BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 6 • N° 26 • SEPTEMBER 2020

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

EUROPEAN LAW ENFORCEMENT AND US DATA COMPANIES: A DECADE OF COOPERATION FREE FROM LAW

by Angela Aguinaldo and Paul De Hert

Online evidence has been indispensable in criminal matters but due to its transnational and volatile nature, there have been issues and challenges as regards access, transfer, and usage in criminal investigations and prosecutions. In recent years, practices have been established to overcome the hurdles of cross-border access to online evidence. One of these practices is direct cooperation between law enforcement authorities and data companies, the latter of which are mostly based in the US. While this cooperation has been less blatant and apparent in its earlier years due to the want of legal basis, law enforcement authorities have been less coy towards the practice more recently. The present contribution walks the reader through the recent developments on codifying the practice of direct cooperation between European law enforcement authorities and US data companies. These developments evince how law enforcement authorities are willingly and wittingly overlooking protective safeguards and issues that ought to be addressed and thoroughly discussed. By sanctioning a relationship of direct cooperation, not only are state interests affected, but likewise issues of trust, MLA rights, privacy and data protection are affected. There ought to be a thorough discussion on these issues and hopefully the lessons learned from the recent CJEU judgments and the German Federal Constitutional Court are taken into consideration.

Key Words: US CLOUD Act, European Union, Council of Europe, cross-border access to online evidence, online evidence, mutual legal assistance, data protection, privacy, Schrems 1, Schrems 2, data companies, direct cooperation, unilateralism, jurisdictional expansion

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
Please quote the final version Angela Aguinaldo & Paul De Hert, 'European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law', in Federico Fabbrini, Edoardo Celeste & John Quinn (eds.), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Pu, 2020, 157-172*

Disclaimer

Introduction

Online evidence has become indispensable in criminal matters but due to its transnational and volatile nature, law enforcement authorities are confronted with challenges in accessing, securing, and using it in their investigations and prosecutions of both online and ordinary crimes. Traditional routes of international cooperation such as mutual legal assistance have allegedly become more of stumbling blocks rather than instruments of efficiency and fluidity in ensuring that law enforcement authorities are not hampered in the fulfilment of their duties and obligations. It does not help that online evidence, and cyberspace matters in general, are riddled with sensitive issues that ought to be addressed, and yet no definite consensus has been made towards a solution.

Thus, it has not been surprising to see on the state, regional, and international levels that recourse to different methods has been made to overcome these challenges. There is, for instance, the phenomenon of data localisation or nationalisation, compelling service providers and tech companies to localise and keep data within the confines of a particular jurisdiction.[1] The evident objective of this state-centric approach is to create domestic-level information controls to shift governance away from international or pluralist governance models.[2] Also oversimplifying, at the cost of the blurred reality of the digital, is the resort to unilateralism or jurisdictional expansion – an expanding, deepening, and more elaborate extraterritorial projection of power which overstretches a state's jurisdiction over data regardless of where the same is located.[3] In connection to this, law enforcement authorities are finding ways to directly cooperate with service providers and tech companies – while attempting to legitimise their actions – to access online evidence without the hurdles posed by traditional international cooperation agreements.

Although initially not acknowledged, voluntary or not-so-voluntary cooperation between law enforcement authorities and service providers has been a reality for more than a decade as regards online evidence in criminal matters.[4] The Council of Europe, in its 2008 Guidelines,[5] tacitly recognised that direct liaison between foreign service providers and law enforcement authorities occurred, albeit that the said practice was highly discouraged.[6] In 2012 and 2013, statistics were provided by the biggest tech companies and service providers that further highlighted this trend.[7] In a 2014 report, the Council of Europe concluded

1 Christoph Burchard, 'Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamental-prinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1' (2018) 7 Zeitschrift für die internationale Strafrechtsdogmatik 52, 52; Paul De Hert, Cihan Parlar and Johannes Thumfart, 'Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland' (2018) 9 New Journal of European Criminal Law 326, 326; Jonas Force Hill, 'Problematic Alternatives: MLAT Reform for the Digital Age', 28 January 2015, Harvard Law School National Security Journal 1.

2 Ronald J Deibert and Louis W Pauly, 'Mutual Entanglement and Complex Sovereignty in Cyberspace' in Didier Bigo, Engin Isin and Evelyn Ruppert (eds), Data Politics: Worlds, Subjects, Rights (Routledge, 2019) 81, 81.

3 Burchard (n 1 above) 52; De Hert, Parlar and Thumfart (n 1 above) 326; Deibert and Pauly (n 2 above) 81; Hill (n 1 above) 1. For illustrations of unilateralism, see David Callaway and Lothar Determann, 'The New US Cloud Act - History, Rules, and Effects' (2018) 35 The Computer & Internet Lawyer 4; Paul De Hert and Monika Kopcheva, 'International Mutual Legal Assistance in Criminal Law Made Redundant: A Comment on the Belgian Yahoo! Case' (2011) 27 Computer Law & Security Review 291, 291–97.

4 Micheál O'Floinn, 'It Wasn't All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe' (2013) 29 Computer Law & Security Review 610, 611.

5 Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, adopted by the global Conference Cooperation against Cybercrime, 01-02 April 2008, Guideline 36.

