White Paper on Cybersecurity Policy

Common Ground for EU-US Collaboration

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

TABLE OF CONTENTS

Page

LIST OF ABBREVIATIONS

ANSI: American National Standards Institute

CAN-SPAM: Controlling the Assault of Non-Solicited Pornography and Marketing Act

CERT: Computer Emergency Response Team

CISA: Cybersecurity Information Sharing Act

CLOUD Act: Clarifying Lawful Overseas Use of Data Act

CONSENT: Customer Online Notification for Stopping Edge-provider Network Transgressions Act

COPPA: Children´s Online Privacy Protection Act

cPPP: Contractual Public-Private Partnerships

CSIRT: Computer Security Incident Response Team

CSDP: Common Security and Defense Policy

DHS: Department of Homeland Security

DSP: Digital Service Provider

e-Privacy: (Proposed) e-Privacy Regulation

EC3: European Cybercrime Center

ECSO: European Cyber Security Organisation

ECPA: Electronic Communications Privacy Act

EDA: European Defense Agency

ENISA: European Agency for Network and Information Security

EO: Executive Order

FinCEN: Financial Crimes Enforcement Network

FTC: Federal Trade Commission

GDPR: General Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

JCAT: Joint Cybercrime Action Taskforce

MLA: Mutual Legal Assistance

MLAT: Mutual Legal Assistance Treaty

NIS Directive: Network and Information Systems Directive

NIST: National Institute of Standards and Technology

NSA: National Security Agency

OES: Operator of Essential Services

R&I: Research and Innovation

1 INTRODUCTION

There is no doubt that the theme of cybersecurity, both in its broadest sense as well as the multiple sectors with which it intersects, is of paramount importance for transatlantic dialogue. Recent years have seen many pivotal changes in cybersecurity and privacy policy in both the European Union (EU) and the United States (US).

In the EU, two of the world´s most stringent data protection laws are taking effect in 2018: the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive). GDPR regulates how businesses and entities obtain, process and protect user data. Meanwhile, the NIS Directive requires states to establish minimum security requirements in order to increase cyber preparedness.

In parallel fashion, with the passage of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), the US Congress has given American law enforcement authorities the power to obtain personal data from technology companies even if it is stored in data centers in other countries, a decision that has ignited significant debate in Europe. In addition, President Donald Trump is expected to announce his national cyber strategy in the coming months, building on policies of predecessors which could have an effect on current American cyber policies and regulations.

On multiple occasions and in multiple venues, the EU and the US have made it clear that they understand the importance of collaboration on cybersecurity and privacy policy and the immense effects and benefits of such cooperation. In light of rapidly-changing technology advances which affect the policy landscape on both sides of the Atlantic, a judicious analysis of the issues facing the bilateral relationship is indispensable to stimulating benefits. While the transatlantic relationship is second to none economically, there are still major differences of opinion regarding substance and implementation as pertains to cyber policy in the EU and the US.

The AEGIS Project, a Coordination and Support Action (CSA) funded by Horizon 2020 (the EU framework program for research and innovation) that aims to facilitate EU-US dialogue and cooperation in cybersecurity and privacy research and innovation (R&I), has developed this White Paper to capture the current landscape of cybersecurity policies on both sides of the Atlantic.

The AEGIS team has worked hard to craft this White Paper so that it can serve as a comprehensive guide for EU-US dialogue decision makers, the cybersecurity and privacy research communities, cybersecurity industry and business leaders, standardization bodies and funding agencies. The foundation of the White Paper are the unique insights and expertise of a range of highly-regarded relevant thought leaders with vast experience in research, government, academia and the private sector. As a result, the Paper offers meaningful input to aid in furthering the understanding of the complexities of EU-US relations in cybersecurity and privacy R&I from a first-hand perspective.

The guide aims to help the key stakeholders mentioned beforehand understand the current collaborative landscape between both regions, underline some key potential focus areas and propose ideas to promote future transatlantic dialogue.

The Paper focuses on three policy areas: standards and certification; privacy and data protection; and public-private information sharing. It later analyzes the similarities and differences of these policies in as much detail as is practical. We have selected the focus policy areas to present the principal leading themes under recent consideration by both regions that impact bilateral cyber dialogues and research and innovation collaboration between the EU and the US.

In its concluding section, the Paper presents a series of policy recommendations for future EU-US collaboration in cybersecurity and privacy R&I.

2 EU AND US CYBERSECURITY STRATEGIES

The EU and the US have approached establishing cyber preparedness through different perspectives, although both share key priorities in their cybersecurity strategies: protecting critical infrastructures; developing a strong cyber defense policy; and creating an international cyberspace policy. Executing each respective strategy requires an intense and lengthy implementation process and appears to be more streamlined in the EU. Part of this is due to the layers of agencies and processes the US involves in cybersecurity as well as the willingness of the respective legislative bodies to pass regulations. We will discuss the key points of each region´s cybersecurity strategy in the following section.

2.1 EU Cybersecurity Strategy

The EU outlined its cybersecurity strategy in 2013 under the rubric of, "An Open, Safe and Secure Cyberspace."[1] The document summarized the EU´s five strategic priorities and actions in the short and long term and how it would achieve these goals. The following are the priorities established in the EU cybersecurity strategy[2]:

- Achieve cyber resilience
- Drastically reduce cybercrime
- Develop a cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity; and
- Establish a coherent international cyberspace policy for the European Union that promotes core EU values.

Since the document´s publication, the EU has made significant strides in carrying out its cybersecurity strategy. In terms of achieving cyber resilience, the EU has enacted the Directive on Security of Network and Information Systems (NIS Directive), which requires Member States and Operators of Essential Services (OESs) to boost their cybersecurity measures.[3] It has also approved the rigorous General Data Protection Regulation, a law meant to harmonize all data protection laws in the EU and that imposes strict fines on those found to be in violation. The European Parliament is currently working on passing the e-Privacy Regulation on Privacy and Electronic Communications.

The EU is also working on a certification framework for ICT security products as part of its priority to develop cybersecurity industrial and technological resources. This is part of the revised EU cybersecurity strategy.

In September 2017, the European Commission adopted a new cybersecurity package, "Resilience, Deterrence and Defence: Building Strong Cybersecurity in Europe." The package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience, deterrence and response. It includes the establishment of a stronger European Union Cybersecurity Agency built upon the basis of the Agency for Network and Information Security (ENISA) to assist Member States in dealing with cyberattacks and the creation of an EU-wide cybersecurity certification scheme that aims to increase the cybersecurity of products and services in the digital world.[4]

The new strategy also proposes the creation of a Network of Cybersecurity Competence Centers in Member States and a European Cybersecurity Research and Competence Center. Working with Member States, these entities will help develop and roll out the tools and technology needed to keep up with ever-changing threats and make sure European defense is as strong as possible.[5] According to the

Commission, the objectives of the networks and the center would be to stimulate development and deployment of technology in cybersecurity and to complement the capacity-building efforts in this area at an EU and national level.[6] The creation of these entities compliments capacity-building efforts in cybersecurity at an EU and national level.[7]

The laws mentioned, including the proposed e-Privacy Regulation, would apply to all companies doing business in the EU, regardless of whether they are established there. As a whole, therefore, they represent a significant step towards achieving a coherent international cyberspace policy.

2.2 US Cybersecurity Strategy

Mapping cyber capabilities in the US in a comprehensive way can be challenging since multiple agencies can embark on multiple initiatives. The US released its first International Strategy for Cyberspace under President Barack Obama in 2011.[8] It was the first time any presidential administration had published its vision and goals for cyberspace and cybersecurity.[9] The strategy included several policy initiatives, which the Obama Administration described as "action lines of our strategic framework," and included the following:[10]

- Promote international standards and innovative, open markets
- Protect US networks by enhancing security, reliability and resiliency
- Extend collaboration with international law enforcement and extend the rule of law
- Prepare the military for 21st century security challenges
- Promote effective and inclusive internet governance structures
- Work on international development by building capacity, security and prosperity; and
- Support fundamental internet freedom and privacy.

The Obama Administration also outlined its cybersecurity priorities that it enacted through Presidential Executive Orders and Presidential Directives. The Administration´s priorities on cybersecurity were the following[11]:

- Protect the nation´s critical infrastructure from cyber threats
- Improve the nation´s ability to identify and report cyber incidents in a timely manner
- Engage with international partners to promote internet freedom and build support for an open interoperable, secure and reliable cyberspace
- Secure federal networks by setting clear security targets and holding agencies accountable for meeting those targets; and
- Create a cyber-savvy workforce.

Through its legislative powers, the US Congress also promotes its own priorities as well as enacts regulations related to presidential cybersecurity priorities such as the landmark Cybersecurity Information Sharing Act (CISA), which encourages public-private information sharing to deter and contain threats.

As in the EU, the US has also developed and sponsored "competence centers" or the equivalent through programs at its various federal agencies. Its main approach has been partnering with the private sector and academia. This stance is reflective of the priorities outlined by the Obama Administration and supports the over-arching objective of creating a cyber-educated workforce.

An example of this effort includes the National Centers of Academic Excellence in Cyber Defense program, an initiative jointly sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). Separately, the NSA also has its National Centers of Academic Excellence in Cyber Operations, which aim to advance efforts to build a digital nation and increase the number of skilled workers capable of supporting a "cyber-secure" nation.

In 2017, President Donald Trump signed Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." This EO aims to increase the cybersecurity of federal networks, improve cybersecurity of the nation´s critical infrastructure and improve the nation´s overall cybersecurity by: engaging with international allies; ensuring the nation has strategic options to deter adversaries; and training a cybersecurity workforce.[12]

President Trump is expected to release an updated national cybersecurity strategy by the end of 2018.[13]

3 KEY CYBERSECURITY POLICIES FOR EFFECTIVE EU-US COLLABORATION

Cybersecurity policy goals and objectives in both the EU and the US are products of the technological disruptions occurring around the globe. These disruptions are helpful in highlighting issues of cooperative reflection that greatly influence the three planks of this Paper: standards and certification; privacy and data protection; and public-private information sharing. In the following section, we analyze key policies in these areas that have been enacted or are currently being considered as new regulations.

3.1 Standards and Certification

One of the key cybersecurity policies areas that has received much attention over the last few years in the US and the EU is standards. In this area, the EU is currently leading the effort to improve overall cybersecurity and privacy preparedness and protections with Directive on Security of Network and Information Systems (NIS Directive), a policy which went into effect in 2018. In general, the NIS Directive requires all Member States, Operators of Essential Services and Digital Service Providers (DSP) to have minimum cybersecurity standards in place.

The NIS Directive must be applied by all EU Member States, but it also applies to US companies doing business in the EU. Although the US has an equivalent of the NIS Directive in its NIST Framework, the US framework is not obligatory. The NIS Directive, although flexible in its application, must be adhered to by all companies it affects. Relatedly, the EU is also working on developing standards for ICT security products, an initiative that does not currently have a US equivalent.

Although new cybersecurity legislation is a welcome sign because it increases protection for nations and companies alike, it is worrisome that the EU and the US do not have shared or mirrored pieces of legislation regarding standards. The EU and the US are two of the largest economies in the world and together account for more than 50% of unique IP addresses on a global level.[14] Not having corresponding standards could create barriers for US companies in the EU and vice versa.

EU Policies

NIS Directive

The Directive on Security of Network and Information Systems was adopted in 2016 and is the first EU cybersecurity law. Member States had to adopt the NIS Directive into their national laws by early May 2018.[15] The directive aims to "boost the overall level of cybersecurity in the EU" by requiring Member States to be adequately prepared to respond during and after a cybersecurity breach. To accomplish this, the NIS Directive instructs each Member State to establish a Computer Security Incident Response Team (CSIRT), a national NIS authority and a national NIS strategy.

In addition to boosting Member States´ cyber preparedness, the directive also aims to reinforce security among EU Operators of Essential Services in certain sectors. The sectors included in the regulation are healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure and water supply.[16] According to the European Commission, the companies in these sectors are vital for the economy and society and rely on ICT, which therefore justifies their protection.

