DISCOVERY
Europe-North America Dialogues for ICT Cooperation

D.1.4 Input Paper ICT Policy and Regulations Working Group

Grant Agreement number: 687780
Project acronym: DISCOVERY
Funding Scheme: Coordination and Support Action

Due date: 1/03/2017
Actual date: 19/05/2017
Document Author/s: EACCNJ, INMARK, in collaboration with Information Technology and Innovation Foundation - ITIF
Version: 1.0
Dissemination level: PU
Status: Final Version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 687780

TABLE OF CONTENTS

Page

1 EXECUTIVE SUMMARY

This report analyzes the **key policies that impact the development and use of information and communications technology (ICT) in the European Union, the United States, and Canada**, including intellectual property rights, data protection rules, the regulatory environment, and support for digital innovation. The report **describes and compares the policies and regulations of these three markets, as well as major international agreements and other bilateral and multilateral efforts to support transatlantic cooperation on policies affecting ICT**. The report illustrates the contrasts by describing the **hypothetical case of AcmeDigital**, a user case where Canadian tech startup trying to open an office in the European Union. Finally, the report analyzes the impact of these policies in these three markets on transatlantic cooperation in ICT research and innovation and **provides recommendations for policymakers in the EU, the US, and Canada**, with regard to how they can build a transatlantic market for ICT that benefits all three entitles.

Differences in policies and regulations are often a challenge for cross-border trade, investment, and research and innovation, but they are often not avoidable in relationships between sovereign nations. Ergo, the basis for transatlantic ICT cooperation should be common principles and joint actions, rather than a singular set of policies. The contrasts between the United States and Canada as two highly-devolved, trans-continental nation-states with federal systems, and the European Union as a supranational association of 28 nation-states (EU27 after Brexit), each with varying levels of devolution of their own, further emphasizes the importance of this point.

These differences are laid out in section 3. For example, while the United States and Canada have national patent regimes, so too does each individual EU country. But European countries inside and outside the EU share a centralized bureaucracy that grants access to all their different national patent systems. And while the United States offers thorough privacy protection through its complex web of data protection laws and regulations, many tied to specific sectors, the EU and Canada each have specific legislation that sets out comprehensive frameworks for the protection of personal data. The three entities share broadly similar and consistent approaches to copyright protection, but contrasting details - such as definitions for "fair use" or "fair dealing"- have important implications for some new technologies, such as text and data mining.

A good **understanding of the distinction between minor and fundamental differences is necessary for either reconciling them or finding compromises**, which then provides a basis for greater cooperation. Matters of detail, such as the legal status of text and data mining in copyright law, can and should be fully resolved though common agreement. Complex fragmentation in the protection of patents and trade secrets should be mitigated through agreements that establish basic principles that can hold throughout the different environments. Meanwhile, fundamentally different regulatory models for data protection demand compromises based on clarity and consistency in the law and its application, mutual respect for sovereignty, and the free flow of data.

2 INTRODUCTION

The purpose of this report is to provide a comparative analysis of information and communication technologies (ICT) policy and regulations in the European Union, United States, and Canada, as well as relevant international agreements, to support recommendations to policymakers in the three regions for improving transatlantic cooperation on ICT research and innovation. In addition to trade in ICT, the report examines obstacles to the free use of some technologies, such as text and data mining, as well as restrictions that inhibit the development of new ICT goods and services. The report focuses on four themes: intellectual property rights (IPR), data protection, the regulatory environment for ICT, and government support for digital innovation. The four topics for analysis have been chosen in order to present the key issues impacting transatlantic ICT cooperation in a way that is comprehensive, but also accessible.

The DISCOVERY Transatlantic ICT Forum held a workshop in Brussels in November 2016, with participants from the industrial, diplomatic and research sectors, in order to identify ways in which the transatlantic partners could cooperate better to support ICT development. Participants highlighted both IPR and data protection as key policy areas affecting such cooperation. These are particularly important because of the impact they have on the extent to which researchers and developers can use, analyze, and re-use data. For example, new research methods related to text and data mining, though legal and uncontroversial in some countries, can run afoul of copyright laws in others, even when their use in no way infringes on the copyright holder's exclusive right to reproduce or redistribute their work. Data protection laws, meanwhile, can be extremely complex, and 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 even force firms to choose between competing legal environments.

The broader regulatory environment determines the circumstances in which such difficulties occur. Divergent approaches to questions of anti-trust policy and technical standards threaten to create incompatible markets where companies with structures or standards struggle to operate effectively across all of them, regardless of how they behave. Furthermore, regional variations within ostensibly single markets—whether that be between EU countries, American states, or Canadian provinces—raise the complexity, and therefore the cost, of conducting research and doing business across borders.

Properly-targeted government support for digital innovation, such as research grants and support for digital startups in their early stages, helps new ideas to take their full form and develop into coherent self-reliant business models. Moreover, international cooperation in this field at the level of government helps to deepen ties between the science and technology communities of the respective countries, by involving them in international research calls and encouraging them to form alliances.

With the right combination of IPR laws; interoperable, evidence-based data protection regimes; regulatory environments open to international trade and research; intergovernmental cooperation on funding and support initiatives, and robust trade agreements and institutions to manage policy differences; the EU, the United States, and Canada will be able to build a strong and competitive shared environment for ICT development. This will be especially important as all three regions face increasing challenges from ICT competitors in other parts of the world, particularly China.

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

The EU, United States, and Canada each have varying approaches to ICT policy and regulations. Individual digital issues, from data protection to R&D funding, have elicited vastly different approaches to regulation across these three regions/countries. For example, while the United States has in many cases 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. That said, all three have fairly robust and largely similar laws with regard to copyright protection. This report shows the distinctions between each country's policies towards ICT goods and services by focusing on four primary policy areas: intellectual property, data protection, ICT regulatory environment, and government support for digital innovation.

3.1 Intellectual Property

3.1.1 European Union

Patents
There is no single patents regime in the EU: each 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, centralized procedure for European patent applications, but does not harmonize patent rights, which are determined nationally. The other is the unitary patent, which promises stronger, harmonized protections, but cannot function effectively until participating countries have ratified the agreement on the court necessary to uphold it.

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, and was established in 1977 under the auspices of the European Patent Convention (EPC) of 1973. It currently 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 law. 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 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 essentially a route of access to these national patents: applicants going through the EPC route 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 unitary patents in the European Union, to be issued by the EPO.[1] 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 Unitary Patent Court (2013/C175/01) has 25 participating EU member states: all of them except for Poland, Spain and Croatia. Poland and Spain did not sign the agreement, and Croatia was not an EU member state when participants signed in 2013.[2] However, as of April 2017, only 12 of the 25 participating member states have ratified the agreement: Austria, Belgium, Bulgaria, Denmark, Finland, France, Italy, Luxembourg, Malta, Netherlands, Portugal, and Sweden. Ergo, until the remaining participants ratify the agreement, there is no functioning unitary patents system in the EU.

Copyright

European copyright law is partially harmonized at EU level: there is a relatively comprehensive set of Directives on copyright, which combined provide a strong framework for copyright protection in national law. However, unlike Regulations, Directives are "secondary laws" that must be transposed, to the letter, into national legislation. Directives are sets of legal requirements that must be upheld, but member states are free to decide precisely how to transpose them into national legislation. This leaves considerable room for fragmentation between member states.

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 currently the subject of an ongoing review of legislation by the EU. 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 hotly debated.

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.[3] 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." (This phrase is the cause of controversy in the current debate over ancillary copyright, see 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.[4]

The Computer Programs Directive (2009/24/EC) protects software, granting the authors of computer programs the same IP rights as literary authors.[5]

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.[6]

The Copyright Term Directive (2006/116/EC), amended by Directive 2011/77/EU, determines the length of protection for copyrighted works:[7]

1. Authors' rights are protected for 75 years from their 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 Directive 2011/77/EU was adopted, 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.[8] This principle covers the rights of performing artists, phonogram producers, film producers, and broadcasting companies. Prior to 2011, the protection under 2006/116/EC was for 50 years.[9] 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 on copyright holders' behalf.[10] It authorizes copyright holders to appoint nonprofit collective 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.[11]

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.[12] However, under article 14(b) (part of section 4), 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 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." In short, the proposal is for a filtering obligation that would require platforms to proactively remove known copyrighted material to lessen the need for copyright holders to repeatedly notify platforms of copyright infringements for the same content.[13]

Text and data mining
Text and data mining of lawfully-accessed copyrighted works without prior permission often constitutes a breach of copyright in the EU. Following some member states, such as the UK, the European Commission proposed an exemption in September 2016, whereby text and data mining would not constitute a breach if it is done for scientific or non-commercial research purposes.[14] However, commercial uses of text and data mining on lawfully-accessed copyrighted works would not be legal.

Amendment 32 of the report by the European Parliament's Legal Affairs Committee on March 10, 2017, recommends the legislative proposal be amended to allow all uses of text and data mining on lawfully accessed works.[15]

Ancillary copyright
Ancillary copyright is the right of press publishers to demand remuneration for the very small portion of their work (such as the title, and introductory sentence) that is often reproduced to accompany links to the complete work, such as on news aggregator sites or on social media. Such measures were introduced in Germany in 2013 and in 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.[16]

There are no provisions for such a right in EU law. However, Article 11 of the Proposal for a Directive on Copyright in the Digital Single Market (which also included the recommendation for the text and data mining exemption in Article 3 and the filtering obligation in Article 13), if adopted, would extend the rights of Article 2 of the Copyright Directive (2001/29/EC) to press publishers "for the digital use of their press publications", limited to 20 years from publication.[17] As stated above, Article 2 of the copyright directive confers the exclusive right to "authorize or prohibit direct or indirect, temporary or permanent, reproduction by any means or in any form, in whole or in part" which campaigners say would, if applied in its entirety to online press publications, confer a right to ancillary copyright similar to that introduced in German and Spanish cases.

Precisely how much, if any, of a preview accompanying a link might be covered is impossible to say, because the 2001 law was not designed for this scenario and does not stipulate the size of the extract. However, it is worth noting that article 5 of the Copyright Directive includes, among other exemptions, a specific allowance for properly-cited quotations used for the purposes of news reporting—but it is far from 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.