6 Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Siani Pearson and George Yee (eds), Privacy and Security for Cloud Computing (Springer, 2013) 47.

7 In April 2013 Google published its annual transparency reports and disclosed how authorities would interact with the company by requesting content removal or user data. Of all the requests Google received, 40% were complied with. One-third of the requests received came from EU Member States. On the other hand, Microsoft released its Law Enforcement Requests Report that shows that in 2012 requests from EU Member States represented 47% of the total requests. See Gertjan Boulet and Nicholas Hernanz, 'Cross-Border Law Enforcement Access to Data on the Internet and Rule of Law Challenges in the EU' (2013) 6 SAPIENT Policy Brief (Deliverable 6.6).

that the prosecution or police services of many States contact foreign service providers directly, in particular those based in the United States, and these may respond positively under certain conditions. Such requests may take the form of domestic production orders. Some providers may respond directly to requests related to emergency situations. Overall, conditions for such direct contacts are unclear; in some countries information thus obtained may need to be validated through a subsequent mutual legal assistance (MLA)- request before use as evidence in court.[8]

In September 2016, a survey was conducted by the European Commission that revealed a lack of common approach to obtaining cross-border access to digital evidence by Member States: either they accessed evidence by going directly to service providers with a request to cooperate or by means of direct cross-border access to digital evidence.[9]

Today law enforcement authorities are less coy on this kind of practice: in many countries they routinely turn to foreign service providers (often based in the US) and are provided with data from these providers, with the latter having readily available mechanisms to grant these requests.[10]

We start our contribution with a short section on the recent reforms to codify direct cooperation between law enforcement authorities and private actors (section II). After a discussion of the 2018 US CLOUD Act, we turn to the proposal of the European Union to facilitate cross-border access to electronic evidence, which was presented by the European Commission in April 2018 (e-evidence package) and the reform process at the Council of Europe to amend the 2001 Cybercrime Convention envisaging a similar mechanism and powers.

The following section discusses the current MLA framework that regulates cooperation in criminal matters and exchange of evidence between the US and Europe (section III). The MLA system allows cooperation between enforcement authorities but does not foresee any basis for direct cooperation with private actors in other states. Nonetheless this practice was dubiously accepted by the regulatory community on shaky interpretative grounds as permissible under Article 18 (on domestic production orders) and 32 (on extraterritorial data access relying on consent) of the Cybercrime Convention (see section IV).

We then proceed in section V with the challenges this kind of relationship poses for state interests and for public international law and the individual concerned that is deprived by these informal practices of certain checks and guarantees built into the formal MLA system as stated above. This discussion includes issues surrounding data protection that arise from the kind of relationship that allows law enforcement authorities to have direct access to online evidence through cooperating directly with service providers and tech companies (see section VI). After a brief reflection on the weight of privacy and data protection in criminal law matters, we identify the relevant dos and don'ts in data protection law and clarify the relationship between our subject matter and the outcomes of the two ***Schrems*** judgments of the CJEU. In particular, the combination of the teachings of ***Schrems II*** (decided on 16 July 2020) about the deficiencies in US law with those of the German Federal Constitutional Court on the proportionality of domestic production orders (BVerfG, 27 May 2020) might add to the relevance of data protection as an argument

8 Cybercrime Convention Committee, 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime', ***12th Plenary of the Cybercrime Convention Committee*** (Council of Europe 2014) 124.

9 Els De Busser, 'The Digital Unfitness of Mutual Legal Assistance' (2017) 28 ***Security and Human Rights*** 161, 171. See for other reports, De Hert, Parlar and Thumfart (n 1 above) 328.

10 Bert-Jaap Koops and Morag Goodwin, 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law' (Tilburg University, 2014) 58; O'Floinn (n 4 above) 61.

against informal trans-border co-operations (section VII). Lastly, we summarise our discussion and provide recommendations for further study and discussion (section VIII).

1. New Alternative Systems to the MLATS

In 2018, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, allowing US federal law enforcement authorities to compel US-based data companies (via warrant or subpoena) to provide data, regardless of whether the data are stored in the US or on foreign soil.[11] With the Act the US now declares that it has the authority to reach into the data centres of US data companies in Europe without any need for international corporation or European judicial controls.[12] But there is also good news for Europe. The CLOUD Act also exempts international requests for data from US firms from the traditional framework of mutual legal assistance treaties in criminal law (MLATs). Rather than operating through treaties, the US executive branch is given the ability to enter into bi-lateral ('executive') agreements with foreign countries to provide requested data related to its citizens in a streamlined manner, as long as the Attorney General, with concurrence of the Secretary of State, agrees that the foreign country adheres to applicable international human rights obligations and has sufficient protections in place to restrict access to data related to US citizens. No special guarantees are built in for data relating to non-US citizens. Once such an agreement is there, direct contacts between foreign law enforcement authorities and US data companies are permitted in response to an order from a foreign government with which the United States has an executive agreement on data access, a provider may intercept or disclose the contents of a stored electronic communication or non-content records or information pertaining to a subscriber or customer. Simultaneously, the same year, the European Union (EU) proposed similar sweeping changes which would allow European law enforcement agencies in Member States to preserve and collect cloud-based evidence outside of the MLAT system. This e-evidence package includes 'a proposed regulation for European Production and Preservation Orders' as well as 'a proposed directive' supplementary thereto, which will mandate the establishment of legal representatives of service providers within the EU that could be served with orders.[13] Like the CLOUD Act, the EU proposals organise direct cooperation with service providers while taking away the need to go through the traditional route of mutual legal assistance.[14] These proposals are intended as fast-track alternatives vis-à-vis online evidence to make it 'easier to secure and gather electronic evidence for criminal proceedings stored or held by service providers in another jurisdiction'.[15] The main idea is that certificates of judicial orders will be transmitted directly to the legal representatives of online service providers. These will be obliged to respond within 10 days or, in urgent cases, within six hours.