Member States will have to identify operators of such essential services by 9 November 2018. Companies and organizations operating in these sectors will have

to adopt "state of the art" security approaches that are "appropriate and proportionate to manage the risks posed" to their systems. The NIS Directive does not specify what measures entities must take to demonstrate compliance.[17]

The NIS Directive also applies to Digital Service Providers (DSP), which include online marketplaces, online search engines and cloud computing services. The Directive requires these entities to inform national authorities when significant security incidents occur. The following are the situations that require companies to inform authorities that they have experienced an incident[18]:

- If a digital service is unavailable for more than 4 million user hours in the EU;
- If more than 100,000 users in the EU are impacted by a disruption of service;
- If the incident has created a risk to public safety, public security or loss of life; or
- If the incident has caused material damage of more than €1 million.

Finally, the legislation requires Member States to set up a CSIRT Network in order to promote cyber cooperation with the goal to ensure effective cooperation on specific cybersecurity incidents and to share information about risks.

Certification framework for ICT security products (Cybersecurity Act)
As the EU continues to work on unifying cybersecurity standards for all Member States, it has also begun to analyze certification standards for ICT security products. Besides giving ENISA a permanent mandate, the "Cybersecurity Act" would transform ENISA into a stronger EU Cybersecurity Agency in charge of capacity building, operational cooperation, international cooperation and cybersecurity certification, among other issues.[19]

One of ENISA´s key tasks would include cybersecurity certification. The European Commission has proposed the creation of a cybersecurity framework, which would include numerous cybersecurity certification schemes in different Member States, for ICT products. ENISA and the European Commission would approve the various schemes, which would then be recognized by each Member State. This would ensure a simple cross border trading system and facilitate consumer understanding of security information.

The schemes would specify the product and service categories; the evaluation criteria and security requirements for the product in question; and an assurance level. Once the schemes have been established, Member States cannot introduce new national schemes or requirements with the same scope. Additionally, national certification schemes in each Member State will cease to exist and current certificates issued by Member States will be valid until their expiration date.

Nonetheless, the use of this EU-wide certification framework would be non-mandatory.[20]

In addition to the framework, the European Commission plans to establish a "duty of care principle" in order to increase product security and increase consumers´ trust in digital products. The principle would entail a joint Commission and industry initiative to reduce product and software vulnerabilities and promote a "security by design" approach for all connected devices.[21]

Liability Standards in the EU
Another area EU policy makers are working on focuses on liability standards for cybersecurity products and companies affected by a cybersecurity attack or data

breach. In its 2017 mid-term review of its Digital Single Market strategy, the European Commission identified the data economy as one of its key focus areas, highlighting that it will continue to work on liability issues in this area.[22]

There is currently no legislation that comprehensively addresses liability when it comes to new technologies or liability in the case of a cyber attack. Nonetheless, cybersecurity liability is briefly mentioned in other relevant laws and regulations, including:

- *Product Liability Directive*: The Product Liability Directive of 1985 establishes the principle of "liability without fault," which is applicable to European producers. The directive says that a producer may be liable if their product causes damage to a consumer even if there is no proof of negligence or fault from the producer´s side. Although the Directive includes "all movables," it does not provide specific guidance on how to apply the directive to new technologies.[23]

  The European Commission is currently studying how to apply liability to new technologies and in March 2018 issued a call for experts in these areas. The Commission´s Working Group of experts will provide it with expertise on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges.[24] The group will also assist the Commission in developing principles that can serve as guidelines for possible adaptations of laws at an EU and national level relating to new technologies.

- *Directive on Attacks Against Information Systems*: Established in 2013, the Directive on Attacks Against Information Systems aims to fight cybercrime and promote information security through stronger national laws, more severe criminal penalties and greater cooperation between relevant authorities.[25] Although the legislation harmonizes the definitions of criminal cyber acts and the penalties for such acts, it does not elaborate much on the liability – specifically, corporate liability – of the companies that experience a data breach or attack. The law does, however, establish that appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with state of the art protections for specific sectors. Per the directive:

  "Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks."

In addition, another one of the few instances in which the law mentions liability is when defining criminal penalties in major cases. For instance, the law dictates that the imposition of criminal liability is not necessary in minor cases. It also indicates that it does not impose criminal liability in cases where acts were committed without criminal intent.

eID Regulation

Another aspect of standards and certification the EU has been working on is the eID Regulation, which requires all EU Member States to mutually recognize the national electronic identification schemes used by the bloc´s members. According to the European Commission, eID aims to allow citizens of one European country to use their national eIDs to securely access online services – such as those provided by public administrations or certain private service providers – provided in other EU countries.[26]

The eID Regulation requires all online public services to accept eIDs from other EU countries different from their own by 29 September 2018.

US Policies

NIST Framework

In 2013, US President Barack Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," with the aim of increasing core capabilities for critical infrastructure to manage cyber risk.[27] The Executive Order does this by focusing on three areas: information sharing; privacy; and the adoption of cybersecurity practices.

As part of the effort to improve the cybersecurity of critical infrastructures, the Executive Order directed the National Institute for Standards and Technology (NIST) to develop a Cybersecurity Framework. The Framework would be composed of "voluntary consensus standards" and "industry best practices" and serve as a roadmap to help companies safeguard their systems. Obama then tasked the Department of Homeland Security with developing a voluntary program to promote the adoption of the framework.

Released in 2014, the NIST Framework is a voluntary set of standards that help an organization "identify, prioritize, manage, and/or communicate cyber risks." It is not a "one-size-fits-all" approach, as what is appropriate for one company could be ineffective for another. Thus, the framework was designed to be technology and industry neutral, meaning it can be used by a wide range of organizations in different sectors. It can also be adapted to a company´s needs, which may vary based on industry, size and cybersecurity risk. The framework is considered a "living document," a classification that means it can be continuously improved and modified as "technologies and threats evolve."[28]

The framework has been revised in 2017 and 2018.[29] The 2018 version includes updated on authentication and identity, self-assessing cybersecurity risk, managing cybersecurity within the supply chain and vulnerability disclosure.[30] The changes were based on feedback from the public, internal team questions and public workshops in 2016 and 2017.

Standard Setting in the US

Standards activities in the US are coordinated by the Standards Branch of the Science and Technology Directorate within the Department of Homeland Security (DHS). The department focuses on five areas: count terrorism; border security; preparedness, response and recovery; immigration; and cybersecurity. Nonetheless, the standards setting process includes various other organizations within DHS. For example, the Directorate works with the DHS Standards Council, which is made up of representatives from various sub-organizations that have a need for important standards to meet their mission[31], to gather standards requirements.

The US federal government always attempts to adopt standards developed in consensus by the private sector when possible. For the government to accept proposed standards, it requires that they have "credibility based on consensus." DHS works with the American National Standards Institute (ANSI) – an organization that oversees the voluntary standardization system for the private sector – via its Homeland Security Standards Panel to gather feedback from the private and public sectors on standards. The department also promotes the use of ANSI accredited, non-governmental standards development organizations to develop national standards for homeland security.

Liability Standards in the US

As in the EU, there are no comprehensive cybersecurity liability laws in the US on a federal level. Relatedly, there is currently no federal US data breach notification law, but rather a "patchwork" of sometimes contradictory state data breach notification laws.[32]

Cybersecurity liability laws in the US are piecemeal, which means that statues, regulations and laws regarding a company´s cybersecurity obligations are "scattered" in various instances in state and federal law.[33] One way of looking at liability exposure is through categories Enforcement actions can be taken at the following levels:

- **Federal level**: Each of the regulated sectors and industries in the US – for instance, health, energy, transportation, etc. – has an agency in charge of overseeing it and taking enforcement actions, if necessary, in situations where liability is an issue. For example, liability concerns and complaints at a federal level for consumer issues during a data breach would be undertaken by the Federal Trade Commission. The Securities and Exchange Commission, on the other hand, oversees public business disclosure of material breaches, while the Federal Communications Commission oversees telecommunications cybersecurity and liability.

  Therefore, at a federal level, organizations may have liability exposure within and among any number of these agencies.

- **State level**: States also pass their own liability, cybersecurity and breach notification laws; different states have different liability laws. In 2017, New York implemented stringent cybersecurity regulations for the banking, insurance and financial services industries, which require companies to have a cybersecurity program to protect consumer data and a Chief Information Security Officer to help protect data and systems, among other requirements.[34] On this level, state attorneys general, the principal law enforcement officer in each state, can take enforcement actions against companies for violating state cybersecurity and liability laws.

- **Municipal level**: Finally, some municipalities are also creating laws or regulations that create liability exposure for organizations. The consumer credit bureau Equifax was sued by the city of Chicago in 2017 for a data breach that exposed the records of 143 million consumers.[35] The city argued that Equifax violated Chicago´s consumer fraud ordinance by doing a "poor job of protecting sensitive data from hackers" and failing to notify the public promptly after the attack.

In addition, plaintiffs whose data is compromised and a company´s shareholders can also take action against a company for liability in the courts. Individuals and groups have become increasingly more active in this area, termed the plaintiffs´ bar, over the last few years. [36]

3.2 Privacy and Data Protection

Privacy and data protection is a policy area that has received much attention over the past few years, particularly in the EU. In tandem, the US has recently been spurred to a more proactive posture because of the Cambridge Analytica scandal, an incident which resulted in the harvesting of data from as many as 87 million Facebook users in 2015, 2.7 million of whom were Europeans. [37] The data was allegedly used

to create ads for Cambridge Analytica´s clients, which some claim included US President Donald Trump´s campaign. [38] The incident has been the focus of US Congressional hearings and has prompted US authorities to ask whether companies like Facebook should be more strictly regulated.

In this area, the US and the EU have taken vastly different approaches towards regulation. The EU has decided to take a more streamlined policy approach, in which it targets all sectors, with the GDPR and the proposed new e-Privacy regulation, while the US has opted for a multi-faceted, multi-jurisdictional approach depending on the sector and type of information.

EU Policies

General Data Protection Regulation (GDPR)

The GDPR was approved by the EU Parliament on 14 April 2016 and became applicable on 25 May 2018. It applies in all cases in which personal data is collected, stored, processed and exchanged. The GDPR aims to protect all data subjects who are in Europe from privacy and data breaches and harmonize data protection laws in the EU. The law regulates how businesses and entities obtain user data, how they process it and how they protect it. It includes existing EU privacy regulations such as the right to be forgotten and provisions regarding international data transfers. Nonetheless, the GDPR also includes new concepts, from increased territorial scope to the right to data portability. The next section includes a breakdown of the key aspects of the GDPR.

Increased territorial scope

The GDPR applies to businesses in the EU as well as to those outside the EU. Businesses who offer goods or services in the EU or monitor the behavior of data subjects in the EU must adhere to the regulation, even if they are not established in the EU.[39] To quote the GDPR, Article 3: "This Regulation applies to the processing of personal data in the context of activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not."[40]

Accountability principle

In addition, GDPR also establishes what´s known as the "Accountability Principle," a new concept in European data protection law. This principle requires that entities put in place appropriate technical and organizational measures to ensure data protection. In other words, it places a focus on the process of data protection, which is considered crucial. The law also requires that organizations provide evidence to prove that they comply with the principle when required to do so.[41]

Breach notification

Under the regulation, data controllers and processors must notify data protection authorities and data subjects of certain breach incidents.[42] Data controllers must notify data protection authorities of an incident within 72 hours. This applies to all incidents except those where there are no risks to the privacy and freedoms of individuals. Additionally, controllers must notify individuals whose data has been involved or compromised by the incident when there are "high risks to their privacy and freedoms." Data processors must notify data protection authorities "without undue delay" of all breaches.[43]

Right to be forgotten

The GDPR includes the right to erasure and the right to be forgotten. This means that data subjects have the right to delete information about them stored on a data processor. Individuals also have a right to have public information about them erased

by data processors as long as such erasure is deemed not to violate freedom of speech.

Google has responded to the Right to be forgotten by blocking access to the articles in question inside the EU, but not in other areas.[44] It has received 650.000 Right To Be Forgotten requests since 2014. Some Member States, such as France, have gone above and beyond the Right to be forgotten and demanded links blocked in the EU be blocked on a worldwide level.