Content Licensing and Geo-Blocking
Geo-blocking is sometimes used to differentiate prices between locations—not least because different EU countries have different equilibrium prices due to varying levels of income and other factors affecting demand. Cross-border differences in tax and regulation also deter companies from entering certain markets, prompting them to use geo-blocking. In some cases, geo-blocking can result in customers being denied access to content they have already paid for when they cross a border.

Country-specific licenses for video content mean companies often have to use geo-blocking even if they do not differentiate prices between countries and would prefer to supply content to the largest market possible. The reason licensing agreements are often country-specific is because traditional television broadcasters remain important buyers in the market and only operate within individual. The result is that streaming services with international audiences often cannot legally allow access to content they have a license for in one country by customers in the rest of the EU, because this could breach the copyright of other broadcast license holders.

The European Council has approved draft regulations on geo-blocking.[18] The draft regulation outlaws geo-blocking for purposes price differentiation (or "discrimination", as the draft calls it), but allows geo-blocking for licensing concerns to continue. This coincides with plans to reduce cross-border regulatory and tax issues that prompt firms to use geo-blocking, and the Council is also due to decide

on the portability of digital content, which would ensure customers who cross internal borders within the EU retain temporary access to content they have paid for.[19]

Trademarks
Trademarks can be registered at national level or at 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 ad-hoc legislation addressing the criminal misappropriation of trade secrets; other member states address the issue through a variety of different rules in criminal and civil law.[20]

3.1.2 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 are primarily broken down into three areas: patents, copyrights, and trademarks.

Patents
U.S. patent law give 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).[21] 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.[22] To acquire a patent, inventors file an application with the U.S. Patent and Trademark Office.

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.[23] Congress has amended this law several times since it was enacted, such as by the Semiconductor Chip Protection Act (SCPA) and the Digital Millennium Copyright Act (DMCA).[24] 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 Copyright 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 accessing or copying works to which they do not have a legal right. Another key provision of the DMCA establishes limitations on liability for online service providers for the actions of their users, an important provision that 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 businesses with protections for words, phrases or logos that distinguish their goods or services from 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 owners of trademarks against infringement, and establishes guidelines and remedies for trademark owners.[25] The purpose of this act is to help avoid confusion and deter misleading advertising. Lanham Act has been amended several times since it was enacted in 1946, including in the Trademark Counterfeiting Act of 1984.[26] Businesses only need to use a trademark in order for it to have limited protection under the law. However, by registering the trademarks with the U.S. Patent and Trademark Office, owners can receive additional protections. And 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.[27]

Several U.S. laws provide additional protections to intellectual property owners, and punishments for infringement. For example, the Economic Espionage Act of 1996 protects businesses from the theft or misappropriation of trade secrets by making it a federal crime.[28] Similarly, in the United States, 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 infringing products that are imported into the country.[29] The ITC can prevent these products from being imported into the United States as injunctive relief.

3.1.3 Canada

Patents
Federal patent law in Canada dates to the founding of the country itself in the British North America Act of 1897 and through common law.[30] Since that time, Canadian patent law has evolved through numerous iterations into the modern Canadian Patent Act of 1985.[31]

The Canadian Patent Act protects products, compositions, machines, processes, or any new improvement to an existing invention[32]. To be granted a patent, the inventor must prove the invention is novel (i.e., first of its kind), useful (i.e., the invention must work), and inventive (i.e., not obvious to the profession). Patents are granted to a maximum of 20 years after the day of the patent application is filed.[33] Canada has a first-to-file patent system, where the patent application filing date is the priority for infringement claims.[34]

The Canadian Intellectual Property Office, which issues patents, does not have jurisdiction over litigating patent infringement—this is the job of the courts.[35] Further, Canada 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.[36]

Copyright
The Canadian Copyright Act was first passed in 1921, and was amended substantially in 1988, 1997, and 2012.[37] The 2012 version is frequently referred to as Bill C-11 or the Copyright Modernization Act. It came into full force in 2015.

Under Canadian law, a copyright provides protection for literary, musical, or otherwise artistic works, including computer programs, performances, and communications signals.[38] A copyright applies in Canada if the work was published in Canada even if the author is not a Canadian citizen or resident. Regardless of merit or commercial value, the Copyright Act protects all original creative works and establishes the legal framework doing so.[39]

Many of the updates to Canadian copyright law were prompted by technological developments that created new areas of potential vagueness under the previously existing iteration of the law. Portions of the Copyright Modernization Act sought to reduce digital piracy.[40] The bill prohibits circumvention of "digital locks", measures installed in digital media to block piracy attempts. The law prohibits the removal of these locks from a copyrighted work for personal use, and also bans the making, selling or using of technology to circumvent anti-piracy protections.[41]

The law does permit the reproduction of copyrighted works for satire, parody, and educational purposes. There is also an exemption to allow for the creation of user-generated content, such as sampling music in order to create a mashup or new musical work.[42] But the Copyright Modernization Act remains controversial in Canada, with critics arguing that it weakens rights the right to personal use, the ability to backup files with copyrighted works, and the ability to convert copyrighted works from one format into another.[43]

Enforcement of copyright law in Canada comes through the courts. Courts are empowered by the Copyright Act 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.[44] 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 Canadian 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.[45] Under the Trade-marks Act, there are three types of trademarks: ordinary marks (e.g., words or sounds that distinguish some goods from others), certification marks (e.g., markings that show goods or services meet a defined standard), and distinguishing guises (e.g., the shape or packaging of a good that signifies a specific business or individual).[46] Under Canadian law, a trade mark 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 United States, Canadian trademark law is solely a matter of federal jurisdiction, and businesses cannot register trademarks with individual provinces.

3.2 Data Protection

3.2.1 European Union

In the field of Data protection, EU Member states are bound by two legal orders, EU Law, and the European Convention on Human Rights (ECHR)[47]as well as the Council of Europe Convention for the Protection of Individuals with regards of automatic Processing of Personal Data (Convention108)[48] and other Coe Instruments.

The European Convention of Human Rights
The right of protection of personal data is stated in Article 8 of the ECHR and it guarantees the right to respect for private and family life, including home and correspondence and establishing the conditions under which restriction of this rights are permitted.

Council of Europe Convention 108
CoE Convention 108 was opened as a result of the growing need for more detailed rules to protect individuals by protecting their personal data.

Convention 108 applies to all data processing carried out by both public and private sector, on the one hand providing guarantees on the collection and processing of personal data and seeking to regulate their transborder flow and on the other hand it outlaws the processing of "sensitive data" (person's race, health, religion, sexual life politics or criminal record) without the proper legal safeguards.

It remains the first international legally binding instrument dealing explicitly with data protection. All EU Member States ratified Convention 108 and currently is open for accession to non-member states of the CoE, including non-European countries (Uruguay has already acceded and Morocco has been formally invited to accede).

The Charter of Fundamental Rights
Article 8 of the Charter for Fundamental Rights includes a right to the protection of personal data.[49] 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 (2009), meaning any change to the Charter would require treaty change, with unanimous agreement among member state governments and ratification in national legislatures.[50] As the Charter is primary legislation, all secondary legislation (laws passed by the 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 European Union Data Protection Directive and the GDPR
The current EU legal instrument on data protection is Data Protection Directive (95/46/EC). It was adopted in 1995 at the same time when several EU Member States had already adopted their respective national data protection laws.

The aim of the Directive is harmonization of data protection national laws since the free movement of people, services and goods within the internal market required the free flow of data too which couldn't be possible unless EU could rely on a uniform high level of data protection. Its territorial application extends beyond the EU28 including countries part of the European Economic Area (EEA)[51], i.e. Iceland, Liechtenstein and Norway.

The GDPR will replace the Data Protection Directive (95/46/EC), which at the time of writing is still in force.[52]

The intention of the General Data Protection Regulation (GDPR), adopted in 2016 and entering into force in 2018 (25/05/2018), is to fully harmonize data protection law in the EU, so that the exact same data protection laws apply across borders.[53] Whether or not it will eliminate fragmentation in practice remains to be seen.

The GDPR is a gigantic document, and it is intended to cover all cases where personal data is collected or processed. It includes existing EU privacy provisions such as restrictions on data transfers outside the EU, data minimization, and the right to be forgotten (codified for the first time, following case law). It also includes entirely new measures, such as the right to explanation of algorithmic decisions and the right to opt-out of them, and the right to data portability. The privacy of communications services, such as telephone or Internet browsing, is covered by the ePrivacy directive (see next section).

Data minimization and purpose limitation (Article 5)
Data minimization means collecting no more data than is required to fulfill the originally stated purposes. Purpose limitation means not using data for anything other than the originally-stated purpose for which it was collected. If data is anonymized, it is deemed non-personal and so falls outside the scope of the GDPR and can be re-purposed. Restrictions on repurposing are relaxed for "pseudonymized" data, under GDPR article 6. The two concepts originate in Data Protection Directive 95/46/EC Article 6.

Right to explanation and to opt out of algorithmic decisions (Articles 13, 14 and 22)
The right to explanation is a new concept introduced by the GDPR. Data subjects have a right to an explanation of the logic involved in an algorithmic decision whenever it may have significant legal effects upon them, and they can refuse to be subject to a solely-automated decision. In theory, the purpose of this is to ensure transparency and accountability in the use of algorithms, such that companies using algorithms cannot avoid responsibility for unjust decisions made by their algorithms, and so data subjects can find out whether decisions made about them may have been biased, or based on inappropriate characteristics (such as ethnicity or religion). However, the rule presupposes that auditors trying to put together such an explanation will be able to identify and understand such bias if it is there, even though it may be based on subtle markers for ethnicity that vary greatly from one place to another.

Right to erasure and the right be forgotten (Article 17)
Article 17(1) confers on data subjects the right to have deleted personal data stored by a data processor (the right to erasure). Article 17(2) of the GDPR confers a right to have publicly-available information removed by data processors (right to be forgotten). Article 17(3) includes exceptions to 17(2), including to protect freedom of speech.