11 The Act was signed by Trump on 23 March 2018 and amends the Stored Communications Act (SCA) of 1986 and the Electronic Communications Privacy Act of the same year.

12 Lawrence Siry, 'Cloudy Days Ahead: Cross-Border Evidence Collection and Its Impact on the Rights of EU Citizens' (2019) 10 New Journal of European Criminal Law 227, 241.

13 European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final; Council of Europe, 'Legal Opinion on Budapest Cybercrime Convention: Use of a Disconnection Clause in the Second Additional Protocol to the Budapest Convention on Cybercrime'; Sofie Depauw, 'Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?' (2018) 8 European Criminal Law Review 62, 1–23; Ángel Tinoco Pastrana, 'The Proposal on Electronic Evidence in the European Union' (2020) 15 EUCrim 46, 46–50.

14 See Proposed Regulation on the European Preservation and Production Orders, arts 2, 4-7.

15 Other international cooperation instruments such as the European Investigative Order and mutual legal assistance will continue to exist. See the Explanatory Memorandum on the Proposed Regulation on the European Preservation and Production Orders.

Finally, there is the work of the Council of Europe (CoE), mother organisation of the 2001 Cybercrime Convention.[16] Currently, the organisation is drafting a second new Protocol to the Cybercrime Convention. The work on the Second Additional Protocol started in June 2017.[17] The Second Additional Protocol is meant to clarify matters on transnational access to electronic evidence and is supposed to 'to set out, among other things, a clearer framework and stronger safeguards for existing practices of transborder access to data and safeguards, including data protection requirements',[18] including provisions for an efficient and effective mutual legal assistance, direct trans-border cooperation with providers, a framework and safeguards for practices of trans-border access to data, including trans-border searches, and data protection provisions.[19] With regard to mutual legal assistance, the Second Additional Protocol is intended to be the legal basis for international production orders or simplified MLA for subscriber information, direct cooperation between authorities, joint investigations, requests to be made in English, and emergency procedures.[20]

A detailed account of these regulatory initiatives can be found in other contributions to this volume,[21] but for purposes of the present discussion, it can be said that in terms of human rights and data protection concerns, much will depend on the implementation of the US CLOUD Act by the US executive, and on the details of the two European initiatives. In terms of state choice between unilateralism and multilateralism to face extraterritorial challenges, the same 'wait and see' attitude is warranted. In particular, the US and the EU initiatives have an aggressive unilateral dimension in facilitating their law enforcement authorities to obtain data abroad, and it is likely that other states, including authoritarian ones, are going to seek the same kind of access.[22] If the US limits its executive agreements to 'like-minded states' in terms of human rights, without MLA reform to help out the others, these states will likely move ahead with their own national initiatives to access user data, including measures like forced data localisation or government-sponsored hacking. Such approaches can threaten user rights and hurt businesses.[23]

2. The MLA Framework with the US

MLA represents the classical treaty-based mechanism allowing for foreign law enforcement cooperation and assistance in ongoing criminal investigations and proceedings, while respecting the notions of jurisdiction and national sovereignty in criminal justice matters. MLA is mostly based on treaties between states that confirm that authorities can send each other requests for help (to search a house, to hear a witness, to send over a copy of a criminal record). These treaties then specify the modalities of cooperation based on requests and contain mechanisms that allow requested states to perform certain checks

16 Convention on Cybercrime, Budapest, 23 November 2001, available at conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.
17 Europe (n 13 above); Cybercrime Convention Committee (T-CY), 'Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime: State of Play', p 2.
18 See Depauw (n 13 above) 3; Luca Tosoni, 'Rethinking Privacy in the Council of Europe's Convention on Cybercrime' (2018) 34(6) Computer Law & Security Review 1197, 1210.
19 De Hert, Parlar and Thumfart (n 1 above) 335; Alexander Seger, 'E-Evidence and Access to Data in the Cloud Results of the Cloud Evidence Group of the Cybercrime Convention Committee', Handling and Exchanging Electronic Evidence Across Europe (Springer, 2018).
20 Seger (n 19 above) 40; Cybercrime Convention Committee (T-CY) (n 17above) 2.
21 See for a first analysis, Mirko Hohmann and Sophie Barnett, 'System Upgrade. Improving Cross-Border Access to Electronic Evidence', GPPI Policy Brief.
22 'In general, the EU should be aware that the scope of the change to the system of international data access it proposes with the Regulation and the respective production orders is quite dramatic. If it gives its member states access to data stored by companies that are not incorporated in the EU, other states, including authoritarian ones, are going to seek the same kind of access. This does not mean that one should not establish such a system, but it is necessary to be aware of the consequences': Hohmann and Barnett (n 21 above) 25
23 Hohmann and Barnett (n 21 above) 25.

