Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence

*Clare Sullivan* [a,*], *Eric Burger* [b]

[a] *Law Center, Georgetown University, Washington, DC, USA*
[b] *Department of Computer Science, Georgetown University, Washington, DC, USA*

*Keywords:*
Privacy
Cyber-threat
Intelligence
Business-to-business sharing
Data collection
Disclosure
Privacy and public interest

A B S T R A C T

This article reports on preliminary findings and recommendations of a cross-discipline project to accelerate international business-to-business automated sharing of cyber-threat intelligence, particularly IP addresses. The article outlines the project and its objectives and the importance of determining whether IP addresses can be lawfully shared as cyber threat intelligence.

The goal of the project is to enhance cyber-threat intelligence sharing throughout the cyber ecosystem. The findings and recommendations from this project enable businesses to navigate the international legal environment and develop their policy and procedures to enable timely, effective and legal sharing of cyber-threat information. The project is the first of its kind in the world. It is unique in both focus and scope. Unlike the cyber-threat information sharing reviews and initiatives being developed at country and regional levels, the focus of this project and this article is on business-to-business sharing. The scope of this project in terms of the 34 jurisdictions reviewed as to their data protection requirements is more comprehensive than any similar study to date.

This article focuses on the sharing of IP addresses as cyber threat intelligence in the context of the new European Union (EU) data protection initiatives agreed in December 2015 and formally adopted by the European Council and Parliament in April 2016. The new EU General Data Protection Regulation (GDPR) applies to EU member countries, a major focus of the international cyber threat sharing project. The research also reveals that EU data protection requirements, particularly the currently applicable law of the Data Protection Directive 95/46/EC (1995 Directive) (the rules of which the GDPR will replace in practice in 2018), generally form the basis of current data protection requirements in countries outside Europe. It is expected that this influence will continue and that the GDPR will shape the development of data protection internationally.

* *Corresponding author.* Law Center, Georgetown University, 600 New Jersey Ave NW, Washington, DC 20001, USA.
*E-mail address:* cls268@georgetown.edu (C. Sullivan).

http://dx.doi.org/10.1016/j.clsr.2016.11.015

0267-3649/© 2016 Clare Sullivan & Eric Burger. Published by Elsevier Ltd. All rights reserved.

In this article, the authors examine whether static and dynamic IP addresses are "personal data" as defined in the GDPR and its predecessor the 1995 Directive that is currently the model for data protection in many jurisdictions outside Europe. The authors then consider whether sharing of that data by a business without the consent of the data subject, can be justified in the public interest so as to override individual rights under Articles 7 and 8(1) of the Charter of Fundamental Rights of the European Union, which underpin EU data protection. The analysis shows that the sharing of cyber threat intelligence is in the public interest so as to override the rights of a data subject, as long as it is carried out in ways that are strictly necessary in order to achieve security objectives. The article concludes by summarizing the project findings to date, and how they inform international sharing of cyber-threat intelligence within the private sector.

© 2016 Clare Sullivan & Eric Burger. Published by Elsevier Ltd. All rights reserved.

## 1. The International Cyber Threat Information Sharing project in context

The International Cyber Threat Information Sharing (ICTS) project is cross-discipline research being conducted by the Security and Software Engineering Research Center ($S^2$ERC) at Georgetown University in Washington DC. The ICTS project is part of the Cyber Threat Intelligence Information Sharing Exchange Ecosystem program (CyberISE) program at the $S^2$ERC.

CyberISE consists of a number of related projects, all with the goal of enhancing the world's network security posture through the accelerated adoption of automated threat intelligence sharing. The ultimate goal is for automation and standardization in this area to transform monitoring, detection, sharing, reaction to and remediation of, cyber threats. Participation in the CyberISE program draws from interrelated, but autonomous, entities:

- Enterprises and end users that may or may not be under attack, or that notice unusual host or network behaviour, and wish to keep their own networks safe and operational;
- Organizations responsible for operating secure networks and systems, both in the public and private sectors, that have a mandate (public sector) or contract (private sector) to keep other's networks safe and operational;
- Information-sharing organizations that produce, collect, analyse, vet and distribute cyber threat intelligence on behalf of their stakeholders, both as a proprietary business, and as a community resource, such as Information Sharing and Analysis Centers and Organizations (ISAC and ISAO); and
- Vendors of cybersecurity products and services.

There has been a lot of effort over the past decade by technical standards development organizations such as the Internet Engineering Task Force (IETF), the International Telecommunications Union Telecommunication Standardization Sector (ITU-T), and most recently OASIS to standardize technologies for cyber threat intelligence sharing. Clearly, with a decade of availability of technical standards, if there has not been uptick in information sharing, the barriers are most likely not solely due to a lack of availability of standardized technologies. Exploration of international norms for the sharing of data, as well as the technical means to make that happen, is necessary. As important as all of the technology and standardization is, this is also a policy problem, which is inter-jurisdictional.

A common cyber security ecosystem is within grasp, but all stakeholders must be comfortable that it supports their policies and legal obligations. Cyber threats cross enterprise, network, and national boundaries, so solutions to the cyber threat intelligence sharing issue must take into account different policies and laws on information sharing within industry sectors and across national boundaries. Not only does this problem span agencies, it spans governments and industry verticals. This key reality underpins the ICTS project and the cross-discipline strategy for accelerating International business-to-business sharing of cyber-threat intelligence. The ICTS team is cross-discipline, bringing together computer science and legal experts.

### 1.1. *Overview of ICTS project technical issues – automated sharing of threat intelligence*

Automated exchange of cyber threat intelligence information is a key part of the ICTS Project. This automation is designed to accelerate the pace of intelligence exchange, which is a key objective of the broader CyberISE program.

To date, there have been a number of *ad hoc* mechanisms for automated cyber threat exchange, such as IODEF/RID and STIX/TAXII. Often, and particularly within commercial enterprises, businesses use proprietary formats that are not interoperable beyond the business' network. Moreover, these technologies were developed in a legal vacuum, so they neither support the legal regimes in which they might operate, nor appropriately redact or obfuscate personal information when transmitted. These technologies are also not yet mature. Consequently, exploring the legal and policy environment in which trans-border business-to-business cyber threat intelligence sharing occurs is timely.

While no single technology can fully protect organisations from all cyber intrusions and attacks, automated sharing of threat intelligence is an important factor to addressing the problem. The technical specifics of this part of the project are outside the focus of this article, but briefly, the automation being

developed as part of this project improves the speed at which information about a potential threat can be disseminated around the world. This provides organizations with real-time warning of impending threats. Timely warning enables an organization to prepare its systems and personnel to address the threat. Early warning enables an organisation to position itself, ideally to prevent intrusion and attack, but at least to minimize impact. Automated intelligence sharing also enables an organization to monitor the threat, and obtain valuable insight into its nature including intrusion points, and other aspects of modus operandi and source, including possible attribution, which further inform threat assessment and response.

### 1.2. *Overview of legal issues – legality of automated sharing of threat intelligence*

The perception that automated sharing of some information may not be legal in all jurisdictions can hinder effective sharing of cyber threat intelligence. Data protection legislation and privacy law applies to the sharing of data if it contains personal or private information as defined by the applicable law. Other aspects such as, the purpose for which that information was originally collected, the location of the original collection and where it is to be transferred and disclosed and under what circumstances, all affect the legality of the sharing. Domestic law and regional regulation can also impact the legality and effectiveness of non-disclosure agreements. These aspects all affect the willingness and legal ability of organizations to engage in business-to-business sharing of cyber-threat information internationally.

A major impediment identified by the project, as hindering the implementation and adoption of business-to-business threat sharing, is the perception that sharing of IP addresses may not be legal in all jurisdictions. A multi-national corporation's internal information sharing may, of course, be subject to differing national rules; and there is a belief that different jurisdictions have very different rules and regulations pertaining to privacy and data protection. To formulate the requirements for automated cyber threat information sharing, and to evaluate other efforts for information exchange,[1] an understanding of the international legal situation is required. This is the research focus of the legal component of the ICTS project (ICTS-Legal) and it is the focus of this article.