Data portability
The right to data portability is new to EU law. It gives an individual the right to receive their personal data in a standard, machine-readable format. This will allow the user to move his or her data to another electronic service, such as a social media platform.[45] The right to data portability ensures that access to data remains meaningful as the amount of data held relating to an individual increases over time. Allowing consumers to move their data to other services also offers new opportunities for services and stimulates competition.

International data transfers
Under the GDPR, it is generally prohibited to transfer data outside the EU unless the country where the data will be held has adequate data protection practices. The European Commission decides whether a third country´s data protection policies are adequate. However, a data processor can still process data if it puts the appropriate safeguards in place even if the Commission does not approve the policies of the country where the processor is established. The European Commission must approve any safeguards adopted.

One example of these types of international data transfers are the data transfers between the US and the EU. In order for these transfers to take place, both the US and the EU had to come to an agreement that would satisfy EU data protection requirements. The agreement, approved by the European Commission in July 2016, was referred to as the Privacy Shield Framework and established provisions for US companies to comply with European data protection requirements. In practice, companies that enter the framework have permission to transfer data between the US and the EU.[46]

Stronger enforcement
The GDPR takes serious measures to create a strong enforcement team. It creates a European Data Protection Board, which is composed of the 28 data protection authorities from each Member State. The board will have the power to provide guidance and interpretation of the GDPR and adopt binding decisions in important data protection cases.[47] Additionally, the Regulation gives data protection authorities the power to impose strict penalties to businesses that don´t comply with the law. Businesses found to incompliant could face a fine of up to 4% their worldwide turnover or €20 million, whichever is greater.

GDPR impacted US companies well before its implementation on 25 May 2018. In many cases, it caused confusion, as US companies were not sure they had to comply with GDPR if they did not have a presence in Europe.[48] Moreover, the regulation forced companies like Facebook to prepare for the changes well over a year in advance, modifying products specifically for its European audience.[49]Some companies were not sure how to comply with the new regulations or whether the benefits from compliance would outweigh the investment of time and financial resources. News about the impact of GDPR is still being published, and it´s likely that we won´t know the long-term impacts for some time.

GDPR Real World Impact: US publishers consider blocking European visitors because of new data protection law

In May 2018, the month the GDPR was set to go into effect in the EU, a number of U.S. publishers declared they were planning to block European IP addresses from accessing their websites.

The publishers expressed various reasons for doing this, citing small European audiences, wariness at the possibility of being fined up to 4 percent of global revenue or €20 million, vague language in the GDPR and concerns about not being fully compliant with the new law.

"There´s a lot of things within GDPR that are kind of vague," said Christina Roberts, executive vice president at the health and lifestyle publication Well + Good. "Seeing what our competitors are doing will be helpful to seeing what is absolutely necessary. Blocking gives us some time."

Although blocking European IP addresses may sound extreme, other publishers say it´s a common practice. Chris Tolles, CEO of the entertainment news site Topix, is considering banning European users from his site due to the GDPR. Tolles already bans IP addresses from other countries.

"It´s pretty easy to block people by IP address," he said. "I´ve blocked most of Africa, Asia, most of the nations that cause me problems legally or from a spam or scam standpoint. I´ve already blocked most of the former Soviet Union."

Blocking European users may also boil down to pure business. Tolles said although he gets 10% of his revenue from the UK, which he does not want to lose, investing to comply with GDPR may not be worth it because of the high ad-blocking rates in countries like Germany.

Even the companies that have worked hard to get GDPR compliant are considering banning EU users. Tom Sly, senior vice president at the broadcaster E.W. Scripps Co., said his company had been working to get GDPR compliant for the past eight months. Sly said that if the company has doubts about its compliance with the law, it will block European IP addresses.

"Some would look at it as an extreme step," Sly said. "But we´re serious about compliance."

Source: Digiday, published online 15 May 2018

e-Privacy Regulation

In terms of privacy, there is another legislative initiative currently being worked on in the EU: the e-Privacy Regulation. This proposed legislation aims to replace the e-Privacy Directive of 2002 and will work in tandem with the GDPR. The proposed regulation concerns electronic communications, the right to confidentiality and privacy protection, among others.[50] From a legal standpoint, the regulation would harmonize EU privacy law in the communications realm by giving all people and businesses the "same level of protection."[51]

The proposed regulation would apply to companies that provide electronic communication services, or so-called Over The Top (OTTs) services, such as WhatsApp, Facebook Messenger and Skype.

Communications content and metadata

The e-Privacy Regulation guarantees the confidentiality of the content of communications as well as the metadata (the time of a call and the location, for instance) of those communications.[52] Individuals will have to give their consent in order for their communications data, including content and metadata, to be processed. The Regulation considers that metadata has a high privacy component and determines that it must be anonymized or deleted if users do not give their consent. There is one exception to this, which is when the data is needed for billing.

Simpler cookie rules
In the past, EU rules on cookies have created an excessive amount of consent requests for users. e-Privacy aims to streamline this consent requirement by requiring browser settings to provide an easy way to accept or refuse cooking tracking. The Regulation also clarifies which types of cookies fall under the law and which do not. For instance, non-intrusive cookies – identified by the European Commission as those which, for instance, track shopping cart history or count the number of visitors a website receives – are not prohibited.[53]

Spam protection
The proposed regulation also imposes strict limits on spam. It prohibits unsolicited communication via email, SMS and automated calling machines. e-Privacy will either protect individuals by default or enable a mechanism that will allow people to sign up and opt-out of marketing phone calls. Additionally, one of the biggest changes would require marketers to identify themselves as such by displaying their phone number – in order words, marketers will no longer be able to block their number – or adopting a pre-fix that identifies the call as a marketing call.[54]

Enforcement
Enforcement of the e-Privacy Regulation will fall to the enforcement body established under the GDPR, the European Data Protection Board, which is made up of the 28 national data protection officers.

Privacy Shield
On another note, the EU and the US have worked together on one very important aspect of privacy and data protection over the last few years: the transfer of European users´ data to the United States for commercial purposes. The bilateral agreement went into effect in 2016 and is referred to as Privacy Shield Framework. It requires companies that transfer data from European users out of the EU to self-certify to the US Department of Commerce that it meets the framework´s requirements and publicly commit to doing so.[55] More than 3.300 organizations use Privacy Shield to for their transatlantic data transfers, including Facebook, Google, Microsoft, Amazon and Twitter.[56]

The Privacy Shield Framework is based on the following principles[57]:

- **Strong obligations on companies handling data**: The US Department of Commerce conducts regular updates and reviews of the companies that participate in the program. This is done to ensure that the participating companies are following the rules they agreed to. Companies that do not comply can be fined or removed from the list.

- **Clear safeguards and transparency obligations on US government access**: US law enforcement and national security authorities will not have unlimited access to EU users´ data. The US government has agreed that data access for the aforementioned purposes will have clear limitations, safeguards and overview mechanisms. In addition, EU citizens will have legal redress mechanisms – outlined in the Judicial Redress Act of 2015 – if they feel their data has been misused.

- **Effective protection of individual rights**: Under Privacy Shield, EU citizens have access to "accessible and affordable" dispute resolution mechanisms.

- **Annual joint review mechanism:** The European Commission and the US Department of Commerce will carry out an annual joint review of Privacy Shield and analyze whether the US has been meeting its commitments and assurances with regards to data access for law enforcement and national security purposes.

Privacy Shield replaced Safe Harbor, also a self-certification program, which US companies had been using to transfer EU users´ data for 15 years. Safe Harbor allowed US companies to "self-certify" that they provided EU users the protections required by the Data Protection Directive of 1995. The Directive was replaced by the GDPR, which went into effect in May 2018.

In 2018, the European Parliament raised concerns about the Clarifying Lawful Overseas Use of Data Act (also known as the CLOUD Act), which gives US and foreign law enforcement authorities the ability to access certain digital information located in other countries. The Parliament stated that the CLOUD Act could potentially violate EU data protection laws. GDPR, for instance, prohibits the transfer of data outside the EU for law enforcement purposes if there is no international agreement, such as a mutual legal assistance treaty, between the countries in place.[58]

Unlike Privacy Shield, which addresses EU user data transferred to the US, the CLOUD Act addresses data that is of interest to US law enforcement authorities stored in other countries. It also allows other countries that enter into bilateral agreements with the US to request law enforcement information directly from US companies instead of using the established Mutual Legal Assistance (MLA) instruments.[59]

US Policies

Unlike in the EU, in the US there is no comprehensive federal data protection law. The closest equivalent to such a law is the Privacy Act of 1974, which we will describe below. Instead, the US relies on a "patchwork" of federal laws, state laws and regulations. Some of these laws apply to categories of information, such as financial or health information, while others apply to activities that rely on personal information for their execution, including telemarketing and marketing via email. These laws sometimes overlap and "contradict" one another.[60] In addition, the US systems contains guidelines and frameworks, which are self-regulatory and voluntary standards that are not enforceable by law.[61]

There are also consumer protection laws that are not privacy laws, but that also have aspects that dictate the protection and disclosure of personal data.[62]

Privacy Act of 1974

One of the most important hallmarks of US privacy policy, and by extension cybersecurity policy, is the Privacy Act of 1974. In essence, the law "regulates the collection, maintenance, use and dissemination of personal information by federal executive branch agencies."[63] It provides individuals with the right to request the records a federal agency has on them, the right to request a change to their records in the spirit of accuracy, relevance, timeliness and completeness and the right to be protected against an unwanted invasion of privacy due to the "collection, maintenance, use and disclosure of their personal information."[64] The law requires that agencies publish their system of records in the publicly accessible Federal Registrar.

Judicial Redress Act of 2015
The Judicial Redress Act of 2015 is directly related to the Privacy Act of 1974. It allows citizens of certain foreign countries and regional economic organizations the right to judicial redress – more specifically, the right to challenge how their data is used – under the provisions of the 1974 law. The law, which was passed in 2016, was specifically prompted by the negotiations for the US-EU Data Protection Agreement. The European Commission required the US Congress to pass a judicial redress act as part of the negotiations. US citizens in the EU had the same right before the Judicial Redress Act was passed.

Federal Trade Commission Act
The Federal Trade Commission Act is a federal consumer protection law that prohibits unfair or deceptive acts or practices in or affecting commerce.[65] The law gives the Federal Trade Commission (FTC) the power to seek monetary damages or other forms of "relief" for actions that have harmed consumers, emit rules that define unfair or deceptive acts and requirements to prevent such acts and investigate organizations and businesses involved in commerce, among others. The FTC has disciplined companies that fail to comply with their published privacy policies and for unauthorized disclosure of personal data.[66]

Children´s Online Privacy Protection Act (COPPA)
The US Congress approved the Children´s Online Privacy Protection Act (COPPA) in 1998. COPPA limits the collection of information from children under the age of 13 without their parents´ consent. It requires websites to post their entire privacy policy online, inform parents about their data collection policies and practices and get "verifiable consent" before collecting a child´s personal information and sharing it with third parties.[67] Under COPPA, parents have the right to review the information a website has on their child, delete their child´s information and prevent the website from collecting any further information on their child. It also requires websites to establish practices that protect the children´s information and not encourage children to engage in activities that would allow the website to collect more information than is "reasonably necessary."[68] The FTC is the primary agency in charge of enforcing COPPA.

Financial Services Modernization Act (Gramm-Leach-Bliley Act or GLB)
The Financial Services Modernization Act (GLB) required financial institutions to disclose their information-sharing practices to customers and allow them to declare if they want their personal information shared. This information, which includes bank balances and account numbers, is often bought and sold by banks, credit card companies and others.[69]

Health Insurance Portability and Accountability Act (HIPAA)
The law protects a person´s "individually identifiable health information" held by an entity. It is classified as an individual´s past, present or future physical or mental health or condition, the provision of health care provided to that individual and the past, present or future payment for the provision of health care to the individual.[70] Other common identifiers include name, address, birth date and Social Security number. Demographic data is also considered protected information. Nevertheless, HIPAA allows for the release of certain information in order to maintain high and continuous standards of care. The Department of Health and Human Services is in charge of enforcing the law.