on the incoming requests before deciding whether to follow up with the request.[24] States can traditionally refuse cooperation when this would be detrimental to their interest or state sovereignty. The MLA system has gained its place in international public law. It is built on the idea of mutual respect between states and the principle of territoriality as the starting point of jurisdiction, giving states wide discretion in law enforcement within their territory but forcing them to request assistance when evidence is situated abroad or when suspects have evaded the territory. The doctrine of territoriality has successfully created trust among the actors involved, preventing states from enforcing their laws extraterritorially and infringing the sovereign territory of other states.[25]

Its success cannot nonetheless shield its shortcomings: not all states have signed MLATs; international public law is poor in enforcing the MLA system and the territoriality principle; it is not designed for handling a high number of requests; it does not distinguish between light and heavy assistance and does not foresee swift, but balanced procedures for 'light' requests about for instance subscriber data; MLATs frequently do not address fundamental issues like the balancing of defence rights or data protection and privacy with law enforcement's need for evidence,[26] and MLATs' strong link with territoriality when applied to data that is often unterritorial does not address contemporary understandings and 'questions of data jurisdiction, like how to treat data held overseas by a subsidiary of a domestic parent company'.[27]

The US has MLATs of a general nature with all Member States of the EU and with the EU itself, all of a recent nature,[28] with broadly formulated possibilities to request assistance suited in relation to many aspects, including obtaining data. It is true, however, that these treaties were conceived in the pre-Internet era, do not envisage contacts with private parties abroad, and do not formulate answers to most of the shortcomings identified in the previous paragraph.

The US has equally ratified, together with other European and non-European states, the more specific 2001 Cybercrime Convention.[29] Cooperation with private partners is featured in this convention,[30] but only at the national level, not at the international level. Most of the shortcomings of MLATs discussed ***above*** are also present. The Convention is poor on defence rights,[31] on privacy and data protection; is based on the territoriality principle and on the idea that data can be located in space; there is no 'light' MLA procedure for requests like obtaining subscriber data, and the text of this convention is bereft of any provision that permits law enforcement authorities to directly contact foreign service providers in pursuit of cross-border access and exchange of online evidence in criminal matters.

24 De Busser (n 9 above) 162–63.
25 Hohmann and Barnett (n 21 above) 17.
26 'MLATs frequently do not specify what constitutes "protected data" or under what conditions "content" differs from "metadata" for the purposes of information sharing. This hinders cooperation between states with differing domestic understanding of these terms': Hill (n 1 above) 2.
27 Hill (n 1 above) 2; Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 ***Yale Law Journal*** 326. Cf Hohmann and Barnett (n 21 above) 17. Under the territoriality principle the data's physical location determines the jurisdiction to which the data and thus the company holding the data is subject. The US CLOUD Act and the EU initiative focus on the locations of the user and the company – rather than that of the data – as the determinant of jurisdiction, in order to oblige companies to transfer data, irrespective of the place of storage. As such, they depart from the principle of territoriality.
28 One national example: Agreement between the Kingdom of Belgium and the United States of America on mutual legal assistance in criminal matters, signed 28 January 1998, Belgian Official Journal, 8 December 1998, entry into force on 18 December 1999. At EU level; Agreement on Mutual Assistance in Criminal Matters between the European Union and the United States of America, 25 June 2003, OJ L 181/34–42, 19 July 2003. The agreement that was concluded in 2008 with the EU further harmonises the 27 Member State agreements. (OJ L 291, 7 November 2009).
29 See the chart of signatures at: https://www.coe.int/en/web/conventions/full-list/- /conventions/treaty/185/signatures?p_auth=ZZawh58m.
30 The convention invites Member States to create on behalf of their law enforcement authorities, powers to order providers to produce certain data, powers to order the preservation of data, and powers to search computers and networks.
31 Jonathan Clough, 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation' (2014) 40 Monash University Law Review 698, 710.

3. The Cybercrime Convention as a Basis for Direct Cooperation

The drafters of the Convention were well aware of the importance of these contacts with internationally based firms, but they only created 'domestic' production orders (and this only) for subscriber data. Article 18 allows them to order 'a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control'. Contacting providers outside the territory is unforeseen in the Convention. Extraterritorial matters or cross-border access instead are covered by classical MLAT terms of cooperation ***between*** law enforcement authorities (Articles 25, 27, 31, 33, and 34), wherein a Party needs to send a request to another Party to obtain or access data found in the latter's territory. Article 32 is the only exception, and allows for domestic law enforcement authorities' trans-border access to stored computer data where publicly available, or to any data in another country if they obtain the 'lawful and voluntary consent of the person who has the lawful authority to disclose the data to the party through that computer system'.