## 2. The ICTS-Legal project

ICTS-Legal commenced in late 2015. It is a continuation of earlier research that focused on business-to-business sharing of cyber-threat intelligence information within the United States of America (U.S.). The ICTS-Legal project examines the international environment, particularly the laws of major US trading partners regarding privacy and data protection.

The immediate objective of the legal component of the ICTS project is to provide a comprehensive picture of the international legal environment for the purposes of fostering international business-to-business cyber intelligence information sharing. The findings from this research can be used to assist companies, including multinationals in focussing and developing their policy and legal procedures to enable effective and legal sharing of cyber-threat information, including automated sharing, within the corporate group and between corporations operating in major jurisdictions. The long-term goal of this project is to enhance the global security posture by enhancing cyber threat intelligence sharing throughout the cyber ecosystem. The ultimate goal is for automation and standardization in this area to transform how cyber threats are monitored, detected, addressed, remediated, and ultimately deterred.

Overall, ICTS-Legal examines the relevant law in 34 major OECD countries[2], beginning with the European Union (EU); then moving on to other nations in Europe, the Asia Pacific, Canada and South America. The EU regulatory environment is the starting point for the legal component of the project because those requirements generally set the highest international standard. The second stage, review of the law of countries in the Asia Pacific and in Canada, has been completed. The third stage, which will examine South America and major countries in Europe,[3] is now underway. Ultimately, the examination may extend to non-OECD countries such as the Russian Federation, Ukraine, and Romania.

The sharing of an Internet Protocol address (IP address) as threat intelligence is a major focus of the ICTS-Legal project. IP addresses can be static and unchanging or dynamic. An administrative authority assigns dynamic addresses to internet-connecting devices when they boot. Some residential Internet service providers periodically reassign different IP addresses for a host, often to deter that user from running a server but also to protect the user from someone tracking them by noting their IP address. Originally, dynamic IP addresses were assigned because they allow the network to use a smaller pool of IP addresses for intermittently connected users, such as for dial-up Internet access; and currently, internet service providers usually assign dynamic IP addresses to their customers.[4]

[1] Other efforts for information exchange include those of RID/IODEF, TAXII/STIX, OpenIOC, ITU-T, and IEEE but without requirements, the different technical directions for automated cyber threat intelligence sharing cannot be properly evaluated.

[2] Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary Iceland, Ireland, Israël, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States.

[3] The European country analysis was to be the second stage of the project but as a result of the recent approval of the new GDPR, the individual country review in Europe will be done later to take into account the impact of its entry in force in each country.

[4] See Rekhter et al., *Address Allocation for Private Internets*, IETF RFC 1918, February 1996. An IPv4 address is a 32-bit integer that identifies a host on the Internet. Sometimes the host is a device called a Network Address Translator, or NAT. A NAT translates from a private network to the NAT's host address on the Internet.

In the US, an IP address is, by case law,[5] not personally identifiable information (the US nearest-equivalent concept to that of the EU concept of personal data under EU data protection law), so it can be lawfully shared domestically. The question examined in ICTS-Legal project and this article is whether an IP address is personal data/information under the European Union (EU) data protection requirements, which apply to EU member states. This is a major focus for the ICTS project because many of the 34 countries, whose laws are to be considered in the project, are in the EU. In addition, the new EU General Data Protection Regulation 5419/16 (GDPR)[6] also has an extraterritorial operation beyond Europe; and as this project has found, the EU requirements are the model for data protection law in most countries outside the EU.

## 3. Overview of the new EU Data Protection Regulation and relevance to the ICTS-Legal project

The GDPR is part of data protection reform to position Europe for the digital age, which includes the move towards achieving the vision of an EU Digital Single Market in 2016/7. The data protection package is also part of the EU Agenda on Security,[7] and it includes a major focus on cyber security. This reform updates and replaces the Data Protection Directive 95/46/EC (1995 Directive)[8] and the 2008 Framework Decision for the police and criminal justice sector.[9]

The data protection reform package consists of the GDPR and the Data Protection Directive for Police and Criminal Justice Authorities (DPDPC).[10] The GDPR and the DPDPC are intended to bring more harmonisation to the domestic laws of EU member states in these areas and are thus designed to facilitate cross-border cooperation to more effectively combat crime and terrorism. For background, a 'Regulation' is a binding legislative act that must be applied in its entirety across the EU; whereas, a 'Directive' is a legislative act that sets out goals that all EU countries must achieve (by way of minimum-level legal provisions), however, it is up to the individual countries to devise their own laws on how to reach these goals.

The GDPR sets out requirements regarding the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[11] The Regulation "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[12] The GDPR is designed to provide individuals with more control over personal data, while updated and unified rules facilitate the development of the new EU Digital Single Market. The GDPR, particularly as it applies to sharing IP addresses as cyber threat intelligence, is a focus of ICTS-Legal and of this article. The GDPR rules will only apply 2 years after it became law, i.e. on 25 May 2018. During the 2-year transition period, the rules of the 1995 Directive remain in effect, and the European Commission will work closely with member state data protection authorities to ensure uniform application of the new rules and will inform EU citizens of their data protection rights, and companies about their data protection obligations.

The DPDPC is intended to protect the data of victims, witnesses, and suspects of crimes, in the context of a criminal investigation and law enforcement action. This reform is designed to improve cooperation to address terrorism and other serious crime in Europe. Processing of the personal data of EU subjects (as defined in Article 4(1)-(3)), which includes victims, witnesses and suspects, must comply with the principles of necessity, proportionality, and legality as set out in Chapter II of the new Regulation. Supervision will be by independent national data protection authorities, and judicial remedies for infringement by data controllers and supervising authorities are set out in Chapter VIII of the new Directive. The DPDPC shows the dual focus of the EU on enhanced data protection of personal data of all data subjects in the EU; and the concern to improve cyber security and enforcement across the Union. This is significant to the ICTS-Legal project because under the reform package, EU data subjects are generally provided with more information about, and more control, over their personal

[5] Johnson v. Microsoft Corp. 2008 WL 803124 W.D. Wash. Mar. 21, (2008) where US District Court Judge Richard Jones stated that "[I]n order for 'personally identifiable information' to be personally identifiable, it must identify a person. But an IP address identifies a computer."

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46EC at http://data.europa.eu/eli/reg/2016/679/oj.

[7] See, "Proposal for a Regulation Of The European Parliament And Of The Council On The Protection Of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf .

[8] Recital (171) of the GDPR explains that Directive 95/46/EC is repealed by this Regulation and states that "[P]rocessing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed."

[9] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. On 8 April 2016, the European Council adopted the GDPR and the DPDPC and on 14 April 2016, the GDPR and DPDPC were adopted by the European Parliament. Both instruments were published in the Official Journal of the EU on 4 May 2016, and came into effect 20 days after that date on 24 May 2016.

[11] Article 1(1).

[12] Article 1 (2).

data. The increased focus on cyber security is also relevant to the public interest argument advanced later in this article to justify the business to business sharing of cyber threat information. It is also significant to the ICTS-Legal project that the GDPR adds to, and builds on, the 1995 Directive but adds some significant new elements.

In most respects, the GDPR does not substantively change the data protection requirements from those of its predecessor, the 1995 Directive. This is important because data protection regimes outside the EU are currently based on the 1995 Directive, including its human rights foundations based on the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (in particular, Article 8 of the ECHR, which sets out the right to respect for private and family life).[13] This is the case even in countries like Australia for example, which do not have a formal national human rights regime established under its Constitution or through regional treaty, but which have 'imported' human rights concepts including balancing the rights of a data subject with public interest considerations, as a consequence of basing its data protection legislation on the EU model.