Fair Credit Reporting Act
The Fair Credit Reporting Act applies to consumer reporting agencies, such as credit bureaus, medical information companies and tenant screening services.[71] Information cannot be provided to anyone who does not meet a purpose covered in

the act. The law also made consumer reporting agencies responsible for investigating disputed customer information. Entities that use the information provided by these agencies and then make adverse credit, insurance or employment decisions based on said information must inform the consumers that the action has been taken due to the information provided in the reports.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)

The Controlling the Assault of Non-Solicited Pornography and Marketing Act was approved by the US Congress in 2003 and regulates commercial email. It establishes requirements that commercial messages must meet and gives users the right to have marketers stop emailing them. The messages that fall under CAN-SPAM include "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." This also includes business to business email and messages to former customers announcing, for instance, a new product line.[72] Every email found to be in violation of the CAN-SPAM Act can face fines of up to $41,484.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) of 1986 protects "wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers." The law applies to emails, telephone conversations and electronically stored data.[73] The ECPA also safeguards the contents of files and records held by service providers.

Data Protection Real World Impact: After Cambridge Analytica, US Senators introduce CONSENT Act to restrain online data use

A new bill introduced in April 2018 in the US Senate by Sens. Richard Blumenthal (D-CT) and Ed Markley (D-MA) would require that companies obtain explicit consent from users to use, share or sell any personal information they disclose. Additionally, it would force companies to notify individuals any time data is collected, share and used and establish new security and breach reporting requirements.

The Customer Online Notification for Stopping Edge-provider Network Transgressions Act (also known as the CONSENT Act) comes after it was revealed that consulting firm Cambridge Analytica had harvested data from up to 50 million users and used that data in targeted political campaigns. The proposed law has been referred to the Committee on Commerce, Science and Transportation in the US Senate. It would establish the Federal Trade Commission as enforcer of the new rules and would expand the commission´s power and role in online advertising.

Blumenthal directly asked Facebook CEO Mark Zuckerberg, who has apologized for the Cambridge Analytica scandal, if he would support the legislation as a national standard for online data consent.

"In general, I think that principal is exactly right and we should have a discussion," Zuckerberg said.

Blumenthal said the CONSENT Act was a response to the EU´s General Data Protection Regulation, which is set to go into effect in May 2018. Facebook has already said it will comply with the GDPR and announced changes to its user policies to comply with the law.

One such change includes asking users whether they want Facebook to use data from its partners, e.g. websites, to show them ads. Another change will ask users if they wish to continuing sharing information that demonstrates their political views, religious views and relationship status.

"As a principal, I would (support the law)," Zuckerberg said. "I think the details matter a lot."

Source: The Verge, published online on 10 April 2018

3.3 Public-Private Information Sharing

Given that cybersecurity attacks also affect private companies of considerable size that often play important roles in society, it´s logical that both the US and the EU have worked on legislation regarding public-private information sharing. Both jurisdictions recognize the role of information sharing when it comes to preventing and mitigating cybersecurity attacks.

This policy area has been transformed in recent years with the approval of the GDPR and NIS Directive on the EU side and CISA and the CLOUD Act in the US. It has also presented both parties with an opportunity for collaboration with the approval of the CLOUD Act, which relates to information sharing across borders.

EU Policies

GDPR
The GDPR establishes public-private information sharing for data controllers and data processors.[74] Notably, the law makes information sharing mandatory during and data breaches and in situations where it is necessary in order to comply with legal obligations. Under GDPR, a data controller must notify data protection authorities of a breach within 72 hours of becoming aware of the incident and inform the subjects whose data has been compromised "without undue delay."[75]

The law also requires data processors – or third-party companies that process data for their customers, known as data controllers – to notify data controllers without undue delay of a security breach after they become "aware" of such an incident. In this situation, the data controller has the legal responsibility of notifying the relevant data protection authorities.

NIS Directive
Like GDPR, the NIS Directive requires Operators of Essential Services to report cybersecurity breaches that meet certain criteria to the appropriate data protection authorities. In contrast to GDPR, the NIS Directive provides some liability protection for the entity reporting the breach, stating that "notification shall not make the notifying party subject to increased liability."[76] This characteristic is also present in US public-private information sharing legislation.

E-evidence legislation
Another area of critical importance in the realm of public-private information sharing is the access to data during criminal investigations. In 2018, the European Commission proposed rules to govern these situations.[77] The proposal, which could be adopted as a regulation or a directive, is referred to as "e-evidence."

It is considered the European response to the Clarifying Lawful Overseas Use of Data Act, or CLOUD Act, a US law that allows American, and in certain cases foreign law enforcement agencies, access to information stored by US companies overseas.

E-evidence would create various new tools and safeguards for the gathering of this type of information. These include:

- **European Production Order**: The order would allow a judicial authority in one Member State to obtain electronic evidence held in another member state directly from the service provider or its legal representative. The service provider will be required to respond within 10 days and within 6 days in cases of emergency.
- **European Preservation Order**: The European Preservation Order allows a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserve specific data. This is done because the Member State plans to issue a subsequent request to obtain the data via various avenues, such as a mutual legal assistance request, a European Investigation Order or a European Production Order.
- **Strong safeguards**: The safeguards under the proposed legislation guarantee safeguards for the right to protection of personal data.
- **A legal representative for service providers in the EU**: The proposed legislation would require that service providers designate a legal representative in the EU that will be able to receive, comply and respond to these requests for data. This will be required even if service providers have their headquarters outside the EU.
- **Legal certainty for businesses and service providers**: Currently, law enforcement authorities depend on the goodwill of service providers to turn over relevant information. Under the proposed law, all service providers will be subject to the same rules.

According to the Commission, more half of all criminal investigations today require access to electronic evidence, which includes text messages, e-mails or content on messaging applications. E-evidence would make it easier and faster for law enforcement and judicial authorities to request these materials to prosecute criminals and terrorists.

US Policies

Cybersecurity Information Sharing Act (CISA)

In order to promote information sharing on cybersecurity threats between private entities and the federal government, the US Congress passed the Cybersecurity Information Sharing Act in 2015. As noted by the law firm White & Case, "the sharing of cybersecurity information generally conflicts with corporate goals to protect intellectual property and avoid related legal risks."[78] CISA allows companies to monitor cybersecurity threats and implement defensive measures on their systems to counteract such threats. CISA also provides safeguards in order to promote information sharing between private companies and local, state and federal governments as well as between private companies and other entities.

The information covered under the law is information on "cyber threat indicators" and "defensive measures."[79] A cyber threat indicator is defined as the information necessary to describe or identify threats. These threats include methods used to exploit a security vulnerability or methods to cause a user to accidentally enable cyber exploitation. This indicator also includes information on the "actual or potential harm caused by an incident, including a description of the information obtained as a result of a particular cybersecurity threat."[80]

Meanwhile, a defensive measure is a set of actions taken to protect an information system or specific information on that system. These measures "detect, prevent or mitigate a known or suspected cybersecurity threat or security vulnerability."[81] Notably, actions that destroy, provide unauthorized access to or harm third party systems are not considered defensive measures. Nonetheless, CISA does not replace or undermine federal requirements that require entities to report certain information, such as known or suspected cybercrimes, to regulators and law enforcement agencies.[82]

Safeguards for companies that share cyber threat indicators and defensive measures information include liability protection, antitrust exemptions, protection of proprietary information, exemption from federal and state Freedom of Information Act laws and protection from regulation and enforcement actions.[83] In order to receive these protections, entities must share information according to CISA requirements, such as removing all personal information regarding a specific individual.

Of these protections, the most significant are the liability protections offered by CISA. Although CISA does not protect a company in all cases of liability, it does protect companies from two important types of lawsuits: a cause of action for monitoring information systems and a cause of action for sharing or receiving a cyberthreat indicator or a defensive measure.

The protection from lawsuits for monitoring information is considered important by many in the legal and technology communities. For instance, CISA will shield companies from liability if they monitor their employees´ emails for cyber threat information.[84] It also protects companies from lawsuits related to the disclosure of information. Although CISA provides significant protections, it is important to note that it does not shield companies from potential liability during a data breach or other cyberattack.

In addition to encouraging private entities to share information with the US government, CISA also tasks federal agencies with increasing their sharing of cybersecurity threat information, including relevant procedures and a digital portal for private entities, non-federal government agencies and the general public.[85]

CLOUD Act

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was approved by the US Congress in 2018. It was created to streamline how US and international law enforcement agencies obtain digital personal information stored by US tech companies in different territories. The new law requires US technology companies to provide requested data to US law enforcement agencies even if such information is stored in another country.

Notably, it gives technology companies the right to challenge the data request if the request violates the laws of the country the data center is in. It also allows the US to enter into bilateral access agreements with other countries in order to ensure the same data access by international authorities.

Before the CLOUD Act, US enforcement agencies had to undergo a series of steps in order to obtain data stored outside the country. The same was true for foreign law enforcement agencies. Steps for foreign law enforcement agencies included having an established Mutual Legal Assistant Treaty (MLAT) with the US government, sending a request to the US Department of Justice and waiting for the US Department of Justice to obtain approval from a judge.

US authorities faced similar hurdles when requesting data for an investigation held in another country. The incident led to the *US v. Microsoft* case, in which the US government asked the technology company for user information to investigate a drug trafficking case. The company provided the US authorities with some of the information, but not all. The rest of the information in question was held at a Microsoft data server in Ireland, Microsoft told US authorities they would have to coordinate with their Irish counterparts in order to obtain the information. The US responded by suing for access to the information. Nonetheless, the case was dismissed by the US Supreme Court in April 2018 with the passage of the CLOUD Act.[86]

After the passage of the act, EU Justice Commissioner Vera Jourova stated the EU was hoping to establish compatible rules with the US for obtaining evidence obtained in other countries.[87]

Public-Private Information Sharing Real World Impact: *US v. Microsoft*

In 2013, US authorities presented Microsoft with a search warrant for emails that were of interest in a drug trafficking investigation. Microsoft responded to the warrant by providing the information relating to the individual that was held on US data servers, including the subject´s address book.

The company did not provide US authorities with actual emails, which were stored in a Microsoft data center in Dublin, Ireland, the same place the individual had lived when he opened his Outlook email account. Microsoft then directed the authorities to work with their Irish counterparts to get the rest of the information. The US Department of Justice protested Microsoft´s response, arguing that it had a right to obtain the emails under the Stored Communications Act of 1986, which allows the US government to obtain emails and other forms of communication from technology companies. The dispute ended up in one of the most famous court cases of Internet era, *US v. Microsoft*.

Microsoft disagreed with the Department of Justice´s interpretation of the law, stating that the Stored Communications Act was never meant to be applied outside of the United States. Turning over the emails to US law enforcement, it argued, could potentially force it to violate the laws of the countries where its data centers were located. The Justice Department again said there should be no problem because the actions taken to obtain the emails could be carried out by Microsoft employees in the US.

"In other words, the government is saying that *copying* or *moving* the subject´s emails stored in Ireland isn´t search and seizure – only directly handing the emails to the US government is," wrote *Wired*´s Louise Matsakis in February 2018.

Throughout the case, which saw some courts rule in the US government´s favor and others in Microsoft´s favor, Microsoft enjoyed widespread support from the technology industry, foreign governments, privacy advocates and even the media.

The European government, civil liberties organizations, Amazon, Apple, *CNN* and *The Washington Post* filed an amicus brief with the court in the company´s favor. Microsoft also had the support of the Irish government, which said the US should try to obtain the data in question through existing treaties and respect Irish sovereignty.

"We believe that people´s privacy rights should be protected by the laws of their own countries and we believe that information stored in the cloud should have the same protections as the paper stored in your desk," Brad Smith, Microsoft´s Chief Legal Officer, wrote in 2017.

The case eventually made its way to the US Supreme Court, although the court never issued a ruling on the case. The issue was instead resolved by the US

Congress, which passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

The CLOUD Act requires US technology companies to provide US authorities with information even if the information in question is stored in data centers in another country. Importantly, it gives technology companies the right to challenge the data request if it violates the laws of the country the data center is in. It also allows the US to enter into data access agreements with other countries in order to ensure the same data access by international authorities, avoiding the time consuming MLAT process. The CLOUD Act received support from Microsoft and other technology industry giants as well as from US law enforcement authorities.