Today it is felt that that the Cybercrime Convention is a missed opportunity to resolve jurisdictional issues or to regulate investigative measures in cyberspace.[32] In 2011, the Cybercrime Convention Committee (T-CY) discussed possible ways to enable or regulate trans-border access to data through the Cybercrime Convention through either an amendment or a protocol,[33] but, because of the time-consuming nature of this venture, it started focusing on expanding the interpretation of the Convention via interpretative soft law instruments. Thus, the so-called Guidance Notes entered the picture and they taught us that Article 18 on domestic production orders and the exception in Article 32 could work via consent, and be read in such a way as to make possible, legally speaking, coerced cooperation with companies offering services to Europeans (even when they work abroad) and voluntary cooperation with companies in case the data is in another country.[34] Bad faith toward the original spirit and text of the Convention is apparent in these Guidance Notes, as they ignore how the Convention is structured and how it is based on the territoriality principle. Guidance Note No 10 specifically confuses the citizen's consent with the consent of the company processing this citizen's data. This 'guidance' worked nonetheless. In policy discussions of recent years, direct cooperation with providers in the US was generally accepted as compatible with the Cybercrime Convention, albeit lacking further clarification.[35]

32 Catherine Van De Heyning, 'The Boundaries of Jurisdiction in Cybercrime and Constitutional Protection: The European Perspective' in Oresto Pollicino and Graziella Romeo (eds), The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe (Routledge ????) 41–42.

33 Cybercrime Convention Committee (T-CY) Ad-Hoc Subgroup on Transborder Access and Jurisdiction, 'Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY', 8th Plenary of the Cybercrime Convention Committee (Council of Europe, 2012); Koops and Goodwin (n 10 above) 37; O'Floinn (n 4 above) 611.

34 We have elsewhere exhaustively discussed the details and clarifications proffered by Guidance Note No 3 involving transnational access as provided in Article 32 (2014), and Guidance Note No 10 involving domestic production orders as provided in Article 18 (2017) vis-à-vis trans-border access to online evidence in criminal matters in earlier contributions:see Angela Aguinaldo and Paul De Hert, 'The Council of Europe Machinery Influencing International Law Through Guidance Notes and a Proposed Second Additional Protocol' in Vanessa Franssen and Stanislaw Tosza (eds), Cambridge Handbook of Digital Evidence in Criminal Investigations (Cambridge University Press, 2020); Paul De Hert, Cihan Parlar and Juraj Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law' (2018) 34 Computer Law & Security Review 327.

35 In all relevant documents on direct cooperation and data transfers by data protection authorities, it is striking to note that all these authorities (Working Party 29, European Data Protection Board (EDPB) and European Data Protection Supervisor) either seem to accept the practice on the basis of Article 32 of the Convention or at least fail to contradict this view. Compare 'While the Commission highlights that the consent for access or to receive stored computer data, in the sense of Article 32(b) of the Budapest Convention does not refer to the consent of the individual for the processing of personal data, several references to "the affected person" seem to imply that for certain legislative options the consent of a data subject could be considered as a legal ground for access' (Statement of the Article 29 Working Party, 'Data protection and privacy aspects of cross-border access to electronic evidence', Brussels, 29 November 2017, pp 6-7 via: www.ec.europa.eu/newsroom/just/document.cfm?-doc_id=48801) and 'With regards to trans-border direct access to stored computer data as per Article 32(b) of the Budapest

4. Direct Contacts with Private Parties and Issues of Legality, Trust and MLA-Rights

Notwithstanding the practice of direct contacts being 'generally accepted', a lot of issues can be identified. Firstly, both the existence of informal practices and the attempt to shield behind the Cybercrime Convention are problematic with regard to legal analysis and coherence of international public law. Respectable as prosecutors and law enforcement authorities might be, things get troubled when they take a hard swing at the text of the Cybercrime Convention. Article 32 clearly targets consent of users, not of companies processing data of these users. Article 18 is part of a convention clearly based on the idea of territoriality of data and distinguishing between domestically held data (subject to domestic orders under Article 18) and MLA procedures for non-domestically held data. The Convention furthermore provides that all powers and procedures established in the Convention are subject to the conditions and safeguards under the domestic (constitutional) law of the Member States and the protection of human rights, in particular those entrenched in the ECHR.[36] Hence, a legal basis that includes safeguards is imperative for any cooperation with any private actor.

In light of the current practice, trust problems could arise. The MLA system has created trust amongst states due to its formalised nature and its respect for territorial sovereignty. The direct cooperation approach, as an expression of unilateralism, is a fundamental departure therefrom and can affect the trust between stakeholders and carry unexpected ramifications. Codification will only bring this issue to the forefront. The lauded success of direct cooperation might be premature or even fleeting. Hohmann and Barnett rightly point to the aggressiveness (in terms of international law) of the proposed EU e-evidence package: without distinction between democratic states with observation of the rule of law and others, it allows European authorities to demand access from all companies that provide services in their territory. These authors rightly wonder about the follow up by other states (democratic or not) that will demand such access too and will refer to the EU law as justification.[37]

Convention, the EDPB reaffirms in particular that data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required' (EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), Brussels, 13th November 2019, p 2 via: www.edpb.europa.eu/our-work-tools/our-documents/edpb-contribution-consultation-draft-second-additional-protocol-council_en). See also the Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdictions, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, 05/12/2013; EDPS Opinion 3/19 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention, via www.edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf.