While it was anticipated that many countries would have legislation based on the EU model, the extent of adoption has been an unexpected finding of ICTS-Legal project. As expected, this is the case in Australia, and New Zealand, but it is also the case in Canada, Singapore, India, Malaysia, and Japan, for example.[14] The reasons are pragmatic. The EU has required that countries wishing to do business with the EU have similar data protection standards and the EU data protection requirements provided a comparatively early model. Australia for example, was one of the first nations outside Europe to implement data protection legislation based on the EU model and over time Australia has updated its Privacy Act 1988 (Cth) to align with EU requirements in order to facilitate business with the EU. It can be expected that the EU will continue to set the standard for data protection, and that the changes in the GDPR will continue to inform law reform outside Europe.

## 4. Major changes made by the GDPR and their relevance to the ICTS-Legal project

### 4.1. *Expanded extraterritorial reach*

A particular change introduced by the GDPR, however, is the expanded extraterritorial reach of the new Regulation and its potential to apply to businesses outside the EU, including to businesses in the US. Whereas the 1995 Directive applied to organizations based outside Europe when they did business in the EU, the GDPR applies to organizations processing personal data of EU data subjects[15] regardless of the organization's geographical base and area of operation under Article 3.[16] The GDPR applies to all businesses including companies incorporated in the US, which share cyber threat intelligence if that sharing is considered to be processing personal data of an EU subject.

Chapter V covers transfer of personal data to third countries or international organisations. If the personal data of an EU subject is transferred to a country outside the EU, i.e. to "a third country," the Articles in this Chapter apply. Article 44 provides that any transfer of personal data undergoing processing or intended for processing after transfer to a third country or to an international organisation, is subject to the GDPR. The controller and processor, "including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation", must comply with the conditions laid down in Chapter V. The Article specifically states that "[A]ll provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

The most likely scenario in the context of the ICTS-Legal project is that cyber threat data will be transferred to a business in the US. The key provisions, which apply to a US business in this situation, are Article 45[17] that deals with transfers on

[13] Formally, the Convention for the Protection of Human Rights and Fundamental Freedoms, which was signed by all Council of Europe member states in 1950 and became effective in 1953 (at http://www.echr.coe.int/Documents/Convention_ENG.pdf).

[14] While the legislation in Japan is a simplified version, which has a more limited application, the Japanese data protection legislation is nevertheless clearly modelled on the EU 1995 Directive.

[15] Under the GDPR, an EU data subject is a data subject in the EU.

[16] Article 3 states:"1. *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*2. This Regulation applies to the processing of personal data of data subjects who are in the Union *by a controller or processor not established in the Union, where the processing activities are related to:*(a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;* or(b) the monitoring of their behaviour as far as their behaviour takes place within the Union." (Our emphasis) The rationale is explained in the GDPR in Recital (101): "Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor."

[17] Article 45 provides that:"(1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.(2) When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national

the basis of an adequacy decision, and Article 46 which covers transfers that are subject to appropriate safeguards and binding corporate rules in Article 47. As to transfers with appropriate safeguards, the most significant development is the invalidation of the EU/US Safe Harbor Framework[18] under the 1995 Directive and its replacement with the EU/US Privacy Shield on 1 August 2016.[19] This was the result of the decision of the Court of Justice of the European Union (CJEU) in *Schrems v Data Protection Commissioner*[20] in October 2015. Schrems brought the action against the Irish data protection authority regarding his concerns about the transfer of his Facebook data from Ireland to the US. The decision largely turned on the finding that the protections provided under the framework did not meet the EU standards laid out in Directive 1995 read in the light of the Charter of Fundamental rights of the EU (the Charter, which became legally binding in 2009),[21] in particular because the principles of the safe harbor framework did not provide adequate independent oversight and redress for EU data subjects.

On 3 February 2016, the EU and US agreed in principal to a new framework to replace safe harbour and following months of negotiation and revision, the EU-US Privacy Shield was signed on July 12th, 2016. A U.S. company that wants to handle the personal data of an EU citizen can commit to the Privacy Shield Framework and is then obligated to follow it. As the agreement currently stands, the U.S. Department of Commerce (DOC) will monitor compliance and the US Federal Trade Commission (FTC) is responsible for enforcement. A key feature of the agreement is a guarantee by the US Director of National Intelligence (DNI) that the U.S. government will use EU personal data only for purposes that are necessary and proportionate for national security. Another key feature is the appointment of a data privacy ombudsman within the US State Department as the first point of contact for EU citizens for complaints in relation to how their data is processed under the framework. US companies are to comply with mandatory deadlines for dealing with individual complaints. EU individuals will also have access to alternative dispute resolution. Additionally, the Member States' Data Protection Authorities (DPAs) will have the ability to refer complaints directly to the DOC and FTC. The Privacy Shield arrangements will be reviewed annually to ensure that they meet EU privacy standards.[22]

The new agreement signed in July 2016 attempts to address many of the concerns expressed by the highly influential EU Article 29 Working Party (Working Party) in April 2016. The Working Party assessed the first proposed framework "in light of the applicable EU data protection legal framework as set out in Directive 95/46/EC, as well as the fundamental rights to private life and data protection as enshrined in Article 8 of the ECHR, and Articles 7 and 8 of the Charter."[23] The new agreement incorporates many of the Article 29 Working Party's suggestions from April 13, 2016 but there are still concerns about the effectiveness of the current framework and there are indications that it could be the subject of a challenge. Whether or not that occurs it seems that the practical, if not legal, effect will be that the EU data protection standards will eventually apply across the Atlantic. This would bring U.S. corporations which process the personal data of EU citizens into line with

security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

[18] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215/7).

[19] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207/1).

[20] *Maximillian Schrems v. Data Protection Commissioner* (Case C-362/14, 6 October 2015).

[21] Charter of Fundamental Rights of the EU (OJ 2012 C 326/391), at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:12012P/TXT.

[22] See, European Commission – Press release, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016 at http://europa.eu/rapid/press-release_IP-16-433_en.htm. The Privacy Shield agreements and documents are available with this press release. See also Recital (104) of the GDPR which sets out the basis EU concern regarding data transfers: "In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."

[23] Article 29 Working Party, Statement of The Article 29 Working Party on The Opinion on The EU-U.S. Privacy Shield, Brussels. April 13, 2016 at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf.

most other countries, which the ICTS project has found use the EU model as the basis of their data protection legislation.

### 4.2. *Uniform regulation and enhanced enforcement and penalties*

As mentioned, the other key changes made by the GDPR are that data protection regulation will be uniform in application across the EU. The reform is designed on the basis of "one EU single market, one law" and establishes a single set of directly-applicable rules to make it simpler and more cost effective to do business in the EU as companies will only have to deal with one legal regime under the GDPR. This is intended to provide more efficiency and legal certainty. The GDPR adds the new requirement that the national supervisory authority must be notified of serious data breaches; usually within 24 hours[24] and that the company suffering the breach must usually notify the data subject. Article 32 of the GDPR requires that "[w]hen the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject", the company "must communicate the personal data breach to the data subject without undue delay". However, the GDPR takes into account specific circumstances including the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.[25]

Article 77 of the new Regulation states that the supervisory authority in an EU member state can initiate legal proceedings when data protection regulation has been violated. Individuals may lodge complaints about violations to the supervisory authority.[26] Article 78 of the GDPR provides that an individual has the right to an effective judicial remedy against a supervisory authority and that proceedings against a supervisory authority can be before the courts of the Member State where the supervisory authority is established.

Most significantly, in the context of the ICTS project, Article 79 of the GDPR provides a data subject with the right to an effective judicial remedy against a controller[27] or processor.[28] Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence.[29] Like Article 23 of the 1995 Directive, Article 82 of the GDPR provides a broader right to "any person" who has suffered damage; Article 82 however now specifically includes "non-material damage." Article 82 provides that "*any person* who has suffered *material or non-material damage* as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered" (our emphasis). Significant new penalties are also provided in the GDPR. Most member State data protection authorities[30] can fine companies that do not comply with EU requirements up to 10,000,000 Euro for an administrative fine or, in the case of a breach of an undertaking[31], 2% of global annual turnover, whichever is greater.[32] In determining the fine, Article 83 (2) states that the supervisory authority is to take into account the nature, gravity, and duration of the breach and the intentional or negligent character of the infringement. The penalties specified in Article 83 apply to a breach of Article 6, which covers lawful processing of personal information.