Source: Wired, published online 27 February 2018

4 KEY ACTORS IN TRANSATLANTIC CYBERSECURITY POLICIES

The policies mentioned above are crafted and enforced by governmental legislative bodies and agencies. In this regard, we see a similar pattern to what we saw with each region´s cybersecurity strategies. Both the EU and the US follow similar legislative processes in terms of crafting legislation and enacting cybersecurity laws. Key differences emerge in the enforcement of laws and the creation of policies that do not need legislative approval, such as the presidential executive orders in the United States.

The EU and the US have very different approaches to the enforcement of laws. In the EU, enforcement is a more centralized process led by the agencies specialized in cybersecurity. Meanwhile, the US handles cybersecurity through all its governmental agencies as well as through the National Security Council´s Interagency Process, which takes cybersecurity policy matters directly to the president.

The following section will describe the core agencies, legislative bodies and actors involved in cybersecurity policy in the EU and the US. This is not a comprehensive list, but rather a guide that is meant to help the reader understand how policies related to cybersecurity and privacy are formed and then enforced.

4.1 EU Agencies Involved in Cybersecurity Policies

The agencies and policy making bodies mentioned below do not represent a comprehensive list of all actors involved in EU cybersecurity policies. However, they do represent the core agencies that directly support the EU Cybersecurity Strategy.

European Commission

The European Commission presents legislative proposals that must be approved by the EU Parliament. It adopted the EU Cybersecurity Strategy, "An Open, Safe and Secure Cyberspace," in 2013. Within the Commission, there are three main directorate generals that focus on cybersecurity and privacy: DG Research & Innovation, DG Connect and DG Justice. The strategy asked the European Parliament to adopt a variety of new laws relating to cybersecurity and privacy. In 2016, the European Parliament adopted the GDPR and the NIS Directive, the latter of which was a legislative proposal that had been included in the Commission´s Cybersecurity Strategy.

European Parliament

The European Parliament must consider and approve the legislative proposals introduced by the European Commission. It is currently debating the Commission´s proposed e-Privacy Regulation, which will replace the e-Privacy Directive and provide specific privacy rules for electronic communication services.[88]

European Council

The European Council defines the EU´s political direction and priorities in cybersecurity. In 2017, the Council agreed upon a set of priorities to build a successful "digital Europe," which included adopting a common approach to cybersecurity and stepping up efforts to combat terrorism and online crime, among others.[89] The European Commission, Council and Parliament each have an interconnected role when it comes to defining, crafting and approving cybersecurity and privacy legislation.

ENISA

The European Union Agency for Network and Information Security (ENISA) is the EU cybersecurity agency. Created in 2004, the agency´s goal is to harmonize cybersecurity efforts in all Member States. The agency plays a central role in the EU Cybersecurity Strategy by working to achieve the cyber resilience of all Member States and the EU as a whole.[90] It also provides technical advice and solutions for the public and private sector. ENISA is considered a "body of expertise" and advises the Commission and Member States on "NIS-related issues, collection and data analysis to identify emerging risks, promotion of risk assessment and management and encouragement of public-private partnerships."[91] ENISA has been described as an expert "intermediary, assessing capabilities, identifying gaps and shaping policies at national and European levels."[92]

ECSO

The European Cyber Security Organization is a self-financed non-profit organization established under Belgian law in 2016. It is the industry-led contractual counterpart of the European Commission that works on the implementation of cybersecurity Contractual Public-Private partnerships (cPPP). ECSO is made up of representatives from: large companies; SMEs; startups; research centers; universities; end users; operators; European Member State local, regional and national administrations; countries part of the European Economic Area; the European Free Trade Association; and associated countries in the Horizon 2020 program.[93]

ECSO works to support different types of initiatives or projects that develop, promote and foster the European cybersecurity sector. It engages in many different activities to achieve these goals, such as collaborating with the European Commission and national public administrators to promote innovation in cybersecurity, fostering market development and investments in demonstration projects and increasing competitiveness and growth in the cybersecurity industry in Europe in both large and small companies, among others.

Computer Security and Incident Response Teams (CSIRTs)

Under the NIS Directive, the Computer Security and Incident Response Teams (CSIRTs) are part of a network that help deliver a swift and effective response during a cybersecurity incident. After a cybersecurity event, they provide alerts, warnings, advice and training. The teams are also meant to foster confidence and trust between Member States in order to improve cyber incident responses. Every Member State has its own CSIRT network. ENISA also plays a role in CSIRT operations. It facilitates the "set up and running" of the teams, shares best practices and coordinates the exchange of international threat information.[94]

European Cybercrime Centre (EC3)

Part of Europol, the European Cybercrime Centre (EC3) is another initiative meant to harmonize EU cybersecurity strategy. EC3 is the EU cyber intelligence organization, "focusing on cybercrimes committed by organized groups, that affect critical infrastructure or cause serious harm to the victim."[95] EC3 also has an operations function and offers various services to EU political and law enforcement stakeholders, among others. It offers information on emerging cyber trends and methods of criminal activity and also provides training to law enforcement officials inside and outside the EU.[96]

J-CAT

Also housed within Europol is the Joint Cybercrime Action Taskforce, which was created in 2014 and is dedicated to fighting cybercrime on an EU and international level. The unit is part of EC3 and leads cross-border investigations on high-tech crimes, crime facilitation, online fraud and online child exploitation.[97] It is composed

of experts and professionals from EU Member States, non-EU law enforcement partners, including the United States, Norway and Canada, and members of EC3.

ETSI
ETSI is one of the three European Standards Organizations (ESO) along with CEN and CENELEC. It works to support EU policies and to minimize the amount of duplication of standards.[98] ETSI is one of the organizations working on creating framework of consistent cybersecurity standards in Europe.[99] ETSI receives support from ENISA.

Eurojust
Eurojust was created to fortify the judicial arm of EU law enforcement.[100] It facilitates legal processes in cross-border cases and investigations involving at least two EU countries, offering judicial coordination and cooperation between national authorities. The agency provides support for Mutual Legal Assistance (MLA) and extradition requests. Eurojust also plays a role in the crafting of EU legal instruments, such as European arrest warrants, confiscation and freezing orders.[101]

Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU)
Computer Emergency Response Teams (CERTs) are similar to CSIRTs but have different core functions. While CSIRTs assist in receiving and reviewing a cybersecurity incident, CERTs work with organizations to facilitate their response to incidents and raising awareness about cyber issues.[102] The EU has its own CERT for its institutions, agencies and bodies. The CERT-EU team is composed of IT security experts from the main EU institutions, including the European Commission, General Secretariat of the Council, European Parliament and the Committee of the Regions, among others. CERT-EU cooperates with other CERTs in EU Member States.[103]

European Defense Agency (EDA)
The EU Cybersecurity Strategy identifies cyber defense as a priority. This is understandable given that cyberspace is understood as the fifth domain of warfare that is critical to military operations on land, sea, air and space.[104] The agency focuses on helping Member States build a skilled military cyber defense workforce and ensuring the availability of proactive and reactive cyber defense technology.

Real World Impact: Estonia cyber attacks lead country to increase its cybersecurity defenses, adopt interagency process

In April 2007, a statue set off what is considered to be the world´s first cyber war in Estonia. Hackers disabled online banking services, government networks and media outlets. However, the experience also provoked a response in the country, which today has one of the best cybersecurity defense measures in the world.

The statue that sparked Estonia´s cyber conflict was called the Bronze Soldier in Tallinn, the nation´s capital. The monument was installed by the Soviet Union in 1947 to commemorate the Russian victory over Nazism. Nonetheless, ethnic Estonians considered the Russians occupiers and the Bronze Soldier a representation of decades of Soviet oppression.

In 2007, the Estonian government decided to move the statue to a military cemetery on the outskirts of the city, a decision that provoked outrage among Russian speakers in Estonia and Russia-language news media. Protests inundated the capital and cyber attacks followed, bringing down as many as 58 Estonian websites at one point. The attacks are believed to have been orchestrated by the Russian government, which denies any involvement.

After the attacks, Estonia began working on improving its cybersecurity defenses. Part of its efforts focused on setting up an interagency process similar to that in the United States. The approach aimed to improve cyber coordination within different government agencies as well as with private sector companies.

Estonia developed a 2008-2013 Cybersecurity Strategy, which lays out the different cybersecurity roles for each government agency. It also established the Cyber Security Council of the National Security Committee of the government in 2009, which monitors the progress made in strategy implementation.

Like the United States´ National Security Council, the Cyber Security Council include representatives from seven ministries, government agencies, the government office and Estonian Defence Forces. More key players from the private sector, academic sector, etc. can be included in the meetings as needed.

As noted by experts at the French telecommunications giant Orange in reference to Estonia and the European Union, "The cyber threat landscape has changed since the 2007 Estonian cyber attacks: cybersecurity is not an isolated topic anymore, understood by a handful of experts only."

Sources: BBC, published online on 27 April 2017 and *Interagency Cooperation on Cyber Security: The Estonian Model*

4.2 US Agencies Involved in Cybersecurity Policies

Unlike in the EU, where the Commission has designated specific agencies to work on its cybersecurity priorities and strategies, the US does not have specifically designated agencies established to carry out and enforce its cybersecurity goals. The government regulation landscape for cybersecurity issues is complex and involves multiple players, each of which monitors problems and implements solutions.

In general, the US sets and enforces its national security policies, which include cybersecurity policy, through what is referred to as the National Security Council Interagency Process and has designated certain entities as response agencies for cybersecurity incidents.

In addition, the US Congress, as the nation´s legislative body, is key in crafting and passing policy into law. Meanwhile, US courts review policies and laws to ensure they are in harmony with precedent, existing regulations and legal principles.

The following is a broad description of the policy making process, applicable presidential directives and the principal actors and agencies involved in cybersecurity.

US President
The US president establishes the nation´s cybersecurity policy through executive orders, presidential directives and the National Security Council Interagency Process. By issuing executive orders and presidential directives, the president can direct the nation´s agencies to focus on cybersecurity issues in a way he sees fit. The president also works with the US Congress to communicate cybersecurity priorities and legislation proposals.

US Congress
The US Congress proposes and approves cybersecurity legislation which later applies to federal agencies, private companies and the general public, among others.

National Security Council Interagency Process

The National Security Council Interagency Process is the mechanism by which the president of the United States implements national security and foreign policy decisions. The process involves at least four entities: the National Security Council, the Principals Committee, the Deputies Committee and the Policy Coordination Committee.[105] The underlying rationale for the creation of this system is that one issue rarely affects only one agency, but rather influences multiple agencies. Each committee includes representatives from various cabinet departments, such as the Department of State or Department of the Treasury, which head federal agencies on policy areas ranging from finance to defense. Additional agencies can be added as needed.

The National Security Council is the principal agency for coordinating policy related to cyber incidents. Once the policy issue has been thoroughly discussed and consensus as to next steps reached in committee, a recommendation goes to the president who makes the final decision.

Presidential Policy Directive-41

In 2016, President Barack Obama issued Presidential Policy Directive-41 (PPD-41), which established the procedures and standards the government must follow during cyber incidents affecting public or private sector entities.[106] The Directive established lead federal agencies during "significant cyber incidents," or those likely to harm US national security interests, foreign relations, economy, public confidence, civil liberties, public health or public safety.[107] Additionally, the Directive required the Departments of Justice and Homeland Security to develop and maintain a public contact list that entities can use to report incidents to government authorities.

The Directive outlined that federal government agencies were to focus on three "lines of effort" during cyber incidents: threat response, asset response and intelligence support and related activities. In case a federal agency should be the affected party, it will assume a fourth area of focus: mitigation. This effort will include controlling the effects of the cybersecurity incident on agency operations, customers and workforce.[108] Additionally, the Directive also declared that a Cyber Unified Coordination Group was to be formed in the case of a significant cyber incident. This Group would include the lead agency for asset response, and as necessary, the following other actors: other federal agencies; representatives from state, local and tribal governments; the private sector; non-governmental organizations and international counterparts.[109]

US public-private partnerships

As mentioned in the US cybersecurity strategy section, the government´s cybersecurity priorities encourage federal agencies to partner with the private and academic sectors to achieve the nation´s cyber defense objectives. Although the concept of public-private partnerships is not as centralized as in the EU, which coordinates these partnerships through ECSO, there is considerable activity in this area. In addition, NIST coordinates a more formal public-private partnership through its National Cybersecurity Excellence Partnership (NCEP) initiative. Companies involved in the partnership pledge to provide hardware, software and expertise as part of a mutual government and private effort to advance the rapid adoption of secure technologies.[110]

The partnership includes companies such as Amazon Web Services, Cisco, Dell EMC, the Global Cyber Alliance, Hewlett Packard Enterprise, IBM, Intel, Microsoft and Symantec, among others.