The underlying principle of the right to be forgotten is the right to erasure, which originally appeared in Article 12 of Directive 95/46/EC. In a ruling on May 2014 (C-131/12), the ECJ ruled that Article 12 should apply to web links to news stories about the data subject, and that search engines must remove old links if the data subject wishes.[54]

Google has responded by blocking access to relevant articles inside the EU, but not outside it. The French national data protection authority has taken the right to be forgotten a step further, by demanding that links be blocked worldwide, even in

territories without a right to be forgotten, and where there are stronger protections for freedom of speech than in the EU.[55]

The right to be forgotten has now been 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."

The case of the right to be forgotten highlights how replacing Directives with Regulations does not guarantee total harmonization of European law. National regulators will remain responsible for interpreting and enforcing the GDPR when it comes into force, and none of the limitations in Article 17(3) preclude the French interpretation of ECJ ruling C-132/12, or from applying that to Article 17(2).

Right to data portability (Article 20)
Article 20 of the GDPR confers a new right to data portability, which is new to EU law. It extends the right of access to one's personal data to a requirement that data subjects can receive their personal data in a standard, machine-readable format. This 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)
Article 44 imposes a general prohibition on transfers outside EU, unless the non-EU, or "third" country's data protection practices are deemed adequate. This rule has its origin in Article 25 of the Data Protection Directive (95/46/EC).

Article 45 of the GDPR and Article 25(6) of the Directive give the European Commission the job of determining whether a third country is adequate. Under Article 46 of the GDPR, and Article 26 of the Data Protection Directive, personal data can be transferred to a country not ruled adequate if the data processor puts appropriate safeguards in place. This was the legal basis for the Privacy Shield agreement to enable data flows to the United States.[56]

ePrivacy
The current ePrivacy Directive (2002/58/EC) is due to be replaced by an ePrivacy Regulation, the draft of which was published in January 2017.[57] 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 as it pertains to specifically to communications, as opposed to personal data collected for other purposes.

The Cookie Law
Both the 2002 Directive and the draft Regulation impose rules on the use of cookies. Recital 25 of the Directive requires of that "use [of cookies] should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC [the Data Protection Directive] about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using." In addition to transparency

requirements (e.g. privacy policies), the Data Protection Directive also requires the consent of the data subject.

In the years since, national data protection regulators have interpreted and reinterpreted this rule for 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 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 previous rule did, 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 include this option, but they do not force users to change the setting on first use.[58]

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 are subject to the same rules. These include rules such 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 will apply.)

3.2.2 United States

The United States does not have a single dedicated law for data protection. 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 oversee 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.[59] HIPAA creates civil and criminal penalties for violations of the privacy rule by covered entities (e.g. 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.[60]

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.[61] 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.[62] 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.[63]

Similarly, the Fair Credit Reporting Act (FCRA) of 1970 promotes privacy of personal information gathered by Credit Reporting Agencies (CRAs).[64] The FCRA requires CRAs to follow "reasonable procedures" to protect the accuracy, confidentiality, and relevance of credit information, establishing a framework for protections that allows data subjects to access and correct limits, limits how that information is shared, allows users to delete outdated information, allow consumers to choose to not share this information with third parties, and others.[65] 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.[66]

The United States also has specific privacy rules for video rentals, video games, or other audio visual materials (e.g., 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.[67] The VPPA also requires law enforcement agencies to seek a warrant to obtain this information and creates civil penalties for violations of this rule.

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.[68] 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.[69] FERPA requires all schools to receive parental consent prior to sharing a student's educational records, except under limited circumstances.[70] 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.

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.[71] The company then settled with the FTC a year later for violating the terms of the consent decree, resulting in a large fine.[72]

State Data Protection Laws

In addition to federal data protection laws, states have also created numerous specific privacy laws that only apply within their jurisdiction. 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.[73] One of the strongest data breach laws is in California, which requires any business or state

agency to notify a Californian resident of a data breach within 30 days, except under limited circumstances.[74] With any state-specific privacy or security law, the state's attorney general has the ability to bring enforcement actions against violations.

3.2.3 Canada

PIPEDA

Canada has two federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). While the Privacy Act applies to the public sector, PIPEDA regulates how the private sector handles personal information. PIPEDA became law in 2000, and it applies to organizations engaged in commercial activities, as well as to the personal information of employees in federally regulated industries like banks and broadcasting.[75]

These 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.[76]

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.[77] To be considered "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. Alberta, British Columbia, and Québec each have legislation deemed "substantially similar" to PIPEDA.[78]

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 is empowered to audit federal institutions to ensure the appropriate handling and availability of personal information under both the Privacy Act and PIPEDA.[79]

3.3 Regulatory Environment

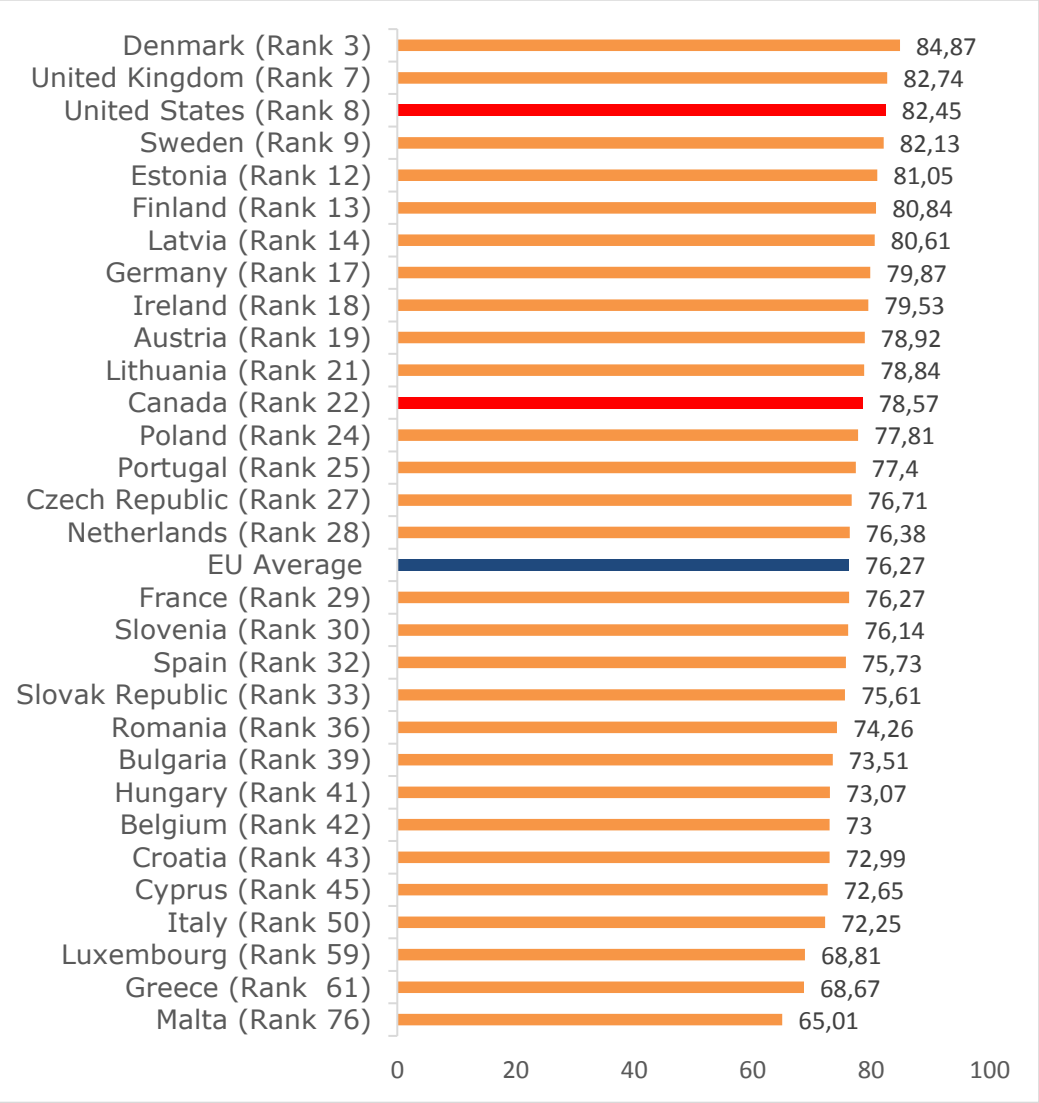
Many countries strive to create an environment that attracts businesses and cultivates economic growth, such as by streamlining regulatory requirements imposed on businesses and decreasing barriers to entry into local markets. The World Bank measures this quality in nations—known as the ease of doing 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.[80]

3.3.1 European Union

Ease of Doing Business and Market Fragmentation

As the European Union is a union of 28 nations, its members occupy 28 different places in the World Bank's ease of doing business rankings. The regional average score for the entire EU would put it in 30th place globally, on a par with EU member state Slovenia.[81] However, that average is based on wide variation between EU countries. 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[82]

Because the EU is a supranational union, rather than a federal-national union like the United States and Canada, the EU exhibits far greater variation between member states than that seen between American states or Canadian provinces. The wide range of ease of doing business scores among EU countries demonstrates how fragmented and varied the EU's regulatory environment and market is. 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 19 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.[83]

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.[84]

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.[85]

Subsidiarity
According to Article 5(3) of the Treaty on European Union (TEU), the European Union can only act in policy areas outside its exclusive competencies if the desired objectives cannot be achieved by the member states.[86] In other words, any EU act outside of the exclusive competencies needs to be accompanied with an appropriate explanation for why it is being carried out at EU level, and not member state level.

The upshot of these competencies and the subsidiarity principle is that the regulatory environment varies considerably in different parts of the European Union. National regulators are also often responsible for implementing some EU-level legislation: the GDPR, for instance, will be an EU-wide law, but enforcement of it will be the responsibility of data protection authorities in each member state.

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.