### 4.3. *Pseudonymisation*

Another major change relevant to the ICTS project is that the GDPR encourages 'pseudonymisation'[33] as part of protecting individual privacy. 'Pseudonymisation' is defined in Article 4 (5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." This emphasis is troubling from both a technical and a legal perspective if it is taken to suggest that pseudonymised data is no longer personal data under EU data protection law, because it is well known that anonymization can be easily defeated so that pseudonymisation does not protect an individual from being directly or indirectly identified.[34] Even if totally random tokens are used, a

[24] See Article 31 of the New Regulation.
[25] See Recital (88).
[26] Article 4 (21) defines "supervisory authority" as "an independent public authority which is established by a Member State pursuant to Article 51". Article 4 (22) defines "supervisory authority concerned" to mean "a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority."
[27] Article 4 (7) of the GDPR defines "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."
[28] Article 4 (8) states that "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."
[29] Article 79(2).
[30] Estonia and Denmark are exempted.
[31] Recital (150) of the GDPR states that: "Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes." Undertaking is not defined in the TFEU, i.e. the Treaty on the Functioning of the European Union, but the CJEU has stated that "the concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed." See, Case 41/90, *Höfner and Elsner v Macrotron*, para 21. Any activity consisting of offering goods and services on a given market is economic activity. See case C-180/98 *Pavel Pavlov and Others v Stichting Pensioenfonds Medische Specialisten*.
[32] Article 83 (4) and (5).
[33] Encryption is also encouraged.
[34] For a technical discussion see, de Montjoye Y. A., Radaelli L., Singh V. K., Pentland A. S., "Unique in the Shopping Mall: On the Re-identifiability of Credit Card Metadata," Science, 347 (6221), 536–539.

small number of tokens uniquely identify an individual.[35] It is not clear therefore if this reform package is being forward-looking in anticipation of development and adoption of new technologies, such as multi-party encryption,[36] or is failing to recognize the present fallibilities of pseudonymisation. However, the stated reason for encouraging pseudonymisation is to harness the economic and social benefits of big data,[37] as well as reduce risks for data subjects (Recital 28 of the GDPR).

In any event, while encryption is used for cyber threat intelligence sharing, pseudonymization is not relevant to achieving that outcome. For example, in the case of phishing emails, to be of use, most of the interesting data from the email needs to be shared. If it is a phishing email, it will, almost by definition, contain someone's personal information. In this situation, anonymization and pseudonymisation can render the cyber threat intelligence virtually useless. One technique is to share hashes of the information, so only when a match occurs would there be a leak of information. Current research at Georgetown is working on how to 'share without sharing,' this information.[38]

## 5. Substantive similarities of the GDPR to the 1995 Directive and their relevance to sharing IP addresses as threat intelligence under the ICTS-Legal project

### 5.1. *Are IP addresses personal data?*

Like the 1995 Directive, the GDPR applies to the processing of personal data of an EU data subject and personal data is defined simply and broadly. In Article 4(1) of the GDPR we find the definition of personal data as "any information relating to a data subject".[39] The GDPR then defines "data subject" as "an identified or identifiable natural person". In turn, "an identifiable natural person" means one "who can be identified, directly or indirectly, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." We find further clarification in the non-binding but influential Recitals of the GDPR, in particular Recital 26: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. . ."

Such definitions are similar but broader than the ones for such terms in the 1995 Directive. For example, the GDPR retains the direct and indirect identification terminology that it employs in the 1995 Directive (Article 2), and includes similar wording to Recital 26 of the Directive and its reference to "means likely reasonably to be used" by any natural or legal person (such as a corporation) as relevant to the assessment of whether an individual is identifiable from data in combination with other information. The new definition also goes beyond the listing of 'identification number' as an indirect identifier example as specified in the 1995 Directive, to also include "location data" and "online identifier."

Whether information is "personal data" under the GDPR depends on the circumstances as to whether it can be used to identify an EU data subject (either now, or potentially in the future if it were combined with other information that could be accessed). Consider, for example, the name of a customer that may need to be disclosed as part of cyber-threat intelligence sharing. Unless it is unusual, name alone may not identify an individual. Even when name, date of birth and gender are combined, that may not be sufficient to identify an individual directly or indirectly so that they fall within the definition of "data subject" in the GDPR.[40] Of course, the more detail provided in the data about a person – or the addition of other information to the data – the greater the likelihood that the data will be capable of being used to identify a data subject and be considered personal data under the GDPR.[41] In *Lindqvist v Sweden*[42] where the CJEU provided guidance about what constitutes personal data under the 1995 Directive, the Court stated that personal information ". . . undoubtedly covers the name

For the seminal legal article, see Ohm, P. "Broken Promises of Privacy: Responding To The Surprising Failure Of Anonymization" 57 UCLA Law Review 1701 (2010).

[35] Hind, J. R., Mathewson II, J.M., Peters, M. L., "Identification and tracking of persons using RFID-tagged items in store environments," US Patent 7,976,441, Filed 3 May 2001, Issued 11 July 2006.

[36] Gentry, C. Fully homomorphic encryption using ideal lattices. STOC. M. Mitzenmacher ed. ACM, 2009, 169–178.

[37] See European Commission, "Questions and Answers – Data protection reform", Fact Sheet, 21 December 2015 at http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm, where the Commission states, "[T]he Regulation promotes techniques such as anonymisation (removing personally identifiable information where it is not needed), pseudonymisation (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data. This will encourage the use of 'big data' analytics, which can done using anonymised or pseudonymised data."

[38] For example, using homomorphic encryption techniques and unique implementation architectures, even the match would not be noted by any single piece of network equipment. See https://s2erc.georgetown.edu/projects/sps.

[39] To be considered personal data as defined, the data and information must relate to a living person. For more information on interpreting this 'relating to' criterion, see Article 29 Working Group, Opinion 04/2007 on the concept of personal data at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf. The Working Party provides guidance on how this criterion might be established with reference to one of three elements that should be present: 'content' (the information is given about a particular person), 'purpose' (the data is used, or is likely to be used, to evaluate, treat in a certain way or influence the status or behaviour of an individual), or 'result' (the use of the data is likely to have an impact on a person's rights and interests).

[40] See "*Handbook on European Data Protection Law*", European Union Agency for Fundamental Rights, 2014 Council of Europe, 2014, p 39–41 at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. See also, ECtHR, *Odièvre v. France* [GC], No. 42326/98, 13 February 2003; and ECtHR, *Godelli v. Italy*, No. 33783/09, 25 September 2012.

[41] See Anmerkung zu LG Berlin, Urt. v. 31.1.12013 – 57 S 87/08: Personenbezug von IP Adressen, ZD 2013, 618 - zuerst erschienen in ZD 2013, 625 at http://www.retosphere.de/files/2013-12-Mantz, AnmLGBerlin-IP-Adressen,ZD_web.pdf.

[42] [2003] ECRI-12971, ¶ 24.

of a person in conjunction with telephone coordinates or information about his working conditions or hobbies."[43]

While that type of information is not expected to be shared between businesses, the key question for the ICTS-Legal project is whether IP addresses are personal data as defined in the GDPR. Although the GDPR defines personal data in similar terms to the 1995 Directive, Recital (24) of the GDPR adds a new perspective which was not included in the 1995 Directive and specifically includes IP addresses: "Individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers or other identifiers such as Radio Frequency Identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them."[44]

As mentioned in the introduction to this article, one of the legal arguments successfully used in the US, Finland, and France in determining whether an IP address is personal data, is that IP addresses are not always static (that is, that can change in respect of the internet-connecting device they are assigned to). While this is often so, according to research by the Fraunhofer Institute for Secure Information Technology on Web tracking, 72 percent of Internet users have the same IP address for two weeks. However, many ISPs in Germany for example, change a user's IP address every 24 hours.[45] However, even when an IP address is changed, when it is combined with other information associated with it, an individual may become identifiable so as to bring the IP address within the definition of "personal data" under the GDPR.[46] As such, its processing would become subject to the full gamut of the new rules in the GDPR when they become effective (as it would do now under the 1995 Directive).