Department of Homeland Security (DHS)

PPD-41 establishes the Department of Homeland Security as the federal lead agency for asset response activities, such as providing technical assistance to affected entities, containing vulnerabilities, reducing impact of cyber incidents and identifying other affected entities, among others.

Office of the Director of National Intelligence
The Directive determines that the Office of the Director of National Intelligence, through its Cyber Threat Intelligence Integration Center, will be the lead agency for intelligence support and related activities. Such activities include building situational threat awareness and sharing related intelligence, integrated analysis of threat trends and events, identification of knowledge gaps and the ability to degrade or mitigate threat capabilities, among others.[111]

Department of State
The US Department of State is the leading player in international cybersecurity policy. It aims to promote an "open, interoperable, secure and reliable information and communications infrastructure." It has been described as a "soft power approach" to compliment the hard power exhibited by the Departments of Justice and Defense.[112] The cyber division resides within the Department´s Bureau of Economic Affairs.[113]

Department of Defense
The Department of Defense is responsible for national cyber defense. It has its own cybersecurity strategy and three missions: to defend Department of Defense networks, systems and information; defend the US homeland and US national interests against cyberattacks of significant consequence; and support operational and contingency plans.[114] The Department of Defense also houses US Cyber Command, a military unit established in 2009 trained to defend against cyber attacks and to initiate them.

Department of the Treasury
The Department of the Treasury is tasked with preparing for cyber attacks aimed at the US financial services sector and protecting critical infrastructure within it.[115] Within the department, the Office of Critical Infrastructure Protection and Compliance coordinates with the public and private sector in order to achieve its goals.

In addition, the Department of the Treasury coordinates the Financial Crimes Enforcement Network, which works to safeguard the US financial system from illicit use, combat money laundering and promote national security through various initiatives. FinCEN works to ensure financial institutions are aware of their obligations during a cyber attack, encourage institutions to share cybersecurity-related information and foster the sharing of cybersecurity-related information between institutions, among others.[116]

Department of Commerce
The Department of Commerce is responsible for enhancing the nation´s cybersecurity awareness and safeguards, protecting privacy and supporting economic and national security, among others.[117] It does this through its National Institute of Standards and Technology, which publishes the NIST Framework to assist public and private sector companies with their cybersecurity plan.

Federal Trade Commission (FTC)
The Federal Trade Commission plays an important role in US cybersecurity and has a tremendous amount of interaction with the EU. It is the nation´s lead cybersecurity enforcement agency[118], acting as the regulator for the Privacy Act of 1974 and COPPA. It also ensures companies adhere to their established privacy policies and do not disclose consumer data without permission.

Department of Justice
The Department of Justice, acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force is the lead agency for threat response activities. These activities include carrying out law enforcement and national security investigative activities at the affected entity´s site, collecting evidence and gathering intelligence and linking related incidents, among others.[119]

Key Actors Real World Impact: White House eliminates cybersecurity coordinator role

In May 2018, the Trump administration decided to eliminate the "cyber coordinator" position, the nation´s top cyber policy professional in charge of harmonizing the government´s approach to cybersecurity policy and digital warfare.

According to the White House, the decision was made in order to "streamline authority" for the senior directors who lead National Security Council teams. The NSC is chaired by the US president and is the main vehicle for considering national security and foreign policy matters. The NSC cyber team has two senior directors, which ensures that "cyber coordination is already a core capability."

The cyber coordinator led a team that worked with agencies to develop a unified strategy for issues ranging from election security to digital deterrence. Part of the job also included representing the Trump administration in meetings with foreign partners. Cutting the position had been discouraged by many in the industry and on Capitol Hill.

"I don´t see how getting rid of the top cyber official in the White House does anything to make our country safer from cyber threats," Senate Intelligence ranking member Mark Warner said after the announcement, according to *Politico*.

Source: Politico, published online on 15 May 2018

5 COMPARATIVE ANALYSIS BETWEEN US AND EU CYBERSECURITY POLICIES

Overall, the biggest differences in US and EU cybersecurity policy landscapes can be explained by analysing the most significant laws passed by each region. In the EU, for instance, the biggest changes in cybersecurity and privacy have been prompted by the adoption of the NIS Directive and GDPR. The US has similarly undergone changes with the creation of the NIST Framework and the passage of the CLOUD Act and CISA.

The key differences emerge in various areas and concepts: laws vs. standards; the work toward harmonizing liability standards; regulation for all sectors vs. regulation for individual sectors; and streamlined enforcement vs. different enforcement actors. Naturally, some will ask, which approach is better? The question cannot be answered objectively. Each region has a different concept of cybersecurity and privacy and therefore shapes its policy using those ideas as a base.

The table below summarizes the common themes in the key cybersecurity policies in Europe and the US described above.

Cybersecurity Key points	EU	US	Similarities	Differences
Standards	**NIS Directive**: Law creates a common set of security standards that Member States must adhere to in order to be adequately prepared in case of a cyber attack. Also creates standards for operators of essential services in the EU. **Cybersecurity Act**: Legislative proposal would create a cybersecurity standards and certification scheme for ICT products in the EU. Certificates would be recognized by all Member States. **Liability standards in the EU**: No legislation that comprehensively address liability when it comes to new technologies	**NIST Framework**: Voluntary cybersecurity standards for the public and private sector. The framework aims to help companies safeguard their systems with flexible standards that help them "identify, prioritize, manage and/or communicate cyber risks." **Standard setting in the US**: Coordinated through the Department of Homeland Security. Adopts private sector consensus based standards if possible. **Liability standards in the US**: Liability laws are piecemeal and there is no comprehensive legislation in this	**Improve cyber preparedness**. The NIS Directive and the NIST Framework aim to improve cyber preparedness of public and private sector entities. **Best measures available**. The NIS Directive and the NIST Framework call on entities to use the best cybersecurity measures available. **Not one-size-fits-all**. Neither NIS or NIST are a one-size-fits-all solution. They recognize that organizations must employ measures that make sense for them and their specific risks. **Voluntary standards are important**. The	**Law vs. voluntary standards**. The NIS Directive is a law that must be followed by all EU Member States and operators of essential services. NIST is a voluntary framework that organizations can choose to adopt if they so wish. **EU appears to be actively working on harmonizing and clarifying liability standards.** It has called for the formation of a working group on this matter. There is no similar effort on a federal level in the US,

Cybersecurity Key points	EU	US	Similarities	Differences
	or liability in the case of a cyber attack. **eID Regulation**: eID would allow citizens of one European country to access services they have a right to in other EU countries by showing an ID.	area. There are federal, state and municipal laws.	certification framework for ICT products under the Cybersecurity Act would not be mandatory in the EU. Meanwhile, DHS always works to adopt voluntary standards adopted by the private sector. **Liability is not clearly defined**. Liability is mentioned in both regions at various levels but not defined at a comprehensive level or EU level.	although states and municipalities are active.
Privacy and Data Protection	**GDPR**: The regulation aims to control how businesses and entities obtain user data, how they process it and how they protect it, among many others. **E-privacy**: The E-Privacy Regulation is a legislative proposal that would establish privacy and data protection standards for electronic communications, guaranteeing confidentiality, simpler cookie rules and spam protection. **Privacy Shield**: EU and US agreement that establishes strict guidelines US companies must follow in order to transfer commercial data of EU users´	**Privacy Act of 1974**: The Privacy Act regulates the collection and use of data by US federal agencies. **Judicial Redress Act of 2015**: The law gives citizens of foreign countries the legal right to challenge how their data is used and processed by US federal agencies. **Federal Trade Commission Act**: This law gives the FTC the power to discipline companies that do not comply with their published privacy policies or disclose personal data without authorization. **Children´s Online Privacy Protection Act**: COPPA limits the	**Certain information must be protected**. The GDPR and the various US laws concerning privacy clearly establish that there are some types of information that must be protected at all costs. **Spam protection**. The US and the EU recognize that spam is a problem and attempt to cut down on the amount of spam users receive with specific proposed and current regulations.	**One regulation for all sectors vs. various regulations for different sectors**. With the GDPR, the EU has established the same rules for all sectors that collect data. The US has chosen to take a different approach, regulating specific sectors with specific laws. **Streamlined enforcement vs. various actors**. The GDPR establishes data protection authorities as the watchdogs to ensure that companies and entities

Cybersecurity Key points	EU	US	Similarities	Differences
	across the Atlantic.	collection of information from children under the age of 13 and gives parents certain control over the data. **Financial Services Modernization Act**: The law requires financial institutions to disclose their information-sharing practices and allow customers to decide if they want their information shared with other entities. **Health Insurance Portability and Accountability Act**: HIPAA protects an individual´s "personally identifiable health information" and requires entities safeguard this information, except under certain circumstances. **Fair Credit Reporting Act**: The Fair Credit Reporting Act regulates certain information can be shared and with who. It also requires entities to inform customers when they have taken an adverse decision based on the information. **CAN-SPAM Act**: The Controlling the Assault of		are complying with the law. This enforcement role is not as focused in the US, where different agencies may regulate different sectors.

Cybersecurity Key points	EU	US	Similarities	Differences
		Non-Solicited Pornography and Marketing Act regulates commercial email. It establishes standards that marketers must meet to send email and gives customers the right to have entities stop emailing them. **Electronic Communications Privacy Act**: The Electronic Communications Privacy Act protects wire, oral and electronic communications when they are being made, are in transit or are stored on computers. It also protects the contents of files held by service providers. **Privacy Shield**: EU and US agreement that establishes strict guidelines US companies must follow in order to transfer commercial data of EU users´ across the Atlantic.		
Public-Private Sharing	**GDPR**: Mandated public-private information sharing. The law requires private data controllers to notify data protection authorities of a security breach within 72 hours of becoming aware of the incident.	**Cybersecurity Information Sharing Act**: The Cybersecurity Information Sharing Act establishes safeguards and liability protection for private companies in order to encourage information	**Recognized need for information sharing between public and private entities**. With breach notification in the GDPR and the NIS Directive, the EU establishes the need to share	**Liability protection**. CISA recognizes that one of the barriers to information-sharing is liability and provides liability protection. The NIS Directive also

Cybersecurity Key points	EU	US	Similarities	Differences
	NIS Directive: Mandated public-private information sharing. The NIS Directive requires operators of essential services to report cybersecurity breaches that meet certain criteria to the appropriate data protection authorities. **E-evidence legislation**: EU response to the US CLOUD Act. Gives EU law enforcement authorities the right to request data from national and international service providers in other EU states.	sharing between these parties, other companies and the federal government. **CLOUD Act**: The Clarifying Lawful Overseas Use of Data Act requires US technology companies to provide the nation´s law enforcement agencies with information even if such information is in another country. It also provides a faster avenue for other countries to request data from law enforcement.	information. CISA clearly supports this goal, coordinating clear channels of communication between the public and private sectors. **Law enforcement access to data**. Law enforcement is given priority access to data even if the data is held in another country.	provides this, although it does not emphasize it. GDPR does not mention liability protection. E-evidence does not provide liability protection. **Mandatory vs. encouraged**. NIS and GDPR make breach reporting, and information sharing, mandatory. The US encourages sharing of cyber incidents.
Key actors in transatlantic cybersecurity policies	European Commission, EU Parliament, enforcement agencies and others.	US President, Congress, federal agencies and others.	**Clear recognition that cybersecurity is an important priority**. Both the executive and legislative arms of the parties acknowledge the importance of cybersecurity. Agencies also identify cybersecurity as important.	**EU adopts more streamlined policy-making process. US has various actors.** There are not many actors involved in the EU policy making process. The US, on the other hand, has various different processes, agencies and entities involved.