3.3.2 United States

In 2017, the United States ranked 8th in the World Bank list for ease of doing business.[87] 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 are created and given authority through laws passed by Congress, have the ability to create administrative rules and regulations. The act that governs how U.S. agencies may establish regulations is the Administrative Procedure Act of 1946.[88] The Act requires agencies to keep the public informed on 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 (e.g., Department of Transportation) and independent agencies (e.g., the Federal Communications Commission). 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.[89] Self-regulation can be defined as "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.[90]" This involves private, market-based 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 endorsement by government, such as 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).[91] 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.[92]

Self-regulatory frameworks do not operate in the United States without supervision by the public sector. Industry and government jointly administer the regulatory process by providing oversight of industry standards or self-regulatory organizations and enforcing penalties for violations. For example, the Federal Trade Commission (FTC), through the FTC Act, has the authority to enforce voluntary frameworks by penalizing companies that behave unfairly or deceptively. If a company mischaracterizes the level of security it offers its users, for example, then the FTC can bring an enforcement action against that company. Similarly, if a securities company's employees do not follow FINRA's code of conduct, they could be subject to a penalty from the Securities and Exchange Commission (SEC).[93]

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.[94] For example, if operators of unmanned aircraft systems, also known as drones, adopt the National Telecommunication and Information Administration's voluntary best practices for drone privacy and break their commitments, the FTC can pursue an enforcement action against them.[95]

The role of U.S. regulators is expanding. ICT goods and services constitute an area where many U.S. regulators have traditionally not created rules. However, in recent years, regulators in the United States 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 has always created rules for automobiles and planes, but responding to changing technology, it recently proposed policies for automated vehicles and drones.[96] Similarly, the Office of the Comptroller of the Currency, an agency of the U.S. Department of Treasury that oversees banks, has announced draft plans to give fintech companies the ability to apply for partial bank charters.[97] As ICT continues to become integral to various goods and services, U.S. regulators continue to expand their role.

Furthermore, U.S. taxes can also affect ICT goods and services. U.S. tax policy towards ICT goods and services can be interventionist, sometimes for good policy reasons (e.g., the R&D tax credits) and other times due to pressures from special interest for particular tax provisions.[98] However, most U.S. policymakers 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.[99] Moreover, the U.S. corporate tax rate is quite high, both in statutory and effective terms.[100] In addition, the U.S. R&D tax credit is relatively anemic compared to other nations, ranking 27th in 2012 for R&D tax generosity.[101] And unlike many European countries and Canada, the United States does not use a

border-adjustable value added tax (VAT).[102] (Although a similar border adjustment tax, or BAT, has been considered by the Trump Administration.)[103]

3.3.3 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.[104] Most notably, Canada is the second-easiest place to start a business in the world due to factors such as the short time it takes and low number of procedures involved in 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. Canada's business climate does have some noticeable weak spots, however. For example, 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 lengthy.[105]

In Canada, legislative authority is divided between the federal government and provincial governments. At the federal level, an enacted law sets the scope of regulatory power of and assigns authority to a ministry to make subordinate regulations. The Statutory Instruments Act governs how ministries create federal regulations.[106] 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 becomes available for public comment.[107] The regulation is then amended based on this feedback as necessary, registered, and published in its final form in the Canada Gazette.

One major focus of Canada's regulatory climate is on competition and antitrust. 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 equitable opportunities for small business. For example, the Competition Act contains provisions to prohibit false or misleading practices by businesses, such as deceptive marketing practices.[108] Regarding antitrust, besides criminalizing explicitly anti-competitive business practices, the Act also requires premerger notification and contains noncriminal provisions which 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 focuses on competition outside of 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 explicitly provide that 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, the European Union, the United Kingdom, and the United States.

Canadian regulators have the authority to enforce laws and subsequent regulations by bringing enforcement actions against infringing companies. For example, in 2015, the Competition Bureau took enforcement action against Aviscar and Budgetcar, two of Canada's largest rental car companies, for advertising prices that were unavailable to consumers at the time of purchase due to extra fees.[109] Similarly, in 2015 the Canadian Radio-television and Telecommunication Commission announced enforcement proceedings against Compu-Finder for sending commercial messages without a recipients' consent and without a functioning "unsubscribe" button (as is required by Canada's anti-spam laws).[110]

Like the U.S. government, where there are no set laws or regulations, the Canadian government allows for industry self-regulation, in which private, market-based institutions govern their own actions through voluntary agreements. For example, in 2013 the Canadian advertisers, marketing trade associations, and industry groups formed the Digital Advertising Alliance of Canada and created a self-regulatory program for online advertising called AdChoices.[111] 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.[112]

At the provincial level, regulators also create rules that affect the Canadian digital economy. A large portion of Canadian consumer protection legislation is administered by provincial governments. Provinces and territories regulate some areas that the federal government does not, such as credit reporting and contracts.[113] Legislation and regulation can vary from province to province. 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 companies using digital currency technology (e.g., block chain or distributed ledger technology) may be subject to Ontario securities law requirements.[114]

3.4 Government Funding for Digital Innovation

3.4.1 European Union

Government support for innovation is a shared competence: both the EU and the member states provide financial support. The main source of EU funding for digital innovation is the Horizon 2020 program, but European Structural Funds—which are primarily for regional development—can also support digital projects, provided they are geared towards the goals of the structural funds.[115] The European Commission also plays a role in standards development, particularly with a view to maintaining compatibility between member states' own efforts to support the development of standards.

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."[116] 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 the relevant goals. For example, some Horizon 2020 funds go to smart city

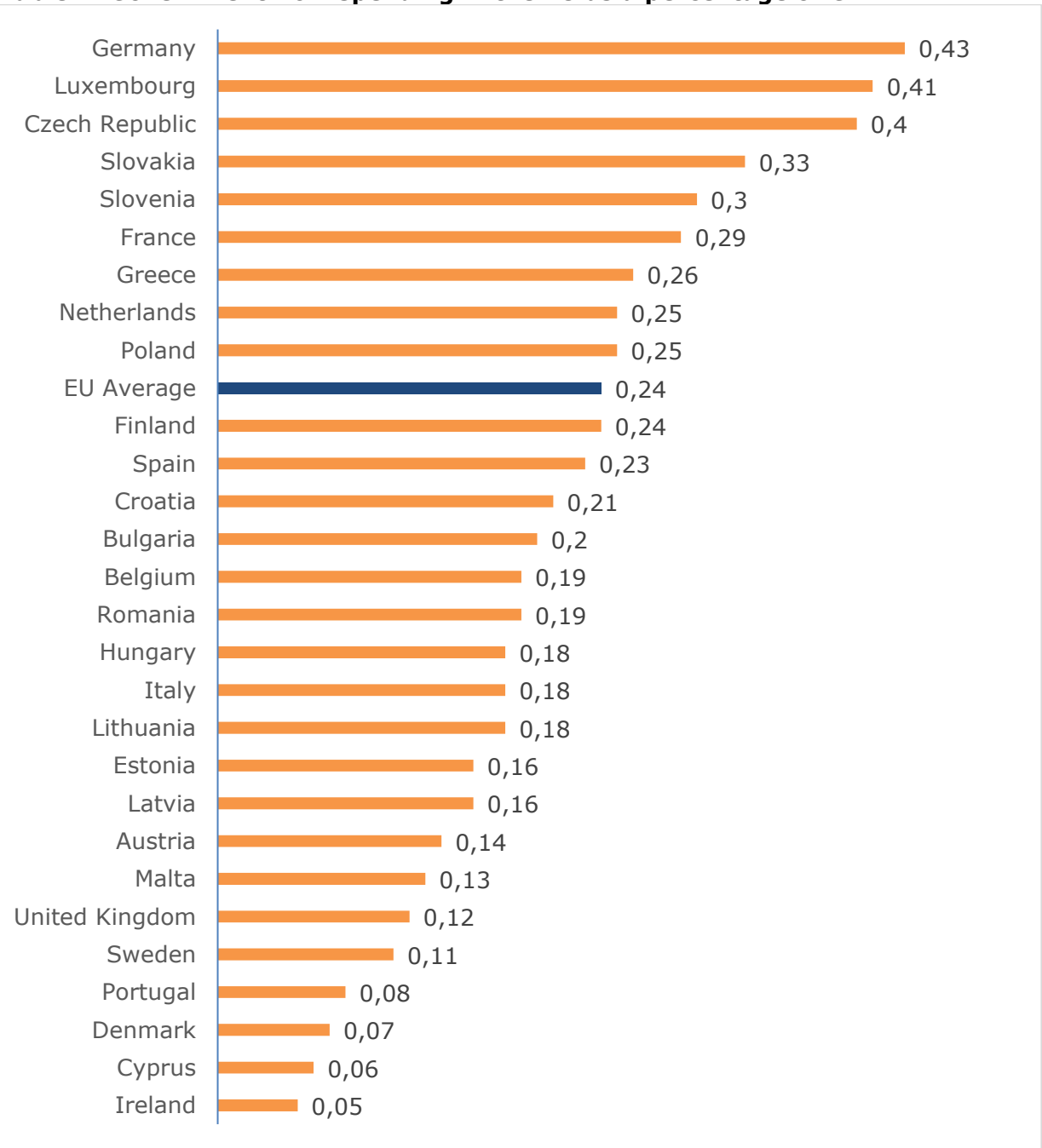
projects, which use digital technologies to make urban life more efficient and sustainable.

The European Institute for Innovation & Technology (EIT) is an independent organization 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 very diverse. 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, including by private companies. Figure 2 shows EU member states governments' spending on R&D in 2014, the most recent year for which complete figures are available.

Table 2: Government R&D spending in the EU as a percentage of GDP



Source: Eurostat[117]

3.4.2 United States

The primary form of support the U.S. government provides for digital innovation has been in its 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 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 (e.g., magnetic core memory and multiple central processors) between 1946 and 1965.[118] However, unlike the EU's Horizon 2020 program, 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 is based on two aspects: 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 (although this remains higher than in any EU country).[119] 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.[120] 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, 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. The U.S. agencies—such as the Departments of Defense, Energy, and Health—also fund a system of between 80 to 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.[121] 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 outcomes.[122] Overall, while policies have been put in place 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 (e.g., lasers). DARPA also hosts open competitions to help develop new technologies or solve tricky technological challenges. For example, in 2004 DARPA hosted a prize competition to develop autonomous vehicles, known as the DARPA grand challenge, and has periodically hosted similar competitions to advance innovation.[123]

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 where 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.[124] 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.[125] These groups work cooperatively to develop open voluntary national standards using a consensus-based approval process.[126] The content of these standards may relate to products, processes, services, systems, or personnel.