36 The Convention stresses the importance of a proper legal basis, of judicial and independent supervision and of limitations of scope and duration of the powers and procedures provided. Article 18 needs to be read together with, and refers explicitly to, Articles 14 and 15 of the same Convention. We repeat that Article 18 is only about domestic production orders and allows 'persons in the territory to be ordered to hand over all data and 'service providers offering services in the territory' to hand over subscriber data. The first important element is the duty for states to introduce specific legal provisions to allow these domestic orders: Member States should introduce a cooperation duty for service providers (Article 14). Only then can enforcement authorities compel ISPs to provide data within their possession or control. See Van De Heyning (n 32 above) 42–43. Given the reference to fundamental rights, in particular the ECHR, in the Convention (Article 15), this cooperation duty is to be developed with respect for the defence of privacy and data protection. The second element in Article 18 and its distinction between 'orders to persons' in the territory (Article 18 (1a)) and 'orders to service providers' offering services in the territory (Article 18 (1b)) is that more can be asked from the former than from the latter: all computer data can be requested from persons in the territory, but only subscriber data (hence, no traffic data or content data) can be requested from service providers offering services in the territory.

37 Hohmann and Barnett (n 21 above) 22.

Another trust issue is with civil society and human rights groups, representatives of which have already spoken out against the CLOUD Act and against the EU and CoE initiatives because, as stakeholders, they were evidently kept out of the policy loop in the informal co-creation of the direct contact system (built by law enforcement authorities together with US data firms) and in most of the regulatory work by the US and 'the two Europes'.[38]

A third trust aspect concerns the involvement of private actors in the investigation of crimes and in assisting law enforcement authorities from all parts of the world. Legal experts have difficulties with this 'natural trend' to ask data from companies that are then supposed to assess and vet these requests from foreign authorities. What criteria will they use to say 'yes' or 'no' to requests? Hohmann and Barnett observe that there is a risk in privatising legal assistance, 'because companies will follow their own guidance and establish their own mechanisms for evaluating such requests, which are neither wholly transparent nor determined in democratic processes'.[39]

Further, as De Busser has opined, a service provider is a company and not an authority, so invoking grounds for refusal as one knows them from mutual legal assistance agreements and mutual recognition would not be a task for the provider.[40] De Busser further notes that it is not generally part of the interests of service provider companies to refuse cooperation based on, for example, double criminality or ***ne bis in idem***, and in fact they cannot be expected to have the knowledge base or capacity to thoroughly assess such grounds and other issues.[41] Thus, it would not be surprising that, even if private companies were given the responsibilities to be aware of all the relevant data protection legislation, mutual legal assistance and other cooperation legislation, grounds of refusal, etc, as well as increased capacity to entertain requests coming from different countries, service providers would never grasp completely the idea of political and constitutional responsibility, let alone the common public spirit.[42]

5. Privacy and Data Protection Repercussions

The confrontation between criminal procedural law and privacy or data protection seldom delivers groundbreaking results. Investigating crimes often trumps privacy and data protection concerns as long as there is a firm legal basis for investigatory powers and a graduated system of checks and balances proportional to the seriousness of the privacy infringements. In order to pass the European human rights standards of the European Court of Human Rights it helps - but it is not enough - to have a judge involved in the investigation either beforehand, during, or after the investigative measure of some importance is carried out.[43] Other measures can be left to the discretion of authorities. Serious privacy objections in criminal law will trigger serious guarantees, but usually lack the clout to block certain powers asked for by the law

38 Hohmann and Barnett (n 21 above) 25; Paul De Hert and Angela Aguinaldo, 'A Leading Role for the EU in Drafting Criminal Law Powers? Use of the Council of Europe for Policy Laundering' (2019) 10(2) New Journal of European Criminal Law 99. Interesting is the proposal to establish an expert and stakeholder input process for non-governmental stakeholders to rebuild trust in the CLOUD Act system and the proposal to demand transparency reports from both US data firms and governments detailing the number of requests sent or received, respectively (including the number of requests that were declined) combined with regular reviews and audits to check whether governments as well as companies are complying with the legal framework.

39 Hohmann and Barnett (n 21 above) 19.

40 De Busser (n 9 above) 172.

41 De Busser (n 9 above) 172.

42 Christoph Burchard, 'Der Grenzüberschreitende Zugriff Auf Clouddaten Im Lichte Der Fundamental-Prinzipien Der Internationalen Zusammenarbeit in Strafsachen – Teil 2' (2018) 7/8 Zeitschrift für die internationale Strafrechtsdogmatik 249, 260.

43 Gianclaudio Malgieri and Paul De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably But Not Necessarily by Judges' in David Gray and Stephen Henderson (eds), Cambridge Handbook of Surveillance Law (Cambridge University Press, 2017).

enforcement community permanently. Having said that, it is more than useful to discuss here privacy and data protection powers, in a law enforcement context, to set limits on what is collected, where, by whom, and to impose a duty of care on law enforcement authorities once the data is collected.

