HCCH

Connecter Protéger Coopérer Depuis 1893
Connecting Protecting Cooperating Since 1893

HCCH a|Bridged Edition 2019

The HCCH Service Convention in the Era of Electronic and Information Technology

11 December 2019
The Hague
(Netherlands)

Hague **C**onference on Private International Law – **C**onférence de La **H**aye de droit international privé

HCCH a|Bridged
Edition 2019:

The HCCH Service Convention in the Era of Electronic and Information Technology

Published by
The Hague Conference on Private International Law – HCCH
Permanent Bureau
Churchillplein 6b
2517 JW The Hague
Netherlands

+31 70 363 3303
+31 70 360 4867
secretariat@hcch.net
www.hcch.net

Published in The Hague, the Netherlands

FOREWORD

We live in a world of private international law. A world that is increasingly interdependent, filled with cross-border interactions, transactions, relations, and litigation. The work of the HCCH has never been more important. The bridges we build across the world have never been more important. This being said, for our work to continue to be relevant – for the bridges to be able to support new forms of traffic – we need to take technical developments into account and assess whether or not HCCH Conventions evolve with their time.

It is against this background that I am particularly pleased to present the post-event publication of the inaugural *HCCH a|Bridged* event. The *HCCH a|Bridged* event concept is a novel set up, which illustrates how dynamic, innovative and young the HCCH is, more than 125 years after its inception. The event resulted in this exciting publication on a topic dear to my heart – the intersection of new technology and law.

The *HCCH a|Bridged* series allows us to continue and deepen our discussions on the use of modern technology in the context of the work of the HCCH. These discussions started 20 years ago at the 1999 Geneva Roundtable. The success and longevity of the HCCH Conventions not only result from their ability to facilitate effective, practical justice to all by simplifying and streamlining procedures, but also, and maybe in particular, from their *technology neutrality*. It is this neutrality that enables HCCH Conventions to embrace new developments and new technologies to pass the test of time, and to adjust effectively to changing environments. The HCCH 1965 Service Convention is no exception. Contributions from our speakers at the *HCCH a|Bridged Edition 2019* event, which are memorialised in this publication, illustrate how practices under the Service Convention have evolved to best employ communications and information technology, as well as what can be anticipated in the area of cross-border service and international civil procedure more generally.

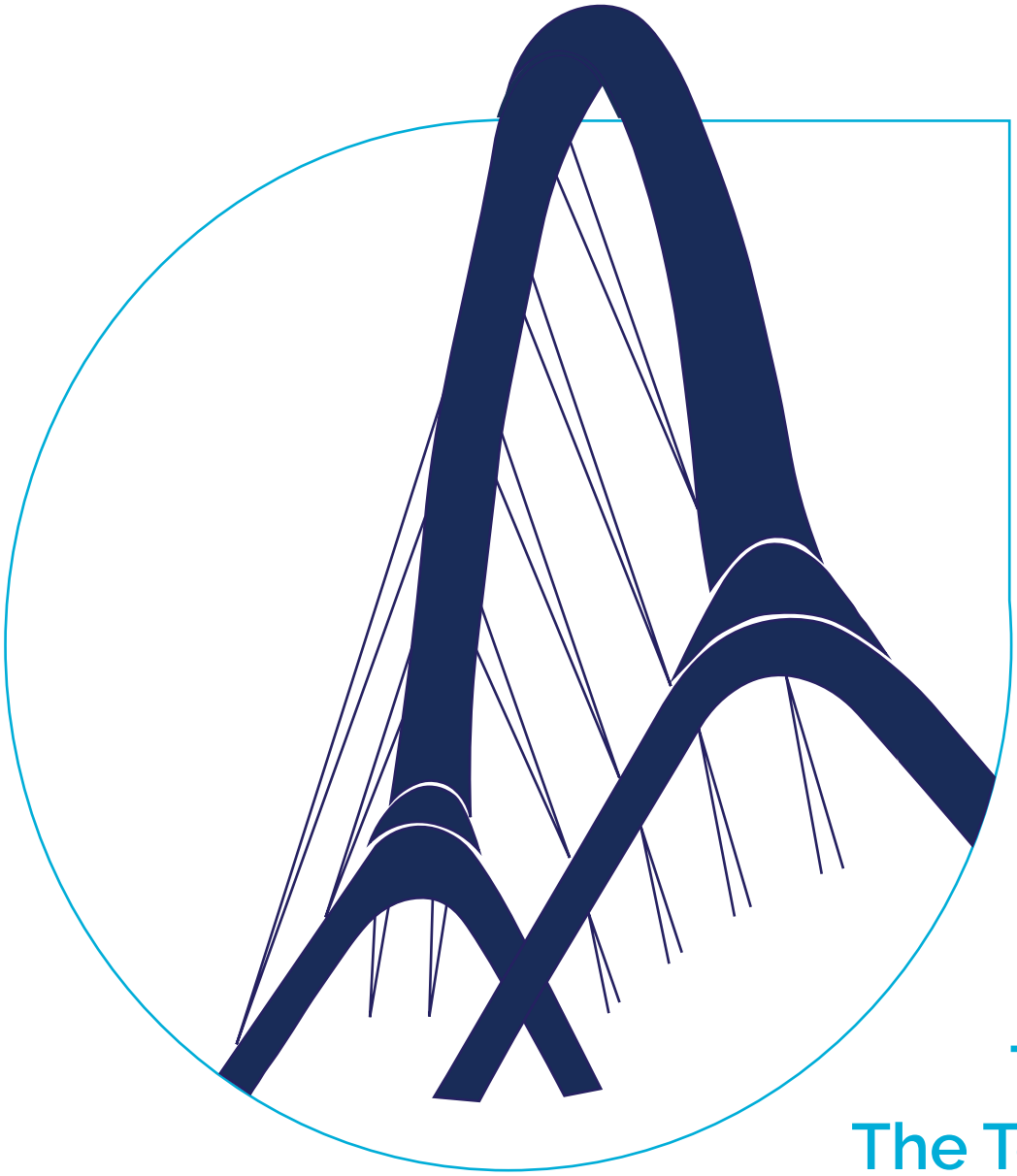
All this not only is in line with the HCCH's Strategic Report 2019-2022, it also contributes to achieving the UN Sustainable Development Goals (SDGs), in particular SDG 16 on 'peace, justice and strong institutions'. The HCCH itself is a strong institution, and through its sturdy yet practical legal frameworks, the HCCH contributes to effective peace and justice, to reinforce the rule of law and to provide for effective access to justice. SDG 16 is intertwined with the international legislative process to which the HCCH greatly contributes. Sound and effective multilateralism – that is what the HCCH stands for.