The U.S. government may also actively guide various private sector stakeholders and interested members of the public to developing guidance or best practices. For example, the National Telecommunications and Information Administration (NTIA) has been 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.[127] In this process, 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 (e.g., NIST's cryptographic standards) and voluntary frameworks (e.g., NIST's Cybersecurity framework).[128] 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. 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.[129]

Similarly, in 2014, NIST partnered with US Ignite—a nonprofit dedicated to advancing smart cities—to launch the Global City Teams Challenge.[130] This challenge was designed to bring together stakeholders from diverse sectors of the economy (e.g., energy, healthcare, manufacturing, etc.), to collaborate and develop standards for smart cities and smart communities.[131]

In addition, the U.S. government has created several programs to promote digital innovation for defense and intelligence gathering. 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.[132] DIUx funds promising technologies through prize competitions, targeted R&D efforts and incubator partnerships.[133] 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.[134]

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 and 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, multiagency strategic vision and 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. The Networking and Information Technology Research and Development (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 are using innovative contracting methods to support innovation with the private sector.[135] The National Oceanic and Atmospheric Administration's (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.[136] 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 novel partnership, NOAA is able to foster digital innovation without making additional any expenditures.[137]

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 in their states. 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.[138] 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.[139] 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 with $2.2 million in tech transfer grants.[140]

3.4.3 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 has fallen substantially over the last few years as a share of GDP to its lowest level since before 1996.[141]

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.[142] 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.[143]

Canada has created several programs to help encourage technology transfer, such as through dedicated technology transfer offices at various universities and agencies.[144] 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 followed suit.[145]

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 C$3 million in research expenditures.[146] 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 C$3 million. A 2014 study found that companies that qualified for a larger tax credit under the Canadian tax laws spent more on R&D when compared to firms with similar income whose situation did not change.[147] Nevertheless, the Council of Canadian Academics found in 2013 that the Canadian business sector invests less in R&D relative to its peers abroad.[148]

The Canadian government also encourages digital innovation through standards setting. 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.[149] The SCC works collaboratively with various stakeholders to develop standards or accreditation for everything from aerospace to radio interference.[150] 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.[151] This approach allows the government to let both industry cooperation and competition, as well as consumer choice determine the 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 the Pan-Canadian Artificial Intelligence, a C$125 million program to bolster the country's AI research and development.[152] 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 the AI development effort. For example, Ontario is contributing C$50 million to building the Vector Institute at the University of Toronto, which will be dedicated to researching deep learning.[153] (CIFAR's Pan-Canadian Artificial Intelligence Strategy is also contributing between C$40 to C$50 million to the Vector institute.)[154]

4 COMPARATIVE ANALYSIS OF TRANSATLANTIC ICT POLICY AND COOPERATION

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

4.1 Intellectual Property

While IPR differ between the EU, the United States, and Canada, there are basic common protections in all three markets established by a variety of international agreements. The United States and the EU both support research into the importance 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% of jobs in the EU during 2011-2013, and accounted for 42% of GDP.[155] 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% of U.S. employment, 30% of U.S. growth, and 38.2% of overall GDP in 2014.[156]

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 twenty-four other subsequent treaties on intellectual property, are today administered by the World Intellectual Property Organization (WIPO).[157]

These treaties establish principles such as the common recognition of the date on which a rights holder initially filed their intellectual property application in a signatory country, and minimum rights for all literary, scientific, and artistic productions. However, WIPO-administered agreements lack strong international mechanisms of enforcement, and therefore are to a large extent dependent on member states adhering to their international commitments and respecting the rule of law.[158]

The World Trade Organization (WTO), however, has stronger legal enforcement procedures, and as members of the WTO, all three parties 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).[159]

The most recent transatlantic agreement that deals with intellectual property is the Canada-EU Comprehensive Economic Trade Agreement (CETA), which was signed by both parties in 2014, ratified by the European Parliament in February 2017, and at time of writing in April 2017 is pending ratification in Canada. When it comes into force, CETA will largely bring Canadian intellectual property protections into line with the stricter protections of EU member states. For example, Canada will extend copyright terms from 50 years to 70 years.[160] EU intellectual property law is managed by Directives, not Regulations, meaning although the relevant member state laws have to adhere to many common requirements, they are not identical. 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.[161] 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.[162] CETA also includes measures for the protection of data related to plant-production products under its intellectual property provisions.[163]

4.2 Data Protection

The EU, the United States, and Canada, have very different data protection regimes. Data flows, and the regulation thereof, are an increasingly important topic for transatlantic trade. The EU and the United States are each respectively one another's largest export markets for digitally-deliverable services, and the United States' underwater cable Internet connections to Europe are its fastest.[164] However, there are barriers to the free flow of data internationally, particularly as a result of data protection concerns. Efforts to harmonize laws have been limited since the EU will not negotiate privacy in trade agreements.[165]

The EU's Data Protection Directive 95/46/EC and the General Data Protection Regulation (GDPR), which will replace the Directive in 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 a binding international agreement to protect the data.[166] 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.[167]

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) has been deemed adequate for transfers of European personal data by the European Commission since 2001.[168] The Commission has not ruled United States law adequate, but data transfers to the US are permitted under the terms of the Privacy Shield Agreement between the United States and the EU, which establishes a framework for the treatment of European personal data in the United States.[169] This 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.[170] The European Court of Justice terminated Safe Harbor in 2015, in light of Edward Snowden's revelations about NSA surveillance.[171] The ensuing crisis led to the Privacy Shield Agreement.

It is notable that Canada, despite being a part of the "Five Eyes" intelligence sharing alliance, along with the United States and outgoing EU member state the UK, retains its EU adequacy for data transfers. The UK, meanwhile, as an EU member state, is not subject to adequacy requirements because it transposes EU legislation into its own. But the European Court of Justice has ruled that the UK's sweeping new surveillance law is in breach of EU law. Whether this will affect data flows across the English Channel after British withdrawal from the EU in 2019 remains to be seen.

Furthermore, although PIPEDA's EU adequacy means data flows from the EU to Canada are unrestricted, this does not mean there are no major differences between European and Canadian data protection regimes and their impact on ICT. For example, the incoming GDPR will introduce restrictions on algorithmic decision-making that do not exist in Canada, such as the so-called "right to explanation."[172]

Despite the existence of data protection regulations at the EU-level, and at the U.S. and Canadian federal levels, all three have domestic differences in their data

protection regimes, with rules, regulatory bodies, and judicial decisions that differ between European countries, American states, and Canadian provinces.[173] This of course has implications for transatlantic trade and cooperation in ICT, as it means companies and researchers need to comply with a variety of different rules.

4.3 Regulatory Environment

Transatlantic regulatory coordination with specific regard to ICT is very limited, although 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.[174] 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.[175]

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 do nevertheless persist in the three markets, although they are far lower than in countries that have not signed the ITA.[176] 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 American Internet platforms—such as for search and social media—with European ones.[177] Such protectionism is not only, by definition, unconducive to transatlantic ICT cooperation, it also inhibits genuine competition through innovation, by encouraging European firms to merely emulate the international firms they are protected from, rather than compete with them by doing something new. The new U.S. administration led by President Trump, meanwhile, is far less enthusiastic about international trade agreements than its predecessors, and it has brought forward protectionist policies such as "Buy American, Hire American."[178] These political pressures further limit the scope for improved transatlantic cooperation in ICT during the next few years.

4.4 Government Support for Digital Innovation

EU-Canada cooperation on science and technology is institutionalized via the Agreement for Scientific and Technological Cooperation between the European Community and Canada, which was signed in 1996 and remains in force.[179] It committed both parties to provide funding, and established the Joint Science and Technology Cooperation Committee (JSTCC), which is responsible for making recommendations to the EU and Canada for supporting, among other things, information technologies, communications technologies and medical and health

research. Canadian organizations can also participate in Horizon 2020, the EU's 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.[180]

Similar agreements were later signed between the European Union and the United States. They signed the Agreement for Scientific and Technological Cooperation in 1998, and extended it in 2009 and 2014.[181] The agreement established the Joint Consultative Group (JCG). The EU and the United States also have a memorandum of understanding (MOU) committing them to cooperation on development of eHealth systems, and have published a joint "roadmap" for development of eHealth technologies, skills, and services on both sides of the Atlantic.[182]

In addition, in October 2016, the European Commission and the United States and Canada, respectively, signed Implementing Arrangements that provide additional flexibility to U.S. and Canadian organizations to participate in Horizon 2020.[183]. Furthermore, the EU, the United States, and Canada, 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 (Germany, Italy, France, and the UK), are signers to the G8 Open Data Charter, the first global commitment to open data.[184]

The United States and Canada 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 do participate.[185] As of late 2016, 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.[186]

Moreover, 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.

5 ICT POLICY - USER SCENARIO

In order to illustrate the meaning of these contrasts for ICT cooperation, one should consider the hypothetical case of a Canadian digital start-up that wants to open an office in the European Union. This section describes AcmeDigital, the services it provides and its business model, and the unfamiliar rules it will have to comply with trying to expand into the European Union.

About AcmeDigital and iGobble

AcmeDigital is an app developer and device manufacturer interested in opening an office in the EU. Its most popular app is iGobble, which offers personalized restaurant and dietary recommendations based information supplied by the user about what they eat, what they like or do not like, their allergies, whether they are vegetarian or vegan, and their budget. In addition, iGobble collects data from a wearable fitness tracker. iGobble also provides links to relevant publicly-available articles, such as restaurant reviews or articles about fitness and human health.

iGobble processes the user data using a machine learning algorithm that becomes more sophisticated as more people use the app and provide it with information. AcmeDigital also uses text and data mining technology to analyze information in academic journals and medical research, which it accesses lawfully, in order to further iGobble recommendations. iGobble uses similar techniques to identify relevant articles for the user.