Data protection is essentially about guaranteeing a full cycle of control over data. Processing data of others is acceptable on legitimate grounds if one controls the flow, nature, and quality (including assessing the proportionality) of data. When, for instance, personal data is inaccurate or erroneous, it falls on the controller of this data to correct and to inform all others who have had access to the erroneous data about the inaccuracy. In transnational matters things become more complicated because one has to consider data protection laws in all countries involved. Nudging or forcing international companies to share data that is stored abroad is a clear violation of the protective rules of privacy and data protection under the domestic law of the state where the server storing the data is established.[44] Practices of direct cooperation, based on a misleading interpretation of the term 'consent' in the Cybercrime Convention, are simply antipodal to the American and European data protection obligations of the US data firms and to the standards of foreseeability identified by the European Court of Human Rights with regard to privacy intrusions.[45]

The informed reader might wonder how our theme relates to the CJEU's Schrems I decision invalidating an EU data protection agreement with the US (Safe Harbour Framework) in 2015, because of insufficiencies in US law that did not set forth any objective criteria for determining limits to the access and use of this personal data by US public authorities.46 Resulting therefrom and the Snowden revelations, the European Commission replaced the Safe Harbour Framework with a new one (the EU-US Privacy Shield Framework), and added Article 48 to the EU General Data Protection Regulation (GDPR) stating that: any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.[47]

Hence, 'no EU data for US law enforcement authorities without MLA', says the GDPR. Interestingly, while Article 48 GDPR addresses law enforcement authorities from non-EU nations, it does not impart any strong cautionary message directed to European law enforcement authorities which obtain data from non-EU firms such as those in the US. Neither does the rest of the GDPR or the Law Enforcement Directive (EU) 2016/680 for Police and Criminal Justice Authorities, which entered into force on 5 May 2016.[48] Significantly, these two instruments are grounded on the message (which we already mentioned above) that data protection is quintessentially legalistic: regulate all data flows vis-à-vis all data protection principles enshrined in law. Thus, there is the need to formalise the informal (or unstated) and regulate it. This is hardly a fundamental objection!

44 Van De Heyning (n 32 above) 42–43.

45 The provider does not own the data of data subjects and needs the data subject's consent or an explicit legal basis in domestic law to give access. A demand by a foreign law enforcement actor is neither of both.

46 Case C-362/14 Maximilian Schrems v Data Protection Commissioner, 6 October 2015, ECLI:EU:C:650. The judgment resulted from a complaint filed by Max Schrems with the Irish data protection authority against Facebook for allowing US law enforcement and intelligence authorities access to his personal data in violation of EU data protection law. The CJEU invalidated the EU 'data-deal' with the US - allowing US data firms to process data about EU citizens in the US - because of the general insufficiency, in the eyes of the Court, of US data protection laws to guarantee controlled data processing cycles in the US when confronted with data-hungry US law enforcement and intelligence agencies.

47 This 'blocking statute', that requires an international agreement for data to be shared with law enforcement officers in non-EU nations, is now being criticised as 'conflicting' since the EU is prohibiting broad access to data for others, while its e-evidence package will allow EU authorities broad access to data stored abroad. See Hohmann and Barnett (n 21 above) 25–26.

48 The political agreement of the co-legislators on the Police and Criminal Justice Directive was, together with the General Data Protection Regulation (GDPR), reached just before Christmas 2015. Subsequently, the PCJ Directive and the GDPR were formally adopted on 14 April 2016, officially signed on 27 April 2016 and published in the Official Journal of the European Union on 4 May 2016.

6. *Schrems II* and the Decision of the Bundesverfassungsgericht on Domestic Production Orders

With this being said, it is yet to be determined if this tone towards European law enforcement authorities would change in light of the Schrems II judgment or whether European policymakers will remain resilient in favouring law enforcement authorities.[49] The validity of standard contractual clauses (SCC) with the US notwithstanding[50], the CJEU held as invalid the EU-US Privacy Shield Framework based on several factors: (1) the primacy of US law enforcement requirements over those of the Privacy Shield (paragraph 164); (2) a lack of necessary limitations and safeguards on the power of the authorities under US law, particularly in light of proportionality requirements (paragraphs 168-185); (3) the lack of an effective remedy in the US for EU data subjects (paragraphs 191-192); and (4) deficiencies in the Privacy Shield Ombudsman mechanism (paragraphs 193-197). In its evaluation of these issues, the Court paid particular heed to Articles 7, 8, and 47 of the EU Charter of Fundamental Rights. In light of these deficiencies, the Court found that the Privacy Shield Framework was invalid (paragraph 201) with immediate effect (paragraph 202).

With this judgment about the imperfect US system in mind, we are dumbfounded by the fact that the issue of direct contacts between law enforcement authorities and US data firms has not triggered intense debates from the data protection community, including the European data protection authorities. In their interventions and recommendations, we find an emphasis on a detailed legal basis, on effective remedies, on a duty to notify (if possible) the data subject after the data has been shared, on the danger of an uncritical distinction between content and non-content data,[51] but in general there has been no fundamental objection to the idea itself of seeking data amongst US-based companies.

We hope nonetheless that this improves in light of the recent decision of the German Federal Constitutional Court (***Bundesverfassungsgericht***) to the effect that direct contact of law enforcement authorities with service providers to obtain subscriber data is unconstitutional for violating the data subject's constitutional right to informational self-determination and privacy of telecommunications.[52] In deciding on the unconstitutionality of § 131 of the German Telecommunications Act that provides for this procedure under challenge, the Federal Constitutional Court states that while providing information on subscriber data is constitutionally permissible, there ought to be a proportionate legal basis for the transfer and retrieval of said data by authorities, which was not provided for in the contested law.[53]

49 Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 16 July 2020.

