Commission, 2013), http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act.

208. Michelle Wein and Stephen J Ezell, *How to Craft an Innovation Maximizing T-TIP Agreement,* (ITIF, October 2013), http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf?_ga=1.133188494.1045463480.1471968194.

209. Nick Wallace, "Norwegian Watchdog Turns Fire on Fitness Trackers and Misses the Mark Entirely" (Center for Data Innovation, January 10, 2017), https://www.datainnovation.org/2017/01/norwegian-watchdog-turns-fire-on-fitness-trackers-and-misses-the-mark-entirely/.

210. For example, Catherine Tucker has found that the EU privacy directive lowered online advertising effectiveness by 65 percent relative to the rest of the world: Catherine Tucker, "Economics of Privacy"

(MIT Sloan and NBER, November 15, 2012), http://www.ftc.gov/sites/default/files/documents/public_events/fifth-annual-microeconomicsconference/tucker.pdf.

211. Nick Wallace, "'Double Consent' Rule for Sharing Data Would Be Useless" (Center for Data Innovation, October 31, 2016), https://www.datainnovation.org/2016/10/double-consent-rule-for-sharing-data-useless/.

212. Nick Wallace, "EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence" (Center for Data Innovation, January 25, 2017), https://www.datainnovation.org/2017/01/eus-right-to-explanation-a-harmful-restriction-on-artificial-intelligence/.

213. Nick Wallace, "European Commission Should Stand Firm on Free Data Flows" (Center for Data Innovation, March 8, 2017), https://www.datainnovation.org/2017/03/european-commission-should-stand-firm-on-free-data-flows/.

214. Ibid; Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," (ITIF, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=2.16502783.854317994.1493726437-1075727067.1489163431.

215. Ibid.

216. Daniel Castro and Alan McQuinn, *Unlocking Encryption: Information Security and the Rule of Law*, (ITIF, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf?_ga=1.132817550.1045463480.1471968194.

217. Daniel Castro, *The False Promise of Data Nationalism*, (ITIF, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

    Brad Smith, "Time for an international convention on government access to data," Microsoft, https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/, (Microsoft, January 20, 2014); "Safety, privacy and the Internet paradox: solutions at hand and the need for new trans-Atlantic rules," (Microsoft, January 20, 2015), https://blogs.microsoft.com/on-the-issues/2015/01/20/brad-smith-time-nations-adapt-laws-reflect-todays-technology/.

    Daniel Castro and Alan McQuinn, "Cross-Border Digital Searches: An Innovation-Friendly Approach," *Information Week,* November 5, 2014, http://www.informationweek.com/strategic-cio/digitalbusiness/cross-border-digital-searches-an-innovation-friendly-approach/a/d-id/1306989.

218. Daniel Castro and Alan McQuinn, "France, you do not own the internet" *Computerworld*, January 11, 2017, http://www.computerworld.com/article/3156296/internet/france-you-do-not-own-the-internet.html.

219. "Commission takes steps to modernise EU's standardisation policy," (European Commission, June 1, 2016), http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8839.

220. Joshua New and Daniel Castro, *Why Countries Need National Strategies for the Internet of Things*, (Center for Data Innovation, December 16, 2015), http://www2.datainnovation.org/2015-national-iot-strategies.pdf.

221. Michelle Wein and Stephen J Ezell, *How to Craft an Innovation Maximizing T-TIP Agreement*, (ITIF, October 2013), http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf?_ga=1.133188494.1045463480.1471968194.

222. Stephen Ezell, Adams Nager, Robert Atkinson, *Contributors and Detractors: Ranking Countries' Impact on Global Innovation*, (ITIF, January 2016), http://www2.itif.org/2016-contributors-and-detractors.pdf.

223. Nick Wallace, "EU bill on data mining lacks ambition," *EUobserver,* October 12, 2016, https://euobserver.com/opinion/135474.

224. Nigel Cory, *The Worst Innovation Mercantilist Policies of 2016*, (ITIF, January 2017), http://www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf.

Nick Wallace, "European Commission Should Stand Firm on Free Data Flows," (Center for Data Innovation, March 8, 2017), https://www.datainnovation.org/2017/03/european-commission-should-stand-firm-on-free-data-flows/.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Joseph Kennedy, Nigel Cory, and Alex Key. Any errors or omissions are the authors' alone.

ABOUT THE REPORT

ITIF completed this report for the DISCOVERY Transatlantic ICT Project, an initiative run by Inmark Europa and supported by the European Commission, with the aim to facilitate dialogue in ICT policy between Canada, the European Union, and the United States.

ABOUT THE AUTHORS

Nick Wallace is a Senior Policy Analyst at ITIF's Center for Data Innovation, and leads the Center's European research in Brussels. Alan McQuinn is a research analyst at ITIF in Washington, D.C. Stephen Ezell is ITIF's vice-president for global innovation policy, also based in Washington. Daniel Castro is vice-president of ITIF and Director of the Center for Data Innovation.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.