The app is free to customers, and the company generates revenue through a combination of fees from restaurants, who want to be included in the app, and targeted advertising for dietary and fitness products. The app does not supply any personal data to third parties.

Certification

Like any other ICT manufacturer—whether European or foreign—Acme must provide a Supplier's Declaration of Conformity for its fitness tracker—a somewhat less rigorous requirement than if it were to set up shop in the United States, where the device would have to go through the Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program.

Intellectual property

Given the existence of the European Trade Mark (EUTM) system, iGobble can set up in a single member state and register its trademarks for the rest of the EU as well. However, other aspects of European IPR law may be more of a challenge. Part of iGobble's capacity to make sound recommendations comes from the use of text and data mining techniques on lawfully-accessed medical journals and online articles, which are subject to copyright restrictions. While this should not cause any problems in Canada, this activity could run afoul of copyright law in the EU.[187]

As described in section 3.1.1, attempts by member states and the European Commission to address this have thus far focused on non-for-profit applications of text and data mining, which would not include AcmeDigital's purposes. Unless and until the recommendation of the European Parliament's Legal Affairs Committee is accepted and made law, the legal status of text and data mining in the EU remains uncertain at best. iGobble may have to limit its text and data mining research not only to Canada, but also to non-European journals.

Data protection

The European Commission views Canadian data protection law as adequate for the transfer of personal data from the EU. However, this does not mean that AcmeDigital can operate the same data protection practices in the EU as it does in Canada. There are three significant EU rules in particular—the right to data portability, the right to be forgotten and the right to explanation—which do not appear in PIPEDA, and may come as a surprise to Acme's compliance team.

Data portability

Under GDPR Article 20, data subjects have the right not only to a copy of all of the data a data processor has on them, which is also required by PIPEDA, but also to a machine-readable copy in a structured, commonly used format. This includes not only data knowingly supplied by the customer, but also data automatically generated by their activity—such as the use of a fitness tracker. The purpose of this is to encourage competition and consent-based re-purposing of personal data, as it allows the customer to supply their data to another company, including a competitor, in order to receive personalized services from them.

Acme would need to make sure it was in a position to provide this data to its customers upon their request. The rule does not cover "inferred" data produced through algorithmic processing, which could be considered Acme's intellectual property, but Acme would nevertheless need to distinguish think carefully about what data might reasonably be considered "observed," and therefore subject to the customer's right to data portability.

The right to be forgotten

The right to be forgotten, described in section 3.2.1, would apply to AcmeDigital once it establishes a base in the European Union (currently, only French courts have attempted to apply the law extraterritorially). AcmeDigital could find itself forced to remove links to some of the publicly-available articles it recommends in iGobble, something it would not have had to do in Canada. For example, if an old review mentions a disgraced chef who was once fired from an otherwise reputable restaurant, that chef could invoke his right to be forgotten.

It is worth noting that Canadian courts recently introduced a precedent that creates some ambiguity around the question of the right to be forgotten. In February 2017, a federal court ruled in the matter of a Romanian company that was republishing Canadian judicial and tribunal decisions and demanding payment from those involved in exchange for the files' swift removal. Although the materials were already in the public domain, they were not indexed on Google. The court ruled that this was a breach of Canadian privacy law, but did not rule on the proper enforcement mechanism. This leaves open the question of whether this sets a precedent for a European-style right to be forgotten—or even a French-style one, given the company in question operates in Romania.[188]

For the time being, however, there is no explicit right to be forgotten in Canada and no statute enforcing one, meaning this is not a requirement AcmeDigital will have had to comply with before.

The right to explanation

The EU's right to explanation, which will come into force with the GDPR, could pose a significant challenge to AcmeDigital's work. For example, the possibility that a user might experience an allergic reaction to a food recommended by iGobble, could conceivably lead to an argument that the recommendations may have 'significant or legal effects' under the GDPR, requiring AcmeDigital to explain any of iGobble's decisions on demand.

A user with an undiagnosed allergy who has such a reaction may wish to know why iGobble recommended that food item, AcmeDigital's team would have to go through the logs for that individual user and come up with an intelligible explanation for why the algorithm drew the conclusions that it did on the basis of the data it had access to. This is a complex and potentially very costly requirement.

Moreover, even if such a scenario never occurs, the mere potential for it could be sufficient for the right to explanation to apply in other cases. Some users may, for example, worry that certain foods were recommended due to ethnic profiling. While Canadian app developers might be forgiven for lacking awareness of the many politically-charged European ethnic distinctions, they may nevertheless have to account for whether their algorithm had included in its analysis subtle ethnic markets of which they were permissibly ignorant.

Tax

Canada offers some of the world's most generous tax credits for collaborative R&D. For example, a business in Ontario can take a 60% flat tax credit when it funds R&D taking place in Canadian universities, which is a strong encouragement for AcmeDigital to maintain some of its research in Canada. Similarly, however, France also has tax breaks for R&D, called the *crédit d'impôt recherché* (CIR), which helps to persuade French start-ups to keep their research teams in France when expanding into the United States.[189] All businesses consider taxation when relocating, but research-driven start-ups face particular contrasts and incentives when moving across borders.

6 IMPACT OF ICT POLICY ON TRANSATLANTIC RESEARCH AND INNOVATION

Technology has changed the methods companies, whether multinational enterprises or SMEs, use to innovate. For them, innovation is now commonly a cross-border, round-the-clock process with product design and development offices spread across multiple time zones working on developing a new offering (whether a product or a service). At the same time, innovation is also increasingly 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.[190] In essence, innovation has been internationalized, and 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.[191] What this means is that data, design files, project management systems, video conferencing, and more, need to flow seamlessly across borders to support the innovation process itself.

Data flows

At the same time, as this report has noted, data is increasingly the source of the innovation itself. Indeed, it is the ability to extract actionable, real-time insight from data (e.g., through data analytics, data mining, machine intelligence, etc.) that is increasingly driving value creation across the global economy. This dynamic explains why 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.[192] It is why the global value of international data flows exceeded the value of global merchandise trade for the first time in 2015. And it is why, going forward, TEKES, Finland's Technology and Innovation Agency, estimates that, by 2025, fully half of all value generated in the global economy will be created digitally. Even already, 22 percent of global economic output can be attributed directly to the digital economy and it's further expected that the continued application of emerging digital technologies—such as cloud computing, data analytics, and the Internet of Things—will increase global GDP by another $2 trillion by 2020. It is further worth noting that 75 percent of this value created by data moving across the Internet accrues to traditional industries.[193]

In short, organizations use data to create better insights, which, in turn, leads 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.[194] Countries that enact barriers to data flows make it harder and more expensive for their companies to gain exposure, and 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 also 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 ones (if they do so at all). Local data storage requirements—also known as data localization—undermines 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 their own innovation.[195]

Smart manufacturing

The EU, the United States, and Canada, are all investing in the promise of smart manufacturing (broadly called "Industry 4.0" in Europe), which refers to the application of information and communications technologies to every facet of modern manufacturing processes.[196] The digitalization of manufacturing will transform how

products are designed, fabricated, used, and serviced post-sale as much as it will transform the operations, processes, and energy footprint of factories and the management of manufacturing supply chains. ICT-enabled smart manufacturing approaches are 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 Industry 4.0. The European Union's Horizon 2020 program plans to allocate €17 billion ($19 billion) for "leadership in deploying six key enabling and industrial technologies," including advanced manufacturing, through 2020, including investing a total of €7 billion ($7.8 billion) in a "Factories of the Future" public-private partnership to develop the blueprints for a smarter manufacturing sector in the European Union.[197] For its part, 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 constitutes a $200-million fund 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.[198]

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 due to the administrative burden required to abide by the current Horizon 2020 grant regulations. One major example of this is that the financial reporting required for Horizon 2020 grants includes line-by-line data entry of individual budget line 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 scenes unnecessarily and expensively burdensome.

Nevertheless, Horizon 2020 is trying to reduce the administrative barriers for the participation of non-European countries. One example is the last modification on April 2017 of the article 14a) of the grant agreement template where a new figure has been added, the so called International partners. They are allowed to participate in H2020 grants without signing the grant agreement.

While Horizon 2020 has a whole set of fellowships and grants, e.g., Maria-Skłodowska Curie Awards and the prestigious European Research Council (ERC) grants, that allow and even 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 actively 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 toward encouraging U.S. researchers to engage in research activities having partnerships at European institutions.

Finally, whereas many European institutions and research 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 actually incentivize their researchers to engage in international/global research partnerships. In contrast, European, some Canadian, and even 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 the EU, the United States, and Canada is how each ensures data protection and privacy. As noted, the United States tends to take a sectoral approach and does not try to enact border check points to control where personal data is transferred, but instead stipulates that the company transferring the data ensure it protects the data, as required by U.S. law, wherever it is stored. America's sector-by-sector approach to privacy regulation has its strengths and weaknesses. American policy toward data protection has tended to give consumers more power over controlling their privacy settings in order to leave open greater space for business model experimentation. On the other hand, it means that enterprises that compete in multiple sectors have to understand and respond to multiple privacy 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, PIPEDA in Canada and the incoming GDPR in the EU both 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, in terms of the limitations on companies providing services based on personal data.

The GDPR requires organizations to implement a wide range of data protection measures. These include accountability measures such as: privacy impact assessments, audits, policy reviews, activity records and (potentially) appointing a Data Protection Officer (DPO).[199] The GDPR may require the assignment of 75,000 or more data protection officers for businesses to comply with the regulation's requirements.[200] Yet this requirement, in particular, for DPOs for companies above a certain size will add significant costs that may actually harm digital innovators operating in Europe. 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 €7,200.00 in additional compliance costs per year.[201] As Paul Hofheinz of The Lisbon Council writes, "This, in turn, would suppress jobs in some sectors, reducing employment by as much as 0.6% in particularly heavy hit industry."[202] 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, it could boost competition between firms by making it easier for companies to get their hands on pre-existing customer data.