6 CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusions

The realm of cybersecurity and all that it encompasses is revolutionizing the technology landscape between Europe and the US. Thus, it is of paramount importance that the transatlantic partnership navigate the challenges ahead so that the vibrancy, health and mutual benefits of the relationship are sustained.

The White Paper delves into relevant legislation and public policies that influence future research and innovation collaboration between the EU and the US in the field of cybersecurity and privacy. These policy areas include standards and certification; privacy and data protection; and public-private information sharing. The White Paper underscores the indispensable role of the major players involved in these policies to effect positive change through collaboration, and the complexity of the interagency process in the US. It concludes with a comparative analysis of selected transatlantic policies on cybersecurity and privacy.

Regarding standards, the EU and the US do not have shared or mirrored pieces of legislation. In the US, the focal point for standards is the NIST Framework, issued in 2014 to improve critical infrastructure cybersecurity and built on voluntary consensus standards and industry best practices. At the EU level, the NIS Directive went into effect in 2018. Additionally, the European Commission proposal for the creation of an EU certification framework for ICT security products (the Cybersecurity Act) aims at unifying cybersecurity standards for all Member States. While the NIS Directive applies not only to EU Member States, but also US companies doing business in the EU, the NIS Framework is not obligatory for any entity.

In the privacy and data protection area, the US and the EU have adopted different strategies towards regulation. The EU follows a cross-cutting policy approach through the General Data Protection Regulation (GDPR) and the new e-Privacy Regulation, while in the US there is no comprehensive federal data protection law. Instead, the US has opted for an approach tailored to specific sectors and types of information, including among many others, the financial and health information sectors.

Regarding public-private information sharing, there is transatlantic a consensus about the role information sharing plays to prevent and mitigate cybersecurity attacks that also affect private companies, in particular, Operators of Essential Services and Digital Service Providers. From this perspective, certain mechanisms for sharing information have been implemented through legislation and policies on both sides of the Atlantic. On the EU side, this has been done through the GDPR and NIS Directive, while the US has adopted CISA and the CLOUD Act. In fact, sharing information across borders is an opportunity to reinforce transatlantic collaboration, since cross-border cyber incidents will continue to occur. The March 2018 resolution of the *US vs. Microsoft* extraterritoriality case illustrates the challenges of government regulations and policy attempting to keep up with technological advances rather than merely reacting, many times years after the actual need.

The analysis of these policies and legislation demonstrates the complexity of the issues surrounding cybersecurity and privacy and the multiple players involved in monitoring problems and implementing solutions, especially in the US. Unlike in the EU, where specific agencies work on the European Commission´s cybersecurity priorities and strategies, the US sets and enforces its national security policies, including cybersecurity policy, through the National Security Council Interagency Process, where multiple players are involved.

Nevertheless, the comparative analysis of EU and US policies on cybersecurity and privacy demonstrates that notwithstanding the differences, many transatlantic approaches to cybersecurity are aligned that can provide common ground for cyberspace harmonization between the US and the EU.

6.2 Policy Recommendations

Strengthening EU-US dialogues and improving cooperation on cybersecurity and privacy research and innovation are not to eliminate policy differences but rather to collaboratively develop common ground measures. In this way, advantageous synergies between EU and US policies and legislation on cybersecurity and privacy will emerge that further the overall benefits of transatlantic innovation, economic ties and private sector investment.

Based on our analysis of key cybersecurity policies, we have crafted policy recommendations, both near-term attainable milestones and longer-term benchmarks detailed below, as to how thought-leaders, policy makers, and elected officials on both sides of the Atlantic can achieve integrated dialogue and cooperation.

Near-term attainable milestones

1. **Raise awareness among thought leaders, policy makers and elected officials about the myriad advantages of pursuing deeper connections in the cybersecurity sector.** Such awareness can be created through low-cost means including real-time information and insights delivered through various social media. In this way, relevant actors involved in cybersecurity policies on both sides of the Atlantic can benefit from a bottom-up approach and social media engagement to effectively address cybersecurity issues.

2. **Increase synergy and collaboration between the agencies responsible for the NIST Framework and those tasked with implementation of the NIS Directive and the GDPR.** The desired outcomes are a common framework, standards and practices that facilitate compliance by companies in the EU and the US. As in any endeavor, the deeper the shared working experiences, the more progress in attaining and the more realistic the expectation of results. To this end, the use of internet-based connections on a regularly scheduled basis to augment travel to conferences and workshops is a no-cost method that will enhance cooperation on these issues. Closer collaboration will aid in creating points of convergence between the EU and the US to implement common policies regarding standards, privacy and data protection.

3. **Adopt a common and harmonised language for stakeholder communication, which will accelerate EU-US collaboration in cybersecurity.** This goal can be achieved through requests for feedback in consultation with relevant industry representatives to advise and inform government officials who are charged with developing agreed-upon terms and taxonomy. This approach also advances improved communication and interactions between policy makers in cybersecurity and privacy.

4. **Strengthen EU-US cybersecurity dialogue.** Existing dialogues like the EU-US Cybersecurity Dialogue and the EU-US Information Society Dialogue must broaden their focus to identify areas for coordination and cooperation in cybersecurity and privacy. Encouragement of meaningful connections among all areas of society, not just limited to experts in the field but extending to commercial enterprises, civil society representatives and elected officials, will expand the demand for intersections of closer collaboration. Such connections

can be fostered at the student level and move on to relevant NGO groups and the political sphere including at the grassroots local level. Policy makers involved in EU-US dialogues will profit from these enhanced transatlantic ties among multiple demographics that also will have a positive influence on discussions about the future of cybersecurity in Europe and the US and transatlantic cooperation in the field.

5. **Lay the groundwork for a joint roadmap for EU-US collaboration in cybersecurity and privacy R&I.** By assembling input through the Action's significant major multiplier groups that enjoy extensive memberships in diverse groups of society, foundational work will be developed that can begin to inform a way forward for transatlantic cooperation in these fields. The over-arching strategy of the AEGIS project is to support policy makers to identify areas of most promise to sustain transatlantic collaboration and dialogue in cybersecurity and privacy R&I.

Longer-term benchmarks

1. **Establish a framework for resolving conflicts that arise from inevitable differences in policy and regulation.** Both the US and the EU have often stated the importance of working with other countries to establish international cybersecurity policies taking into consideration mutual respect for sovereignty and the global nature of the internet. Different regulatory postures regarding the global cybersecurity environment can lead to legal conflicts between countries and have a chilling effect on R & I collaboration as well as private sector investment. A framework to address such conflicts when they arise is of paramount importance because conflicts within the framework of legal requirements can put companies in a position where complying with the law in one country means breaking the law in another. One example of such conflict can be seen per the French interpretation, mentioned in the White Paper, of the Right to be Forgotten. While France requires search engines to remove Right to be Forgotten cases outside the EU, it does not acknowledge that such requirement could represent a violation of freedom of speech laws in other countries. As a potential remedy, a web-based "clearing house" mechanism could be created that would allow input from a variety of public sector, private industry and civil society voices, thereby eliminating as much as possible these types of conflicts.

2. **Establish a new mechanism for more effective coordination between cybersecurity agencies and stakeholders on both sides of the Atlantic.** One example of this is through the NIS Cooperation Group that would enhance the sharing of information on threats and best practices at an international level. Such coordination requires expanded collaboration among key players like the European Commission, ENISA and Member States on the EU side. In the US, coordination would include the agencies working on cybersecurity policies through the interagency process and establishing closer official and informal relationships with European decision-makers to accelerate achievement of mutual objectives. Thus, this coordination mechanism would ensure cooperation and sharing information between cybersecurity-related agencies across the Atlantic.

3. **Promote the adoption of a unified approach based on international standards to foster collaboration in cybersecurity R&I across the Atlantic.** A unified approach will allow EU researchers to develop products and services that have the capabilities to compete in the highly-competitive US market and other international markets. Collaborating on the development of common standards in ICT and ensuring those standards remain voluntary, consensus-based and market-led are critical to this unified approach. With government agencies taking the lead, the private sector, academia and the research communities can ably

guide the facilitation of these objectives through leveraging of existing avenues of communication. Because industry reacts quickly to the needs and desires of its customers, the feedback from companies engaged in these sectors will be invaluable in achieving competitive advantages of benefit to both transatlantic enterprises and policy makers.

4. **Stimulate public-private partnerships (PPPs) by engaging public organizations and private industry to enthusiastically take on the role of champions of transatlantic collaboration in cybersecurity.** Since the private sector is motivated by what serves their customers, engaging civil society and NGO representatives to broaden diversity of opinion and inclusion of disparate perspectives will stimulate company participation. Industry willingness, advocacy and enthusiasm to sustain partnerships with the public sector will be promoted as an outcome and as a vehicle to better support their customers, market advantage and access to innovation. By working together on cybersecurity initiatives, the public and private sectors can both benefit from PPPs, ensuring that cybersecurity developments in the private sector and their policy implications are well understood by those representing the public good as they craft and negotiate policy.

7 REFERENCES

[1] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2013). Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[2] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2013). Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[3] The EU Cybersecurity Strategy | IT Governance. (2018). Retrieved from https://www.itgovernance.eu/en-ie/eu-cybersecurity-strategy-ie

[4] Resilience, Deterrence and Defence: Building strong cybersecurity in Europe. (2017). Retrieved from https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe

[5] Inception Impact Assessment: Proposal to create a cybersecurity competence network with a European Cybersecurity Research and Competence Centre. (2018). Retrieved from https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1598442_en

[6] Paliamentary questions: 9 November 2017. Answer given by Vice-President Ansip on behalf of the Commission. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-005353&language=EN

[7] State of the Union 2017 – Cybersecurity: Commission scales up EU´s response to cyber-attacks. http://europa.eu/rapid/press-release_IP-17-3193_en.htm

[8] Nakashima, E. (2011). Obama administration outlines international strategy for cyberspace. *The Washington* Post. Retrieved from https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html?noredirect=on&utm_term=.81232a4eeaac

[9] Nakashima, E. (2011). Obama administration outlines international strategy for cyberspace. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html?noredirect=on&utm_term=.81232a4eeaac

[10] International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. (2011). Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdfInternational Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

[11] Foreign Policy Cyber Security. (2018). Retrieved from https://obamawhitehouse.archives.gov/node/233081

[12] Executive Order 13800 Update Issue 1 | US-CERT. (2017). Retrieved from https://www.us-cert.gov/eo13800/Issue-1

[13] Marks, J. (2018). National Cyber Strategy Coming Soon From White House. *Nextgov*, pp. https://www.nextgov.com/cybersecurity/2018/04/national-cyber-strategy-coming-soon-white-house/147382/.

