TTIP AND INFORMATION COMMUNICATION TECHNOLOGY
The Information and Communication Technology (ICT) sector is an important economic driver in both the US and EU, which together make up almost 50% of the global ICT market. Trade in ICT involves both the provision of products (for example, computer hardware, software, and telecommunications equipment) and services (for example software development and financial services provision). ICT industry groups have therefore been eager to ensure that TTIP improves conditions for the technology sector and enhances market access. However, the ICT negotiations also touch on several sensitive areas that could result in a loss of privacy, safety, and security for individuals, and as such civil society groups have also been paying close attention to TTIP’s developing legal framework.

TTIP will likely affect the ICT sector in numerous ways. To begin with, it is probable that TTIP will reduce or eliminate tariffs on ICT goods and services, allowing US and EU manufacturers to expand their market access across the Atlantic. More significantly, however, TTIP will likely lead to a greater degree of regulatory cooperation between the US and EU on laws governing the ICT industry. According to the European Commission’s Factsheet on Information and Communication Technology (ICT), the EU’s goals for regulatory cooperation on ICT in TTIP are:

- To “set up ways of working together to better enforce regulations in the EU and US”;
- To “increase cooperation between regulators” in order to “avoid unnecessary differences in our rules and guarantee a high level of consumer protection”; and
- To “set common principles for certifying IT products, especially for encoding and decoding information (‘cryptography’ in the jargon).”

With respect to the second point, the EU is particularly interested in pursuing regulatory cooperation in the areas of:

- “e-labelling” — setting standards for providing product information to consumers in electronic format, where this replaces labels and stickers for items with an integrated electronic display e.g. smart watches;
- “e-accessibility” — making ICT easy to use for people with disabilities; and
- “interoperability” — enabling users to exchange data easily between different products.

In addition, the Commission issued a 20 March 2015 Position Paper on intellectual property (IP) in TTIP, which proposes “binding commitments on a limited number of significant IP issues” including some regulatory cooperation on ICT-relevant areas such as customs enforcement, patent procedures, and copyright.

Some of TTIP’s probable interventions in regulatory cooperation on ICT are relatively unproblematic. For example, ensuring number portability (the ability to keep the same phone number when switching operators) and strong competition (antitrust) rules in the telecom industry could be positive steps. However, as noted above, the ICT negotiations also touch on several sensitive areas that could result in a loss of privacy, safety, and security for individuals.

DATA PROTECTION AND PRIVACY

The exchange of data across borders is an important part of contemporary life. Companies must be able to communicate with their international branches, individuals must be able to access their data from various locations, and producers must be able to sell and service their ICT products overseas. TTIP could help to reduce barriers to e-commerce and data flows by improving regulatory cooperation between the EU and US. Trade associations like the European Services Forum have advocated for such cooperation to ensure the smooth functioning of the international ICT market.

However, civil society groups have expressed concern that such cooperation could result in a ‘race to the bottom’ for safety and privacy standards. Concerns about privacy and data protection have become particularly important in the wake of revelations regarding spying activities by the US government, controversy over the EU Directive on Data Protection (putting in place EU rules to protect the privacy and security of personal data) and Safe Harbour Directive (a recently-overturned work-around that had allowed some US companies to comply with EU privacy and data protection rules, despite the US’s lack of a national protection regime), and the continued threat of data breaches orchestrated by criminals seeking financial gain.

The result has been a struggle between civil society groups campaigning for enhanced privacy rules that would limit the ways that data can be used and shared by companies and governments, businesses advocating more regulatory cooperation and greater freedom to use data for commercial purposes, and the US government’s insistence on its power to gather data for its own activities.

This battle over privacy rights and civil liberties is compounded by the complex legal rules that currently govern the exchange of data between the US and EU. Under the EU’s current Data Protection Directive, EU companies cannot send personal data to countries outside the European Economic Area, including the US, unless there is a guarantee that such data will be protected. This protection could come in the form of a country’s legal regime providing adequate protection (which the US regime does not currently do, since to date it has passed no comprehensive data protection laws), or from US companies themselves if they operate under binding corporate rules, under model contracts, or— until recently—self-certify that they comply with the Safe Harbour Directive. This area of law is currently in flux, however, as the European Court of Justice on 6 October 2015 invalidated the Safe Harbour Decision, stating that “legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.” In response, the EU and US agreed on 2 February 2016 to a new ‘Safe Harbour 2.0’ framework for transatlantic data flows: the EU-US Privacy Shield. In the meantime, a new General Data Protection Regulation (GDPR) has been approved by the EU Parliament’s Civil Liberties Committee, and may soon come to replace the 20-year-old Data Protection Directive.
INTELLECTUAL PROPERTY

Another area of concern for the ICT sector is the protection of intellectual property (IP) in ICT products. Because digital products and designs can easily be shared across platforms and borders, ICT producers often rely heavily on copyright and patent law to protect their interests. ICT industry associations have advocated using TTIP to enhance IP protection by strengthening IP regulations, coordinating US and EU law enforcement efforts, and other mechanisms.

However, strengthening IP protection comes with a number of costs. As demonstrated by the 2012 protests against the Anti-Counterfeiting Trade Agreement (ACTA), which ultimately resulted in the rejection of that agreement by the European Parliament, civil society has many important concerns regarding how expanding IP rights could come at the cost of freedom of expression, privacy, and the public interest. Overly broad IP protections privatize knowledge and shrink the public domain, and can lead to problems such as creating patent trolls, encouraging abusive copyright suits against fair uses of images, text, and music, and expanding realms of civil liability for ordinary citizens.

INTERNATIONAL RULES

One final point of concern for civil society activists is the potential for any agreements reached under TTIP to become ‘globalized’. A significant aim of ICT producers and trade associations has been the creation of international standards for ICT regulation. Because the ICT market is so globalized, they argue, maintaining diverse national and regional regulations only serves to impede the market, and international regulations would be vastly preferable.

A number of international ICT standards are already in existence, and such standards are not objectionable per se, but it is important to maintain a close eye on their continued development in order to ensure that global regulatory standards uphold high levels of protection for privacy, data security, safety, and fundamental rights, and do not enshrine overly restrictive IP regimes. Because TTIP would create rules covering nearly half of the global ICT market, it would be a natural baseline on which to build future versions of international regulatory standards. This means that any data protection and intellectual property rules written into TTIP are of potentially global importance.


3. The Comprehensive Economic and Trade Agreement (CETA) between Canada and the EU, for example, will reduce tariffs on ICT products to zero, and the TTIP is likely to follow a similar path.


5. Id.


9. For example, the European Consumer Organisation (BEUC) has expressed concern that “including data flows in TTIP will result in a significant weakening of consumers’ fundamental rights to privacy and to the protection of personal data.” The European Consumer Organisation (BEUC), “Position Paper and Factsheet: Data Flows in TTIP,” 2015.


14. Case C-362/14, Maximilian Schrems v Data Protection Commissioner, 6 October 2015, at para. 94.


22. See, e.g., the WTO Information Technology Agreement; WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).