Still, the GDPR may make it difficult for digital producers to provide more and higher-quality or lower-priced services, which will reduce adoption. This explains why, in analyzing the impact of the European Union's 2002 Privacy and Electronic Communications Directive, Avi Goldfarb and Catherine Tucker found that it resulted in an average reduction in the effectiveness of online ads of approximately 65 percent.[203] The authors write "the empirical findings of this paper suggest that even moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all Web sites, and that the costs should be weighed against the benefits to consumers."[204] If European advertisers reduced their spending on online advertising in line with the reduction in effectiveness resulting from stricter privacy regulations, "revenue for online display advertising could fall by more than half from $8 billion to $2.8 billion" the authors found.

7 RECOMMENDATIONS AND CONCLUSIONS

The objective for improving transatlantic cooperation on ICT research and innovation and business should not be to eliminate policy differences—which, besides anything else, is impossible. It should be to develop a set of measures that acknowledge these differences and establish as much common ground as possible for cooperation that maximizes the economic benefits of ICT innovation for the EU, the United States, and Canada. This section presents a set of recommendations as to how transatlantic policymakers can achieve this.

7.1 Intellectual Property

Support the free movement of knowledge
To support cross-border research and innovation, 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&I 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 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, promotes 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 for which the trade secret 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]

7.2 Data Protection

Keep data protection rules simple
Overly 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 EU's incoming General Data Protection Regulation (GDPR) creates complex data handling requirements that, while they will require companies to hire more workers to comply with, 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 European, Canadian and American firms know what they must do in order to comply with the law in each market. In addition, the European Union, Canada, and the United States should prevent their respective member states, states, and provinces from obstructing the development of a digital single market 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 pointless 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 currently prohibits foreign transfers of EU personal data, unless the other country's domestic laws are deemed adequate, or there is an international agreement protecting the data. 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 to comply with data protection rules simply by storing EU personal data outside Europe. Moreover, storing it in Europe does not protect it from adversaries abroad: that is a question of proper security.[214]

The EU, the United States, and Canada, should come to an agreement on the free flow of data, and 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
As mentioned above, 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 undermine 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. The EU, Canada, and the U.S. 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
The three actors, 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]

7.3 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 them should ensure they do not impact people outside their jurisdiction.

Stop protectionist ICT procurement policies
The EU, the United States, and Canada have all ratified the Information Technology Agreement (ITA), which commits them to the removal of tariffs and discriminatory taxes on ICT. While such trade barriers have not completely vanished, they are substantially lower than in non-signatory countries. However, non-tariff barriers remain a problem.[219] These are particularly pronounced in procurement policy.

One example is data localization requirements, not just in privacy law, but also in public sector procurement rules.[220] As discussed above, data localization should be abolished. A similar barrier is public sector procurement rules that give preference to local suppliers. This freezes out international competition, which allows domestic firms to charge the taxpayer higher prices, and removes an important driver of innovation.[221]

The EU, the United States, and Canada should agree to regulations against protectionism in ICT procurement, and should encourage bids for European, Canadian and American tenders from firms based in the other two markets.

7.4 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.[222] 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.[223] 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 EU-Canada ICT cooperation already established, the three entities should pull these 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 the EU, the United States, and Canada.[224]

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, or Canadian Tri-Council Agencies (the Canadian Institutes of Health Research (CIHR), the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council (SSHRC). The EU, the Unites States, and Canada should also each set a target for 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.[225]

Boost cooperation between regional bodies
Transatlantic ICT cooperation should go beyond policymakers in Washington, Ottawa, and Brussels: there should also be cooperation involving American states, Canadian provinces, and European countries, 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." The European Union, the United States, and Canada 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.[226]

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, made up of the most effective measures from across Europe and North America.

Promote tech literacy among legislators
MPs, MEPs, representatives, senators, and ministers will have a better chance of drawing up good regulations if they understand properly what they are regulating. Legislators in the EU, the United States, and Canada, 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. The EU, the United States, and Canada, should also work together on emerging and future issues, such as tech-driven economic phenomena in the labor market.

Revive and revise the Transatlantic Trade and Investment Partnership (TTIP)
The United States and the European Union should work to revive TTIP negotiations, which halted in September 2016, when regulators could not overcome political sensitivities. But the success of CETA emphasizes the fact 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.

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 facilitates. 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).[227] 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.

ACKNOWLEDGMENTS

DISCOVERY has been in operation since January 2016 and in this time has contributed to enhanced dialogue between researchers, innovators, industry and policy-makers through its capacity building workshops, the ICT Discovery lab and the Transatlantic ICT Forum – all of which have been facilitated and supported by DISCOVERY.

More specifically, under the umbrella of the Transatlantic ICT Forum, the project has established and supported a dedicated **Working Group on ICT Policy and Regulations**, whose discussions and recommendations presented, have dutifully informed this input paper.

ICT Policy and Regulations Working Group Members:

Chair:
Camille Sailer, President and CEO, EACCNJ

Members:

- Benoit Van Asbroeck, Partner at Bird & Bird
- Debbie Kemp, Deputy Director, Innovation Outreach at Foreign Affairs, Trade & Development Canada.
- María Fernanda Cabrera, Innovation Director, UPM
- James Gumble, Business Intelligence, XPAND
- Joann Halpern, Founder, German Center For Research And Innovation (GCRI)
- Kate Sellen Professor, OCAD University
- Maarten Botterman, Founder and Director, GNKS
- Marco Marinucci, Co-Founder And Managing Partner, Mts Venture Partners
- Marko Turpeinen, Director, Silicon Valley Hub, EIT Digital
- Michael Willmott, Mission of Canada To The EU
- Nick Wallace, Senior Policy Analyst, Center for Data Innovation
- Patrick Consorti, EU-US Industry Partnerships, EIT Digital
- Sabina Guaylupo, Senior Consultant, INMARK
- Stephen Ezell, Vice President, Global Innovation Policy, ITIF
- Tim Bennett, Director-General/CEO, TABC
- Yolanda Ursa, Director of Innovation Management, INMARK

REFERENCES

[1] *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://eur-lex.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

[2] *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

[3] *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

[4] *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

[5] *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

[6] *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

[7] *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

[8] *Directive 2011/77/EU*

[9] *Directive 2006/116/EC*

[10] *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

[11] *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

[12] *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

[13] 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

[14] 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

[15] *DRAFT REPORT on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market* http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.094&format=PDF&language=EN&secondRef=01

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

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

[17] *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;

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

[18] *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC* http://data.consilium.europa.eu/doc/document/ST-9611-2016-INIT/en/pdf

[19] Council of the European Union (2017, February 7), "Portability of Digital Content Services: EU Presidency-Parliament agreement" http://www.consilium.europa.eu/en/press/press-releases/2017/02/07-portability-digital-content-services/

European Commission (2017, May 10) "Digital Single Market: Commission calls for swift adoption of proposals and maps out challenges ahead" http://europa.eu/rapid/press-release_IP-17-1232_en.htm

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

[21] *U.S. Patent Act 1952* https://www.law.cornell.edu/patent/patent.overview.html

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

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

[24] *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

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

[26] *H.R. 6071: Trademark Counterfeiting Act of 1984* https://www.govtrack.us/congress/bills/98/hr6071

[27] USPTO (2010, February 10) *State Trademark Information Links.* Last updated January 10, 2017. https://www.uspto.gov/trademarks-getting-started/process-overview/state-trademark-information-links

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

[29] https://www.usitc.gov/intellectual_property.htm

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

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

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

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

[34] Keith Bird, (2008) "Significant Differences Between Canadian and American Patent Law" *McMillan* http://www.mcmillan.ca/Significant-Differences-Between-Canadian-and-American-Patent-Law

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

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

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

[38] Government of Canada (2016) *A Guide to Copyright* Last Updated November 15, 2016,

https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/h_wr02281.html

[39] Ibid

[40] Schabas, P Fischer, I and DiMatteo, C (2013) "Canada's Copyright Modernization Act: A Delicate

Rebalancing of Interests", *Media Law Resource Center*

http://www.medialaw.org/component/k2/item/1820-canada%E2%80%99s-copyright-modernization-act-a-delicate-rebalancing-of-interests

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

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

[43] Robertson, G (2012, February 8) "Unlocking Bill C-11: What are digital locks, and why should you care?", *Fulcrum,* February 8, 2012,

http://thefulcrum.ca/news/unlocking-bill-c-11-what-are-digital-locks-and-why-should-you-care/

[44] *Copyright Modernization Act*, S.C. 2012, c. 20., 41st Canadian Parliament (2012).

[45] 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

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

[47] *EUROPEAN CONVENTION ON HUMAN RIGHTS* http://www.echr.coe.int/Documents/Convention_ENG.pdf

[48] Convention 108 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[49] *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

[50] *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

[51] European Economic Area Agreement http://publications.europa.eu/resource/cellar/c692168c-a25b-4a3c-aade-ca872bb93f69.0007.02/DOC_1

[52] *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

[53] *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

[54] *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

[55] Castro, D and McQuinn, A (2017, January 11) "France, you do not own the internet" *Computerworld* http://www.computerworld.com/article/3156296/internet/france-you-do-not-own-the-internet.html

[56] *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

[57] *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; European Commission (2017, January 10) *Proposal for a Regulation on Privacy and Electronic Communications* https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

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

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

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

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

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

[63] NAIC, *State Insurance Regulation* 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

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

[65] Equifax (2017) *FCRA Summary of Rights* https://www.equifax.com/privacy/fcra

[66] *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/

[67] 18 U.S.C. § 2710 (2002) http://uscode.house.gov/browse/prelim@title18/part1&edition=prelim

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

[69] *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

[70] Ibid

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

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

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

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

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

[76] *Ibid*

[77] *Ibid*

[78] Office of the Privacy Commissioner of Canada, Overview of Privacy Legislation in Canada, Updated May 2014,

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15 /

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

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

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

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

[83] *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

[84] *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

[85] *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

[86] *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

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

[88] 5 U.S. Code Chapter 5 – Administrative Procedure. https://www.law.cornell.edu/uscode/text/5/part-I/chapter-5.