[14] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[15] The Directive on Security of Network and Information Systems (NIS Directive). (2016). Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[16] What does the NIS Directive mean for the EU Citizens?. (2018, May 3). Retrieved from https://ec.europa.eu/digital-single-market/en/news/what-does-nis-directive-mean-eu-citizens

[17] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[18] What does the NIS Directive mean for the EU Citizens?. (2018, May 3). Retrieved from https://ec.europa.eu/digital-single-market/en/news/what-does-nis-directive-mean-eu-citizens

[19] Kuschewsky, M., & Economides, C. (2017). European Commission issues a new EU Cybersecurity Strategy | Global IP & Technology Law Blog. Retrieved from https://www.iptechblog.com/2017/09/european-commission-issues-a-new-eu-cybersecurity-strategy/

[20] Niebler, A. (2018). Legislative train schedule | European Parliament. Retrieved from http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-eu-cybersecurity-agency-and-cybersecurity-act

[21] Digital Single Market: Cybersecurity. https://ec.europa.eu/digital-single-market/en/cyber-security

[22] European Commission – Press release. Digital Single Market: Commission calls for swift adoption of key proposals and maps out challenges ahead. http://europa.eu/rapid/press-release_IP-17-1232_en.htm

[23] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31985L0374

[24] Call for experts for a group on liability and new technologies. https://ec.europa.eu/digital-single-market/en/news/call-experts-group-liability-and-new-technologies

[25] Attacks against information systems. https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:32013L0040

[26] Digital Single Market. Policy. E-Identification. https://ec.europa.eu/digital-single-market/en/e-identification

[27] Foreign Policy Cyber Security Executive Order 13636. (2018). Retrieved from https://obamawhitehouse.archives.gov/node/298406

[28] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[29] Webcast: Cybersecurity Framework Version 1.1 Overview. (2018). Retrieved from https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview

[30] NIST Releases Version 1.1 of its Popular Cybersecurity Framework. (2018). Retrieved from https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[31] The Benefits of U.S.-European Security Standardization. National Institute of Standards and Technology. https://www.nist.gov/sites/default/files/nistir7861.pdf

[32] After the Breach: Cybersecurity Liability Risk. https://www.lawandsecurity.org/wp-content/uploads/2014/06/CLS-After-the-Breach-Final.pdf

[33] Cybersecurity Failures and Resulting Liability Issues. http://www.acc.com/legalresources/quickcounsel/cybersecurity.cfm

[34] DFS Cybersecurity Regulation Compliance Requirements Are Effective Today. https://www.dfs.ny.gov/about/press/pr1708281.htm

[35] Chicago, Like San Francisco, Sues Equifax Over Breach. http://www.govtech.com/dc/articles/Chicago-Like-San-Francisco-Sues-Equifax-Over-Breach.html

[36] After the Breach: Cybersecurity Liability Risk. https://www.lawandsecurity.org/wp-content/uploads/2014/06/CLS-After-the-Breach-Final.pdf

[37] Scott, M. (2018). Zuckerberg expected to apologize to EU Facebook users. *Politico*. Retrieved from https://www.politico.eu/article/mark-zuckerberg-hearing-eu-european-union-brussels-cambridge-analytica-antonio-tajani/

[38] Brandom, R. (2018). Mark Zuckerberg will appear before Congress to address Cambridge Analytica scandal. *The Verge*. Retrieved from https://www.theverge.com/2018/3/27/17168228/mark-zuckerberg-congress-testify-cambridge-analytica

[39] Voigt, P., & Bussche, A. (2018). The EU General Data Protection Regulation (GDPR). Retrieved from https://www.pwc.lu/en/general-data-protection/docs/pwc-gdpr-territorial-scope.pdf

[40] Art. 3 GDPR – Territorial scope | General Data Protection Regulation (GDPR). (2018). Retrieved from https://gdpr-info.eu/art-3-gdpr/

[41] U.S. firms are still unprepared for looming EU data privacy rules. https://www.reuters.com/article/bc-finreg-data-privacy-rules/u-s-firms-are-still-unprepared-for-looming-eu-data-privacy-rules-idUSKCN1FX2D2

[42] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[43] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[44] Doubek, J. (2018). Google Has Received 650,000 'Right To Be Forgotten' Requests Since 2014. *NPR*. Retrieved from https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014

[45] A new era for data protection in the EU: What changes after May 2018. (2018). Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

[46] Privacy Shield Program Overview | Privacy Shield. (2018). Retrieved from https://www.privacyshield.gov/Program-Overview

[47] A new era for data protection in the EU: What changes after May 2018. (2018). Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

[48] Handley, L. (2018). US companies are not exempt from Europe's new data privacy rules — and here's what they need to do about it. *CNBC*. Retrieved from https://www.cnbc.com/2018/04/25/gdpr-data-privacy-rules-in-europe-and-how-they-apply-to-us-companies.html

[49] Ong, T. (2018). Facebook announces new European privacy controls, for the world. *The Verge*. Retrieved from https://www.theverge.com/2018/4/18/17250840/facebook-privacy-protections-europe-world-gdpr

[50] The new EU ePrivacy Regulation: what you need to know. (https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/)

[51] Proposal for an ePrivacy Regulation. (2018). Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[52] Proposal for an ePrivacy Regulation. (2018). Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[53] Proposal for an ePrivacy Regulation. (2018). Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[54] Proposal for an ePrivacy Regulation. (2018). Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[55] Privacy Shield Program Overview. (n.d.). Retrieved from https://www.privacyshield.gov/Program-Overview

[56] Lomas, N. (2018, July 5). EU parliament calls for Privacy Shield to be pulled until US complies. Retrieved from https://techcrunch.com/2018/07/05/eu-parliament-calls-for-privacy-shield-to-be-pulled-until-us-complies/?guccounter=1

[57] European Commission launches EU-U.S. Privacy Shield: Stronger protection for transatlantic data flows. (2016, July 12). Retrieved from http://europa.eu/rapid/press-release_IP-16-2461_en.htm

[58] Loeb, R., Goldman, B. P., & Tabatabai, E. S. (2018, April 6). The CLOUD Act, Explained. Retrieved from https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained

[59] Loeb, R., Goldman, B. P., & Tabatabai, E. S. (2018, April 6). The CLOUD Act, Explained. Retrieved from https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained

[60] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)

[61] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)

[62] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)

[63] Overview of the Privacy Act of 1974 | OPCL | Department of Justice. (2015). Retrieved from https://www.justice.gov/opcl/introduction

[64] The Privacy Act and the Freedom of Information Act | Social Security Administration. (2018). Retrieved from https://www.ssa.gov/agency/privacyact.html

[65] Federal Trade Commission Act. (2018). Retrieved from https://www.ftc.gov/es/enforcement/statutes/federal-trade-commission-act

[66] Leuan, J. (2018). Data protection in the United States: overview. Retrieved from https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default)

[67] Protecting Children's Privacy Under COPPA: A Survey on Compliance [Ebook]. Retrieved from https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

[68] Protecting Children's Privacy Under COPPA: A Survey on Compliance [Ebook]. Retrieved from https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

[69] The Gramm-Leach-Bliley Act of 1999 (GLBA). Investopedia. Retrieved from https://www.investopedia.com/terms/g/glba.asp

[70] Summary of the HIPAA Privacy Rule. (2013). Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[71] Fair Credit Reporting Act. (2018). Retrieved from https://www.ftc.gov/es/enforcement/statutes/fair-credit-reporting-act

[72] CAN-SPAM Act: A Compliance Guide for Business. (2009). Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

[73] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22. (2013). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

[74] Guidelines on personal data breach notifications – stress test on risk governance. (2018). Retrieved from https://talkingtech.cliffordchance.com/en/cybersecurity/guidelines-on-personal-data-breach-notifications--stress-test-on.html

[75] Guidelines on personal data breach notifications – stress test on risk governance. (2018). Retrieved from https://talkingtech.cliffordchance.com/en/cybersecurity/guidelines-on-personal-data-breach-notifications--stress-test-on.html

[76] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[77] E-evidence – cross-border access to electronic evidence. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

[78] Petrasic, K. (2016, April 18). CISA Guidance Clarifies How to Share Cyber Threat Information… but Issues Remain. Retrieved from https://www.whitecase.com/publications/alert/cisa-guidance-clarifies-how-share-cyber-threat-information-issues-remain

[79] Karp, B., & Weiss, P. (2016). Federal Guidance on the Cybersecurity Information Sharing Act of 2015. Retrieved from https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

[80] Karp, B., & Weiss, P. (2016). Federal Guidance on the Cybersecurity Information Sharing Act of 2015. Retrieved from https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

[81] Karp, B., & Weiss, P. (2016). Federal Guidance on the Cybersecurity Information Sharing Act of 2015. Retrieved from https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

[82] Petrasic, K. (2016, April 18). CISA Guidance Clarifies How to Share Cyber Threat Information… but Issues Remain. Retrieved from https://www.whitecase.com/publications/alert/cisa-guidance-clarifies-how-share-cyber-threat-information-issues-remain

[83] Karp, B., & Weiss, P. (2016). Federal Guidance on the Cybersecurity Information Sharing Act of 2015. Retrieved from https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

[84] Information Sharing Under CISA: What It Means For Companies. https://us.eversheds-sutherland.com/portalresource/lookup/poid/Z1tOl9NPluKPtDNIqLMRV56Pab6TfzcRXncKbDtRr9tObDdEo0JDqG3!/fileUpload.name=/Information%20Sharing%20Under%20CISA%20What%20It%20Means%20For%20Companies.pdf

[85] Transatlantic Cybersecurity Report. Forging a United Response to Universal Threats. (2018). Retrieved from https://www.uschamber.com/TransatlanticCybersecurityReport

[86] Aegis. (2018). U.S. Supreme Court officially dismisses Microsoft data search case | AEGIS. Retrieved from http://aegis-project.org/us-supreme-court-microsoft-data-search/

[87] Nielsen, N. (2018, March 26). Rushed US Cloud Act triggers EU backlash. Euobserver. Retrieved from https://euobserver.com/justice/141446

[88] Legislative train schedule | European Parliament. (2018). Retrieved from http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-e-privacy-reform

[89] European Council, 19-20/10/2017. (2017, October 19). Retrieved from http://www.consilium.europa.eu/en/meetings/european-council/2017/10/19-20/

[90] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[91] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[92] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[93] About ECSO. Mission & Objectives. https://www.ecs-org.eu/about

[94] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[95] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[96] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[97] Joint Cybercrime Action Taskforce (J-CAT). (2018). Retrieved from https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

[98] Standards and certification — ENISA. (2018). Retrieved from https://www.enisa.europa.eu/topics/standards

[99] Standards and certification — ENISA. (2018). Retrieved from https://www.enisa.europa.eu/topics/standards

[100] Cybersecurity in the European Union and beyond: Exploring the Threats and Policy Responses. (2018). Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf

[101] Eurojust - European Union - European Commission. (2018). Retrieved from https://europa.eu/european-union/about-eu/agencies/eurojust_en

[102] CyberSponse. (2017). The Difference Between CERTs and CSIRTs? What are They?. Retrieved from https://cybersponse.com/the-difference-between-certs-and-csirts-what-are-they

[103] CERT-EU — ENISA. (2018). Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building/european-initiatives/cert-eu

[104] Factsheet: Cyber Defence. (2018). Retrieved from https://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-cyber-defence

[105] Marcella, G. (2008). *Affairs of State*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

[106] Presidential Policy Directive -- United States Cyber Incident Coordination. (2015). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[107] Presidential Policy Directive -- United States Cyber Incident Coordination. (2015). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[108] Presidential Policy Directive -- United States Cyber Incident Coordination. (2015). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[109] New U.S. Cyber Security Policy Codifies Agency Roles. (2016). Retrieved from https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role

[110] Partners: National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/partners

[111] Presidential Policy Directive -- United States Cyber Incident Coordination. (2015). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[112] Newmeyer, K. (2015, May 13). The U.S. State Department and Cybersecurity. Retrieved from http://www.nationalcybersecurityinstitute.org/government/the-u-s-state-department-and-cybersecurity/

[113] Johnson, D. B. (2018, February 6). Trump administration announces new cyber office at State. Retrieved from https://fcw.com/articles/2018/02/06/state-cyber-office-hearing.aspx

[114] The DoD cyber strategy. (2015). Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[115] CYBERSECURITY: Department of the Treasury's Activities to Protect Critical Infrastructure in the Financial Services Sector. (2016). Retrieved from https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-16-038.pdf

[116] United States Department of the Treasury, Financial Crimes Enforcement Network. Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime. https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

[117] Cybersecurity. (2018). Retrieved from https://www.commerce.gov/tags/cybersecurityybersecurity. https://www.commerce.gov/tags/cybersecurity

[118] Mitchell, C. (2015). FTC takes over as top cybersecurity enforcer. Examiner Washington. Retrieved from https://www.washingtonexaminer.com/ftc-takes-over-as-top-cybersecurity-enforcer

[119] Presidential Policy Directive -- United States Cyber Incident Coordination. (2016). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

aegis accelerating EU–US Dialogue in Cybersecurity and Privacy

Quotation:

When quoting information from this report, please use the following phrase:

"White Paper on Cybersecurity Policy: Common Ground for EU-US Collaboration. AEGIS project."

Consortium:

inmark europa

Consiglio Nazionale delle Ricerche

Waterford Institute of Technology

Hewlett Packard Enterprise

european american chamber of commerce new jersey

THE PROVIDENCE GROUP

RUTGERS

aegis-project.org linkedin.com/company/aegis-project @aegis_cyber