One mitigating circumstance is that while an IP address may identify the account holder paying an internet service provider (ISP) for internet access, it does not necessarily identify the person using the internet-connecting device to access the Web at the time that the IP address was recorded. While the accuracy of an identification decision is more likely when an IP address is combined with other information associated with it, it is also well known that IP addresses can be hidden and that Internet activity can be routed and re-routed using a number of IP addresses to make identification of the user difficult. Multiple devices can also appear to share IP addresses, either because they are part of a shared hosting web server environment or because a network address translator or proxy server acts as an intermediary. The real originating IP addresses might be hidden from the server receiving a request. A common practice is to have a network address translator hide a large number of IP addresses in a private network. Only the "outside" interface(s) of the network address translator need to have Internet-routable addresses.[47]

Whether an IP address can identify a data subject is central to determining whether an IP address is personal data for the purposes of the GDPR and its predecessor the 1995 Directive (the processing of which makes it subject to their rules). There is currently little CJEU or member state case law directly on this point and none relating to IP addresses in the context of cyber-threat intelligence sharing. In *EMI & Ors v Eircom Ltd*[48], the High Court of Ireland held that IP addresses do not amount to personal data under the 1995 Directive, though it should be noted that the case concerned illegal downloading and copyright infringement. By contrast, the French Constitutional Court has concluded that the collection of IP addresses allowing for the identification of a person did amount to the processing of personal data but like the decision of the Irish court, this decision was reached in different context, in relation to the constitutional standing of the Hadopi law.[49] Similarly, in *Scarlet v Sabam*[50] the CJEU held, as a secondary issue in relation to enforcement of intellectual property rights, that the IP addresses were personal data because users could be directly identified without further explanation.

In Germany, however there is a recent decision on point in relation to which key questions of EU law are now being considered by the CJEU. The Landgericht Berlin, a German regional court, held in 2014 that the retention of IP addresses on official German government websites longer than technically necessary, and without consent of the data subjects, did not infringe data protection law. Patrick Breyer, a German human rights activist, argued that German government violated his data protection rights by storing his IP address longer than necessary. When Internet users visit German government sites, their IP addresses are stored with the time when they visited a particular page. The government stores this data in a log file, to track and prosecute unlawful hacking, according to the German Federal Court. Breyer argued that this is constituted unnecessary "Internet stalking." Breyer wants the government to refrain from storing his IP address longer than the time he is active on the website. He argued that because the address can be linked to him and could be used to identify him when combined with other information, it is personal data, as defined under the 1995 Directive, which as described is drafted in similar

[43] See also, *Von Hannover v Germany* (2004) 40 EHRR 1, ¶ 50. Note also that in *Roberson v Wakefield Metropolitan District Council and Another*,[1] in considering name and address under the right to private life under Article 8 of the ECHR, the Queens Bench in the United Kingdom added that instead of focusing on the information, consideration should also be given to known and anticipated use of the information.

[44] Recital (30).

[45] Fraunhofer Institute for Secure Information Technology, Web-Tracking-Report 2014, page 44 with reference to Casado, Martin; Freedman, Michael J.: Peering Through the Shroud: The Effect of Edge Opacity on IP-based Client Identification. In: 4th USENIX/ACM Symposium on Networked Systems Design and Implementation, Proceedings, 2007, 173–186.

[46] In particular, ISPs may hold other information that, in combination with IP address data, may enable the identification of an account holder (even when the IP address is dynamic). To note in this context, moreover, some jurisdictions have legislated to require that ISPs retain metadata that could facilitate the mapping of an IP address to a particular subscriber for a defined period of time.

[47] Adapted from Comer, D "Internetworking with TCP/IP: Principles, Protocols, and Architectures" 4th ed (2000), 394.

[48] [2010] IEHC 108.

[49] Décision n° 2009-580 DC du 10 juin 2009.

[50] Case C-70/10, 24 November 2011.

terms to the GDPR.[51] Breyer argued therefore that for the recording and storage of the IP addresses to be lawful processing, his explicit consent was required.[52] The Landgericht Berlin dismissed the action, holding that an IP address itself is not personal data in the sense that it does not directly identify a person. The court did state, however, that an IP address might still be considered personal data with the knowledge of additional identifying information, however, that information was held by a third party (the ISP) and not the government.[53]

On 28 October 2014 the Bundesgerichtshof, the German Federal Court of Justice, was to hear the Breyer case on appeal but it referred two preliminary questions of law to the CJEU. The first question is directly relevant to the ICTS project, whereas the second question relates to a possible conflict of national legislation with the 1995 Directive.[54] The first question is (to paraphrase): Do dynamic IP addresses qualify as "personal data" under the 1995 Directive in cases where only a third person, but not the recipient of the IP address data itself, has access to further information required in order to identify the user of that address? The German Federal Court of Justice stated that in order to grant the injunction sought by Breyer, his dynamic IP addresses must be personal data under Article 2 of the 1995 Directive but that this is questionable where a third party (an ISP) held further information that was not immediately accessible by the recipient (i.e. the German government authority) that might enable Breyer to be identified.

The CJEU considered the questions on February 25, 2016[55] and the decision of the CJEU was delivered on 19 October 2016.[56] The CJEU interpreted "identifiable" broadly to find that dynamic IP addresses are personal data if website operators have "legal means" of enabling the identification of the person associated with the IP address. The CJEU based this finding on the observation that in the event of a cyberattack, German law seems to provide that website operators contact the appropriate authorities, who could obtain information from ISPs to identify the person associated with an IP address. The full implications of the CJEU's finding on this point are unclear however. The Breyer case concerned the definition of personal data in the 1995 Directive. Essentially that definition is the same as the definition in the GDPR so it is likely that the decision of the CJEU in Breyer will be applied to the GDPR when it comes into operation in May 2018. As discussed, the GDPR adds to the 1995 Directive by providing that an identifier can contain name, location data, online identifier and genetic data; and that data of a deceased person or of a legal person such as a corporation, cannot be personal data. Most significantly, however, the GDPR encourages pseudonymization. As discussed in this article, pseudonymization, like anonymization, was troubling from both a technical and a legal perspective even before the CJEU finding in Breyer because it is well known that

[51] See Recital 26 of the GDPR like Recital 26 of the 1995 Directive also suggests that the prospect of identification may be assessed by "all the means reasonably likely to be used . . . either by the controller or by any person". However, what that means exactly in the context of the ICTS project is as yet unclear.

[52] Essers L, "Is your IP address really yours? EU court to decide the question" IDG News Service. Oct 29, 2014 at http://www.pcworld.com/article/2840592/europes-top-court-to-rule-on-whether-ip-addresses-are-personal-data.html.

[53] See, Nr. 152/2014, "Vorlage an den EuGH in Sachen 'Speicherung von dynamischen IP-Adressen'" at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=69184&pos=0&anz=152 [23]. See also, Case C-213/15 P and Case T-188/12 *Patrick Breyer v Commission* ECLI:EU:T:2015:124. According to one German legal commentator. "[t]he question whether a dynamic IP address qualifies as 'personal data' even if it alone does not enable the recipient to identify the user is indeed one of the most debated topics in German and European data protection law. While the German Data Protection Authorities classify IP addresses per se as personal data, the majority of German courts and legal scholars regard IP addresses as personal data only if the recipient has access to additional information that allows the identification of the user." See Munz M, "Are Dynamic IP Addresses Personal Data? German Federal Court of Justice seeks Advice from European Court of Justice" December 9. 2014 at http://www.whitecase.com/publications/article/are-dynamic-ip-addresses-personal-data-german-federal-court-justice-seeks.