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

[90] 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

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

[92] Marine Stewardship Council, "About us" https://www.msc.org/about-us

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

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

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

[96] Department of Transportation (2016, September) *Federal Automated Vehicles Policy* https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016 ;

Dept. Transportation, *Unmanned Aircraft Systems* updated March 31, 2017 https://www.faa.gov/uas/

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

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

[99] Robert Atkinson (2012) *Incentives for Capital Investment and Manufacturing: Hearing on Tax Reform Options Before the Senate Finance Committee*, written testimony.

[100] Joe Kennedy (2014, March) "Assessing U.S. Corporate Tax Reform in an Age of Global Competition" *ITIF* http://www2.itif.org/2014-corporate-tax-reform-global-competition.pdf

[101] Luke A. Stewart, Jacek Warda, and Robert D. Atkinson (2012, July) "We're #27!: The United States Lags Far Behind in R&D Tax Incentive Generosity" *ITIF* http://www2.itif.org/2012-were-27-b-indextax.pdf

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

[103] Campbell, AF (2017, April 2016) "It turns out Trump is open to a border adjustment tax after all" *Vox* http://www.vox.com/policy-and-politics/2017/4/26/15434326/trump-border-adjustment-tax

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

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

[106] Statutory Instruments Act http://laws-lois.justice.gc.ca/eng/acts/S-22/

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

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

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

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

[111] Digital Advertising Alliance of Canada, "About the DAAC" Accessed May 17, 2017, http://youradchoices.ca/about-the-daac/.

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

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

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

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

[116] European Commission, "Factsheet: Horizon 2020 Budget" http://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_horizon2020_budget.pdf

[117] Eurostat (rd_e_gerdtot)

[118] Kenneth Flamm, (1987) *Targeting the Computer: Government Support and International Competition*, Washington, DC: Brookings Institution

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

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

[121] Matt Stepp et al. (2013, June), "Reimaging the National Labs in the 21st Century Innovation Economy," Information Technology and Innovation Foundation, Center for

American Progress, and the Heritage Foundation, http://www2.itif.org/2013-turning-the-page.pdf.

[122] 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

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

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

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

[126] ; Atkinson, R.D. (2014, June) "Understanding the U.S. National Innovation System" *ITIF* http://www2.itif.org/2014-understanding-us-innovation-system.pdf

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

[128] National Institute of Standards and Technology (2014, February 12) "Framework for Improving Critical Infrastructure Cybersecurity" 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

[129] Department of Transportation, "Smart City Challenge" Last Updated January 20, 2017 https://www.transportation.gov/smartcity

[130] US Ignite "Global City Teams Challenge" https://www.us-ignite.org/programs/global-city-teams-challenge/

[131] NIST "Global City Teams Challenge" https://www.nist.gov/el/cyber-physical-systems/smart-americaglobal-cities

[132] 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/.

[133] 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.

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

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

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

[137] National Oceanic and Atmospheric Administration, "Big Data Project" http://www.noaa.gov/big-data-project

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

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

[140] 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.

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

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

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

[144] For example, see the University of Manitoba Technology Transfer Office. Government of Canada "University of Manitoba," 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

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

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

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

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

[149] Standards Council of Canada, "About the Standards Council of Canada,", accessed May 5, 2017, https://www.scc.ca/en/about-scc.

[150] Standards Council of Canada "Participate in committee work—Electronics, information technology and telecommunications,", accessed May 5, 2017, https://www.scc.ca/standards/get-involved-in-standardization/committees?field_sector_value_i18n=4 ; [150] 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.

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

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

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

[154] Ibid.

[155] EPO and EUIPO (2016, October), "Intellectual property rights intensive industries and economic performance in the European Union" 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

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

[157] Carmen-Cristina Cîrlig (2014, July) '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

[158] Ibid, page 8

[159] *AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS*

(as amended on 23 January 2017)
https://www.wto.org/english/docs_e/legal_e/31bis_trips_e.pdf

[160] European Commission, "THE EU'S FREE TRADE AGREEMENT WITH CANADA AND ITS INTELLECTUAL PROPERTY RIGHTS PROVISIONS"
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

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

[162] Ibid, Article 20.11

[163] *Ibid*, Article 20.30

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

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

[166]*Directive 95/46/EC;*
Regulation (EU) 2016/679 (GDPR)

Articles 45-46 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[167] Nigel Cory and Robert Atkinson (2016, April), "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" *Information Technology and Innovation Foundation*,
http://www2.itif.org/2016-financial-data-trade-deals.pdf

[168] *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

[169] *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

[170] *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

[171] *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

tificial-intelligence.htm"
http://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm

[173] Janet Steinmann (2013, October 18) "Book Review: A Guide to the Personal Information Protection and Electronic Documents Act 2013" *IAPP*, https://iapp.org/news/a/book-review-a-guide-to-the-personal-information-protection-and-electronic-d/

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

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

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

[174] European Commission, "EU - US Cooperation" Last updated April 28th, 2017. https://ec.europa.eu/growth/industry/international-aspects/cooperation-governments/eu-us_en

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

[175] *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

[176] Ben Miller and Robert D. Atkinson (2014, October) 'Digital Drag: Ranking 125 Nations by Taxes and Tarrifs on ICT Goods and Services', *Information Technology and Innovation Foundation*, http://www2.itif.org/2014-ict-taxes-tariffs.pdf?_ga=1.167471038.1045463480.1471968194

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

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

Simon Marks and Hans Von Der Bouchard (2016, November 9) "Europe to Trump: Don't give up on free trade" *Politico*, 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 (2017, April 20) "Trump moves towards imposing tariffs on steel imports" *Financial Times* https://www.ft.com/content/d8413fe8-25e6-11e7-8691-d5f7e0cd0a16

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

[179] *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

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

[181] European Commission (2016, October) "Roadmap for EU-USA S&T cooperation" 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.

[182] *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

[183] European Commission (2016, October 17) "Implementing Arrangement" http://ec.europa.eu/research/iscp/index.cfm?pg=usa

http://ec.europa.eu/research/iscp/index.cfm?pg=canada

[184] Open Data Charter "G8 Open Data Charter and Technical Index" http://opendatacharter.net/resource/g8-open-data-charter/

[185] Open Gov Partnership, "Participating Countries" https://www.opengovpartnership.org/countries

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

[187] European Commission (2014) *Standardisation in the area of innovation and technological development, notably in the field of Text and Data Mining: Report from the Expert Group* DG Research & Innovation, http://ec.europa.eu/research/innovation-union/pdf/TDM-report_from_the_expert_group-042014.pdf

[188] Michael Geist (2017, February 6) "Did a Canadian court just establish a new right to be forgotten online?" *The Globe and Mail* http://www.theglobeandmail.com/report-on-business/rob-commentary/did-a-canadian-court-just-establish-a-new-right-to-be-forgotten-online/article33915916/

[189] Nick Wallace (2017, February 8) "5Q's for Franck Carassus, co-foudner of OpenDataSoft" *Center for Data Innovation* https://www.datainnovation.org/2017/02/5-qs-for-franck-carassus-co-founder-of-opendatasoft/

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

[191] Ibid.

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

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

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

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

[196] Stephen J. Ezell, (2016, November), "A Policymaker's Guide to Smart Manufacturing," Information Technology and Innovation Foundation, https://itif.org/publications/2016/11/30/policymakers-guide-smart-manufacturing.

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

[198] http://www.feddevontario.gc.ca/eic/site/723.nsf/eng/h_01855.html; http://www.cme-smart.ca/home-en.

[199]

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

[201] Lauritis R. Christensen, Andrea Colciago, Federico Etro and Greg Rafert, The Impact of the Data Protection Regulation in the EU (Denver: Analysis Group, 2013).

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

[203] Avi Goldfarb and Catherine E. Tucker, (2010, August, 4), "Privacy Regulation and Online Advertising," SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

[204] Daniel Castro, (2010, September, 8), "Stricter Privacy Regulations for Online Advertising Will Harm the Free Internet," Information Technology and Innovation Foundation, http://www.itif.org/files/2010-privacy-regs.pdf?_ga=2.264467530.499167230.1493989310-885725058.1493645549.

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

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

[207] 'Uniform Law Commission' (2013) "Legislative Facts Sheet – Trade Secrets Act," 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" Information Technology and Innovation Foundation, October 2013, http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf?_ga=1.133188494.1045463480.1471968194

[209] Nick Wallace (2017, January 10) "Norwegian Watchdog Turns Fire on Fitness Trackers and Misses the Mark Entirely" *Center for Data Innovation* 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 (2012, November 15) "Economics of Privacy" MIT Sloan and NBER, http://www.ftc.gov/sites/default/files/documents/public_events/fifth-annual-microeconomicsconference/tucker.pdf.

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

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

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

[214] Ibid,
Daniel Castro and Alan McQuinn (2015, February) "Cross-Border Data Flows Enable Growth in All Industries", *Information Technology and Innovation Foundation*, 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' Information Technology and Information Foundation, March 2016, http://www2.itif.org/2016-unlocking-encryption.pdf?_ga=1.132817550.1045463480.1471968194

[217] Daniel Castro (2013, December) "The False Promise of Data Nationalism" The Information Technology and Innovation Foundation, http://www2.itif.org/2013-false-promise-data-nationalism.pdf

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

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

[218] Castro, D and McQuinn, A (2017, January 11) "France, you do not own the internet" *Computerworld* http://www.computerworld.com/article/3156296/internet/france-you-do-not-own-the-internet.html

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

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

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

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

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

[224] Michelle Wein and Stephen J Ezell, "How to Craft an Innovation Maximizing T-TIP Agreement" (2013, October) Information Technology and Innovation Foundation, http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf?_ga=1.133188494.1045463480.1471968194

[225] Stephen Ezell, Adams Nager, Robert Atkinson (2016, January) "Contributors and Detractors: Ranking Countries" Impact on Global Innovation' *Information Technology and Innovation Foundation*, http://www2.itif.org/2016-contributors-and-detractors.pdf

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

[227] Nigel Cory (2017, January) "The Worst Innovation Mercantilist Policies of 2016" *Information Technology and Innovation Foundation*. http://www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf ; Nick Wallace (2017, March 8) "European Commission Should Stand Firm on Free Data Flows" *Center for Data Innovation* https://www.datainnovation.org/2017/03/european-commission-should-stand-firm-on-free-data-flows/