50 In said judgment, the CJEU upheld the validity of standard contractual clauses (SCC) as appropriate protection for EU personal data but enjoined EU organisations to take a proactive role in evaluating the existence of appropriate protection. Also, any inability to comply with the SCC by non-EU data importers must be reported immediately and EU data exporters ought to suspend transfer of data and/or terminate the contract.

51 More in detail, Statement of the Article 29 Working Party (n 35 above), 1-4; EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention (n 35 above), p 4.

52 BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 - Rn. 1-275,

53 As the Court elucidated, 'The First Senate clarified that, in principle, despite the moderate weight of the interference, using the general powers to transfer and retrieve subscriber data in the context of maintaining public security and the activities of intelligence services requires there to be a specific danger in the individual case, and an initial suspicion of criminal conduct (Anfangsverdacht) in the context of the investigation and prosecution of offences. Where, with regard to maintaining public security or activities of intelligence services, the thresholds for the use of powers require less than a specific danger, this must be compensated for by establishing stricter requirements for the weight of the legal interests meriting protection. For the most part, the challenged provisions did not satisfy these requirements.'

Noteworthy is the suggestion by one of the data protection authorities to add more data protection guidance in the CoE draft proposals.[54] Most of their input on the current European e-evidence projects discussed earlier has to do with criminal law and MLAT principles, but not so much with data protection strictly speaking. For example, they invited the EU legislator to move prudently and step by step, taking into account previous measures, often of a recent nature. Hence they asked for consideration and assessment of the potential impact of the recent Directive on the European Investigation Order on the access to e-evidence located in another Member State, before moving forward with the proposal.[55] Other ideas suggested by the data protection authorities are equally not data-protection-specific: for example, the suggestion to allow direct contacts with private companies only for specific, serious crimes,[56] and to impose a double criminality requirement (no collaboration if the facts are not criminalised in both the requesting and requested state).[57]

In our opinion, these suggestions gain considerably in terms of weight in the light of a combined reading of ***Schrems II*** (16 July 2020) about deficiencies in US law and the ruling of the German Federal Constitutional Court on the proportionality of domestic production orders (BVerfG, 27 May 2020).

54 EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention (n 35 above), p 5: 'The EDPB considers that specific provisions on data protection safeguards shall reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. These principles are also in line with the Council of Europe modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Convention on Cybercrime are also Party'.

55 Statement of the Article 29 Working Party (n 35 above), p 4.

56 'The EDPB recommends that the definition of subscriber information, as per Article 18.3 of the Convention, be further clarified in order to avoid inclusion of any traffic data or content data. Information needed for the purpose of identifying a subscriber of a service may indeed include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time, which under EU law constitute traffic data relating to the transmission of a communication. In addition, the EDPB recalls that, in accordance with the relevant CJEU case law, to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way. The CJEU has furthermore ruled in its judgement in joined cases C-203/15 and C-698/15 Tele2 Sverige AB that metadata such as traffic data and location data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications' (EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention (n 35 above), p 4 with reference to CJEU Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970 – para 99).

57 EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention (n 35 above), p 4.

Conclusion

We started our contribution with a short discussion of the 2018 US CLOUD Act, the 2018 EU package to facilitate cross-border access to electronic evidence, and the 2018 CoE reform process to amend the 2001 Cybercrime Convention. All three initiatives open the door for a formal recognition of public-private cooperative mechanisms. How was this legally possible without such frameworks? In section III we discussed the pre-existing MLA framework. This MLA system allowed for cooperation between enforcement authorities but did not foresee any basis for direct cooperation with private actors in other states. Nonetheless this practice was dubiously accepted by the regulatory community on shaky interpretative grounds as being permissible under Articles 18 (on domestic production orders) and 32 (on extraterritorial data access relying on consent) of the Cybercrime Convention (section IV).

We proceeded thereafter to highlight problems arising from the practice of direct contacts. We pointed out the problems about legality, trust, and rights concomitant to the MLA system, which are being wittingly or willingly disregarded (sections V-VII). This includes the dangers of privatising international cooperation and the safeguards that are sacrificed in this regard. Lastly, we pointed out the want of necessary discussion and debate about data protection and privacy vis-à-vis direct contacts. There are lessons to be learned from recent judgments of the CJEU and the German Federal Constitutional Court, but we have yet to determine how these would truly affect the direction policymakers would take in the discussion. This notwithstanding, the message of data protection is clear on formalising informal processes, delineating and defining the needed processes and parameters to be followed. For us, this is not highly objectionable and can be done to ensure safeguards are in place.

Having said this, the work is still not done. Despite our initial observations made herein, the practice of direct contacts between law enforcement authorities and service providers ought to be continually analysed together with the policies being currently pushed regarding it. Reflection is needed to ensure that direct contacts are not merely a quick fix with no long-term solutions. And more importantly, it would be prudent to determine whether direct contacts are the best solution in the first place to address the problems surrounding cross-border exchange of digital evidence.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

N°24 Individuation: re-imagining data privacy laws to protect against digital harms (July 2020) by Anna Johnston (22 pages)

N°25 The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities (August 2020) by Jonas Botta (16 pages)

N°26 European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law (September 2020) by Angela Aguinaldo and Paul De Hert (16 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

BRUSSELS PRIVACY HUB