[54] The second question is: Is Section 15 of the German Telemedia Act which permits the telemedia service provider to collect and use the personal data of a user only to the extent necessary to provide the service and for invoicing purposes consistent with the 1995 Directive? According to Section 12 of the German Telemedia Act (the Act), a telemedia service provider may only collect and use IP addresses (assuming they are as personal data) without the data subject's prior consent to the extent that the Act or another statutory provision referring expressly to the Act, permits it. In the Breyer case, the reason for storing the IP addresses was to maintain the security and functionality of the government websites. The German Federal Court of Justice doubted that this is sufficient for permission under Section 15 of the Act. For systematic reasons, the Court assumed that under section 15, personal data can only be stored beyond the duration of the actual use of the service for invoicing purposes, otherwise the data needs to be deleted afterwards. However, the 1995 Directive might dictate a broader interpretation of section 15. In that event the national TMA might be in conflict with the 1995 Directive under which a service provider may collect and use personal data without Breyer's consent but only as necessary. However, the Court commented that the purpose of ensuring the general functionality of the telemedia service may not justify the storing of the data beyond the duration of the particular user activity. Adapted from Munz M, "Are Dynamic IP Addresses Personal Data? German Federal Court of Justice seeks Advice from European Court of Justice" December 9. 2014 at http://www.whitecase.com/publications/article/are-dynamic-ip-addresses-personal-data-german-federal-court-justice-seeks.

[55] To note, Advocate General (AG) Campos Sánchez-Bordona did provide his non-binding but highly influential Opinion on the case to the CJEU on 12 May 2016 (ECLI:EU:C:2016:339). In that Opinion, he set out his reasons for finding that static IP addresses are always personal data, whereas, he believes that a dynamic IP may be deemed personal data, however, he notes a strict interpretation of "means likely reasonably to be used . . .by any other person" in Recital 26 of the 1995 Directive in this context. This should be interpreted, he says, as "means likely reasonably to be used" by certain third parties, who may reasonably be approached by a controller seeking additional data for identification purposes; typically ISPs. In other words, on the facts of this case, he answers affirmatively, that dynamic IP addresses are personal data in respect of a user who has accessed a website provider's website (to the extent that an ISP has other information which, when linked to the dynamic IP address, facilitates identification of that user).

[56] Mr Patrick Breyer and the Bundesrepublik Deutschland (Federal Republic of Germany) C-582/14 Judgment 19 October 2016 at http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-582/14.

both pseudonymization and anonymization can be easily defeated. The question now is what exactly are the "legal means" referred to by the CJEU in Breyer. While the Court has broadly interpreted "identifiable", by contrast, "legal means" may be restrictively interpreted to the cyber attack circumstances and legal means open to authorities as observed by the CJEU in Breyer. In any event, the decision raises significant new legal doubts about both pseudonymization and anonymization.

The decision of the CJEU in Breyer has immediate implications for the sharing of threat Intelligence under the ICTS-Legal Project in that both static and dynamic IP addresses are now generally presumed to be personal data under the 1995 Directive and by extension, under the GDPR. However, whether an IP address, particularly a dynamic address, is considered personal data will still depend on the particular circumstances of each situation (such as what rules apply in the country at issue around the retention of metadata by ISPs and the duration of any retention obligations). However, in light of the CJEU finding in the Breyer case, it may be that the data controller of a business sharing the IP address as cyber threat intelligence, is sharing personal data, even if that data controller does not have access to further information that enables identification of the data subject. It can be assumed (for example, because domestic law requires it) that the ISPs have retained this information. To be lawful, the sharing (indeed, any processing of that data) must then be justified under one of the legal bases for processing specified in Article 6 of the GDPR from 25 May 2018 onwards (or, under Article 7 of the 1995 Directive before that date).

The first legal basis for justifying personal data processing is where "the data subject has given consent to the processing of his or her personal data for one or more specific purposes." The consent of a data subject who is a customer for example may be obtained as part of initially signing up for service. In future, that consent must comply with the enhanced requirements of Article 7[57] of the GDPR and the onus is on the data controller to demonstrate the data subject's consent. While this consent could be requested by a business as part of its routine sign-up procedures, consent may be withdrawn at any time under Article 7 (3). In any event, it is unlikely to cover the type of threat intelligence that needs to be shared. The IP address user is more likely to be that of an independent bad actor rather than a person with whom the business has an existing relationship.

In the absence of the explicit consent of the data subject, there are two legal bases in Article 6 that could apply in the context of ICTS project. First, where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Article 6(1)(f)); and secondly, where the processing is necessary for the performance of a task carried out in the public interest (Article 6(1)(e)).

### 5.2. *Is sharing IP addresses processing necessary for legitimate interests?*

Like the 1995 Directive, the GDPR defines "processing" widely as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[58] This definition covers business-to-business sharing, including the automated sharing being developed as part of the ICTS project.

Article 5 of the GDPR sets out principles relating to processing of personal data, which underpin rights of a data subject under the regulation. Like the 1995 Directive, it requires that the data must be accurate, kept up to date, and that "every reasonable step must be taken to ensure that data which are inaccurate or incomplete . . . are erased or rectified". The data must not be kept in a form "which permits identification of data subjects for any longer than necessary". Safeguards apply to personal data stored for longer periods for historical, statistical or scientific use.[59] Like the 1995 Directive, the GDPR also requires that personal data collected must be adequate and relevant, and "limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data."[60] Similarly, "personal data" must be collected "fairly and lawfully" for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. However, the GDPR specifically adds the requirement that the data be processed "in a transparent manner in relation to the data subject."[61]

As mentioned, Article 6 of the GDPR sets out the bases under which the processing of personal data is lawful (at least one basis must be found for every processing activity). The first basis is where "the data subject has given consent to the processing of his or her personal data for one or more specific purposes." However, even in the absence of consent, the legitimate interests of the data controller and/or the business/es with which the data shared, can outweigh the rights of the data subject. Article 6(1)(f) of the GDPR (like Article 7 (f) of the 1995 Directive)[62] specifically includes the situation when

[57] The Article requires that "(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration, which constitutes an infringement of this Regulation, shall not be binding.3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

[58] Article 4 (3) and Article 4 (8).

[59] Article 6(a)–(e) of the 1995 Directive and Article 5(c) of the GDPR.

[60] Article 6(a)–(e) of the 1995 Directive and Article 5(c) of the GDPR.

[61] Article 5 of the New Regulation; Article 6 of the 1995 Directive.

[62] Article 7(f) of the 1995 Directive states: "processing is necessary for the purposes of the legitimate interests pursued by the

"processing is necessary for the purposes of *the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject* which require protection of personal data, in particular where the data subject is a child." (our emphasis)

Specific reference is made to ground (f) of Article 6(1) in both Article 13 and Article 14 of the GDPR, which cover notification of a data subject when personal data is obtained. Article 13 covers the information to be provided where the personal data are collected from the data subject, while Article 14 covers personal data that has not been obtained from the data subject.

Article 13 requires the controller shall, at the time when personal data are obtained, provide the data subject with all of the information specified in Article 13 (1) which includes inter alia the identity of the data controller and the recipients to whom the data will be transferred and "the purposes of the processing for which the personal data are intended as well as the legal basis for the processing."[63] Article 14, which is likely to be most applicable to the ICTS project, requires basically the same notification but also includes notification of the period for which the data will be stored. Article 14 (2) requires that the data controller notify the data subject of the legitimate interests pursued by the controller or by a third party. Article 14 (3) requires that the controller provide the information to the data subject "(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed." Of course, these requirements substantially undermine the value and purpose of sharing threat intelligence. Article 14 (5) sets out the circumstances in which the notification is not required but none of the specified grounds[64] are applicable to the businesses which will share intelligence in the context of the ICTS project, especially considering many will be foreign companies incorporated in jurisdictions outside the EU. This is a major impediment to the international sharing of cyber threat intelligence and as such it is a significant flaw in the GDPR, particularly considering the increased focus on cyber security in the EU reform package.[65]

While it is important that this type of information transfer not be disproportionate to its purpose, and that it only be done as necessary using the minimal amount of personal data, Article 6 of the GDPR and its predecessor Article 7 of the 1995 Directive, require that assessment. The factors developed by member states to be considered in this balance test, as identified by the Working Party in its 2014 Opinion on legitimate interest in the context of Article 7 of the 1995 Directive,[66] are "(a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects."[67] The Working Party prepared the Opinion in 2014 because it recognized the need for a more consistent and harmonized approach across Europe in interpreting and applying Article 7 of the 1995 Directive; and to prepare for the new GDPR, which will apply shortly.[68]

Recital (49) of the GDPR covers data processing strictly necessary and proportionate for the purposes of ensuring network and information security, which the recital describes as "the ability of a network or an information system to resist, at a

controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)".

[63] Article 6(1) (c).

[64] See Article 14 (5) which states that: "Paragraphs 1 to 4 shall not apply where and insofar as:(a) the data subject already has the information;(b) the provision of such information proves impossible or would involve a disproportionate effort, in *particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,* subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;(c) obtaining or disclosure is *expressly laid down* by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or(d) where the personal data must remain confidential subject *to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy*." (our emphasis)

[65] While this interpretation seems counter-intuitive, the mere doubt as to the notification requirements is sufficient to impede sharing of threat intelligence.

[66] Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[67] Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 33 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[68] The Working Party observes that: "Studies conducted by the Commission in the framework of the review of the Directive6 as well as cooperation and exchange of views between national data protection authorities ('DPAs') have shown a lack of harmonised interpretation of Article 7(f) of the Directive, which has led to divergent applications in the Member States. In particular, although a true balancing test is required to be performed in several Member States, Article 7(f) is sometimes incorrectly seen as an 'open door' to legitimise any data processing which does not fit in one of the other legal grounds. The lack of a consistent approach may result in lack of legal certainty and predictability, may weaken the position of data subjects and may also impose unnecessary regulatory burdens on businesses and other organisations operating across borders. Such inconsistencies have already led to litigation before the Court of Justice of the European Union ('ECJ'). It is therefore particularly timely, as work towards a new general Data Protection Regulation continues, that the sixth ground for processing (referring to 'legitimate interests') and its relationship with the other grounds for processing, be more clearly understood. In particular, the fact that fundamental rights of data subjects are at stake, entails that the application of all six grounds should – duly and equally – take into account the respect of these rights. Article 7(f) should not become an easy way out from compliance with data protection law." (footnotes in text deleted). See Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 5 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), *by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned*. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems." (Our emphasis)

Recital (49) is sufficiently broad to cover businesses. Taking into account the balance test, the international sharing of cyber-threat intelligence between businesses would certainly be considered processing necessary in the legitimate interests of the data controller and/or a third party under Article 7(f) of the 1995 Directive and Article 6(1)(f) of the GDPR. This view is supported by the Opinion of the Working Group, which is highly influential. The Working Group specifically acknowledges that public interest can be invoked to establish legitimate interest:

> "In some cases, the controller may wish to invoke the public interest or the interest of the wider community (whether or not this is provided for in national laws or regulations) . . . It can also be the case that a private business interest of a company coincides with a public interest to some degree. This may happen, for example, with regard to combatting financial fraud or other fraudulent use of services. A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the customers of the company, taxpayers, and the public at large also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur. *In general, the fact that a controller acts not only in its own legitimate (e.g. business) interest, but also in the interests of the wider community, can give more 'weight' to that interest*. The more compelling the public interest or the interest of the wider community, and the more clearly acknowledged and expected it is in the community and by data subjects that the controller can take action and process data in pursuit of these interests, the more heavily this legitimate interest weighs in the balance." (footnote in text deleted) (our emphasis)[69]

The Working Party also refers to the legitimate interest of third parties under Article 7 in this context. In a statement, which is particularly relevant to the business receiving cyber threat intelligence, the Working Party observes that: "This is the case where the controller – sometimes encouraged by public authorities – is pursuing an interest that corresponds with a general public interest or a third party's interest. This may include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as money laundering, child grooming, or illegal file sharing online. In these situations, however, it is particularly important to ensure that the limits of Article 7(f) are fully respected."[70] (our emphasis)

Taking account of, and balancing, the rights of the data subject as required by Article 6 of the GDPR so they are not subject to disproportionate interference, the sharing of IP addresses as threat information would be both necessary and proportionate. On this basis, the international sharing of cyber-threat intelligence between businesses is likely to be processing necessary in the legitimate interests of the data controller and/or a third party under Article 6(1)(f) of the GDPR. However, the notification requirements of Article 14 make reliance on that ground untenable.

### 5.3. *Is the sharing of IP addresses "processing necessary in the public interest"?*

Article 6(1)(e) of the GDPR, and its equivalent in the 1995 Directive,[71] specifically includes the situation when "processing is *necessary* for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. . ." (our emphasis).[72] Unlike legitimate interest under Article 6(1)(f), Article 6(1)(e) is sensibly not included in either Article 13 or 14 regarding the need for prior notification to the data subject.

Article 6(3) requires that the basis for the processing referred to in (c) and (e) of paragraph 1 be laid down by (a) Union law; or (b) Member State law to which the controller is subject.

---

[69] The opinion goes on to state: "On the other hand, 'private enforcement' of the law should not be used to legitimise intrusive practices that would, were they carried out by a government organisation, be prohibited pursuant to the case law of the European Court of Human Rights on grounds that the activities of the public authority would interfere with the privacy of data subjects without meeting the stringent test under Article 8(2) of the ECHR." Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 35 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. The deleted footnote refers to Example 21: Smart metering data mined to detect fraudulent energy use on page 67 in the Working Party's Opinion 3/2013 on purpose limitation.

[70] Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 28–29 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[71] Article 6 (1) has slightly different wording: "*processing is necessary for the performance of a task carried out in the public interest* or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed."(Our emphasis)

[72] Other parts of Article 6(1) of the GDPR which are also of potential application to business-to-business sharing of cyber-threat intelligence are:"(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;(c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject."

Article 6(3) goes on to state: "The purpose of the processing shall be determined in that legal basis or, *as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest* or in the exercise of official authority vested in the controller" (our emphasis). On a literal interpretation, this part of the Article could be viewed as equivalent to establishing public interest as a justification for personal data processing in itself (without the need to find a legal basis in EU law for the processing, as a requirement to which the data controller is subject).

That interpretation is consistent with established human rights principles, which underpin the GDPR, particularly the individual rights to data protection and privacy under the EU (which is based upon the ECHR) that can be waived to overriding public interest. It is also consistent with the view of the Working Party. When discussing public interest, albeit in relation to Article 7 of the 1995 Directive, the Working Party stated "[i]n some cases, the controller may wish to invoke the public interest or the interest of the wider community (whether or not this is provided for in national laws or regulations)." The interpretation is also confirmed by Article 6(4) of the GDPR which states that: "Where the processing for a purpose other than that for which the personal data have been collected *is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)* (our emphasis),[73] the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

As mentioned above, the Charter[74] underpins the GDPR[75]. The first Recital of the GDPR provides that "[T]he protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her." The Charter sets out protection of personal data as a fundamental right under Article 8, and distinguishes it from the right to respect for private and family life under Article 7. Article 8(2) establishes the requirement for a legitimate basis for processing, providing that personal data must be processed 'on the basis of the consent of the person concerned or *some other legitimate basis laid down by law*' (our emphasis).[76] The public interest limitation is also evident in Article 52, which covers the scope and interpretation of rights, and principles set out in the Charter. Article 52(1) acknowledges a limitation on the exercise of the rights and freedoms recognized by the Charter and provides that they must meet the principle of proportionality, and "may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[77]

The purpose of automated sharing of IP addresses is system security. That threat intelligence assists businesses in system defense and protection and in minimizing the impact of an attack. Considering that purpose, certain types of processing in that regard may be deemed proportional and justified even if under the considerations set out in Article 6(4) of the GDPR, the processing is considered to be for a purpose other than that for which the personal data have been collected.

Public interest is not defined in the GDPR or other relevant EU instruments. Public interest is a broad and evolving concept that depends on the particular facts and circumstances of the data processing. Article 8 of the ECHR supports this view and provides examples of public interest considerations. As mentioned, the 1995 Directive is explicitly based on the ECHR,[78] as is the Charter, which has applied since 2009. The Charter is

[73] Article 23 provides that Union or Member State law which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12–22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12–22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard public interests. Article 23 lists national security, defence, pubic security as well as a number of other public interest grounds.

[74] Under Article 6(1) of the Treaty on the European Union, the Charter has "the same legal value as the Treaties." This has been the case since the Lisbon Treaty entered into force on 1 December 2009. At that time the Charter became legally binding on the EU institutions and on national governments, like the EU Treaties. The Charter strengthens the protection of fundamental rights "by making those rights more visible and more explicit for citizens." See, European Commission, "How the Charter became part of the EU Treaties" at http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm.

[75] The Charter applies when EU member countries adopt or apply a national law implementing an EU Directive or when they apply an EU Regulation directly.

[76] Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 8 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. As the Working Party points out, "[t]hese provisions reinforce both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data."

[77] This ties in which obligations of the data controller under the GDPR and the 1995 Directive regarding security of personal data. See for example Section 2 of the GDPR.

[78] See Recital (1) of the 1995 Directive.

consistent with the ECHR and Article 6 (3) of the Treaty of the EU provides that the fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States, "constitute general principles of the Union's law." Under Article 52 (3) of the Charter, moreover, in light of the fact that the Charter contains rights that stem from the ECHR, their meaning and scope are the same.

Unlike the Charter, the ECHR does not contain an Article specifically dealing with an individual right to data protection. Under the ECHR that right is part of the broader right to respect for private and family life, which is regarded as the general right to privacy.[79] Article 8 of the ECHR specifically requires that there be no interference with the exercise of this right "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[80] Considering the purpose under consideration is system security, "the protection of the rights and freedoms of others" is most relevant to the automated sharing of IP addresses as cyber-threat intelligence. In applying Article 8 (2) in the context of the 1995 Directive the European Court of Human Rights (ECtHR) in *Peck v United Kingdom*[81] for example, commented that "[i]n cases concerning the disclosure of personal data, the court has also recognised that a margin of appreciation should be left. . ..in striking a fair balance between the relevant conflicting public and private interests. However, this margin goes hand in hand with European supervision (*Funke v France*, judgment of February 23, 1993, Series A No.256-A, §55) and the scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference (*Z. v Finland*, judgment of February 25, 1997, Reports of judgments and Decisions 1997-I, §99)."[82]

The Working Party provides further guidance in its discussion of processing in the public interest: "For example, a charitable organisation may process personal data for purposes of medical research, or a non-profit organisation in order to raise awareness of government corruption. It can also be the case that a private business interest of a company coincides with a public interest to some degree. This may happen, for example, with regard to combatting financial fraud or other fraudulent use of services. A service provider may have a legitimate business interest in ensuring that its customers will not misuse the service (or will not be able to obtain services without payment), while at the same time, the customers of the company, taxpayers, and the public at large also have a legitimate interest in ensuring that fraudulent activities are discouraged and detected when they occur."[83]

On this view the sharing of IP addresses as cyber-threat intelligence, may clearly be justified and lawful on public interest grounds as long as the processing measures that surround this sharing are strictly necessary and proportionate to purpose: this includes any specifications affecting, not just the nature of the automated processing, but also regarding data retention and further usage.

## 6. Conclusion

The ICTS project uses cross-discipline collaboration to explore international norms for the sharing of data, as well as the technical means to enable automated sharing of threat intelligence. Automated sharing of cyber-threat intelligence, particularly IP addresses, is an important step in transforming the monitoring, detection, and reaction to, and remediation of, cyber threats. Cyber security threats cross enterprise, network, and national boundaries so to be most effective, threat intelligence sharing has to be done across national boundaries as well as within the US.

At the outset of the project, there was concern by some multi-national corporations that even internal information sharing within the corporate group may be subject to differing laws; and that around the world there are very different rules and regulations regarding data protection. The goal of the ICTS-Legal project is to address these concerns by providing an understanding of the international legal environment. The analysis shows there is an existing international norm established by the EU.

One of the most significant changes introduced by the GDPR is its application to businesses anywhere in the world that process the personal data of an EU data subject. This directly impacts the international sharing of cyber-threat intelligence between businesses. Where that sharing involves data transfer to the US the US/EU Privacy Shield will also apply. While the exact operation and effectiveness of Privacy Shield is not yet clear, it is clear that, in effect, the EU privacy standards will likely set the operational standard.

The 1995 Directive is currently the model used as the basis for data protection law in most major US trading and alliance partners outside the EU. The GDPR being phased-in by EU member nations makes some important new changes but there are substantive similarities with the 1995 Directive, which is currently the international norm. This is important because the analysis in this article addresses the perception that automated sharing of IP addresses as cyber threat information may not be legal, a perception that had the potential to affect the willingness and legal ability of organizations to engage in business-to-business sharing of cyber-threat information internationally.

As the analysis shows, automated sharing of IP addresses is clearly "processing" as defined under both the GDPR and the corresponding provisions of its predecessor, the 1995 Directive. The major issue therefore is the classification of an IP address as "personal data" under the 1995 Directive and the GDPR. As discussed, the recent decision of the CJEU in the Breyer case raises more questions than answers.

[79] See for example, *Rotaru v Romania* (28341/95) 8 BHRC 449.
[80] Article 8 (2).
[81] *Peck v United Kingdom*, [2003] All ER 255, (2003) 36 EHRR 719.
[82] *Peck v United Kingdom*, [2003] All ER 255, (2003) 36 EHRR 719 at 77.
[83] Article 29 Working Group, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 35 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

Nevertheless, the analysis in this article shows that automated business to business sharing of that data can be done in the public interest under Article 6(1)(e) of the GDPR and its equivalent in the 1995 Directive.

This is an important finding because while automated sharing of cyber threat information is a legitimate interest of the data controller and a third party under Article 6 (1)(f) of the GDPR, notification of the data subject (who is the suspected bad actor) seems to be required by Articles 13 and 14. In this respect, the authors assert that the GDPR is flawed. However, sharing of IP addresses as cyber-threat intelligence can be justified in the public interest under Article 6 (1)(e) of the GDPR to which the notification requirements of Articles 13 and 14 do not apply. Sharing of threat intelligence is in the public interest and that interest overrides the individual rights of a data subject under Article 8(1) of the Charter of Fundamental Rights of the European Union which underpins the GDPR and its equivalent in the 1995 Directive as long as the concepts of necessity and proportionality-of-purpose are adhered to in respect of the design of the specific measures proposed (which is particularly important when it comes to automated sharing that can be done on bulk).

This result of the ICTS-Legal project and the analysis in this paper show that a common cyber security ecosystem is possible and brings it closer to fruition. This is a major contribution to cyber security.

## Acknowledgement

The authors thank Andrew Tabas, Georgetown University for his research assistance in the preparation of this article.

The National Science Foundation supports this work under Grant No. 1362046. This work receives support from the industry affiliates of the Security and Software Engineering Research Center ($S^2$ERC). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or $S^2$ERC affiliates. Affiliates pay Georgetown University and the funds are used to cover the expenses of the study and related academic and research activities of the institution.