I would like to take this opportunity to renew my sincere thanks to all those who contributed to the successful organisation of the *HCCH a|Bridged Edition 2019* event on 11 December 2019. First, to the Federal Ministry of Justice and Consumer Protection of Germany, which provided a voluntary contribution that enabled us to bring this project to fruition. My thanks as well to our other generous sponsors, Ropes & Gray LLP, and AVEQ Group. At the Permanent Bureau, the 2019 event and this publication were conceptualised and brought to life by Dr Gérardine Goh Escolar (First Secretary), with strong legal and practical support provided by Brody Warren (Attaché to the Secretary General/Senior Legal Officer), Elizabeth Zorrilla (Legal Officer), Raquel Salinas Peixoto (Legal Officer), my colleagues from the administrative team, as well as our interns.

It gives me great pleasure to present to you the *HCCH a|Bridged* publication on the *HCCH 1965 Service Convention in the Era of Electronic and Information Technology* – the first edition of what will hopefully become a series. The HCCH – growing from strength to strength.

Dr Christophe Bernasconi | *Secretary General, HCCH*

TABLE OF CONTENTS



The Prism: The Tech Battle for e-Service

This keynote session examined everything from secure e-mail to electronic submission and transmission platforms; from distributed ledger technology to artificial intelligence. The panellists considered these in the context of a moderated debate of the most appropriate technological solution for end-to-end digitisation of transmission and execution procedures under the HCCH Service Convention. This section contains their written contributions.

EMAIL AS A SECURE MEANS OF TRANSMISSION UNDER THE HCCH SERVICE CONVENTION

BY THEODORE J. FOLKMAN

The security of electronic methods of communication in the operation of the Hague Service Convention has had the attention of experts in private international law for longer than one might think. In 1999, Commission V of the Geneva Round Table, organised by the Permanent Bureau of the Hague Conference on Private International Law, recommended that transmissions between central authorities and transmissions to competent persons under Article 10 "should be carried out by electronic means, provided they meet [certain] security requirements," namely, that the message should be confidential, that the message should reach its recipient without being broken up or altered, that the sender should be provably identifiable, that the dates of dispatch and receipt should be provable, and that the system for transmission should be operational at all times.[1] At its most recent meeting, the Special Commission encouraged the use of electronic means to transmit and receive requests for service and recommended that states "consider security matters when evaluating methods of electronic transmission."[2] And the Practical Handbook points out that the "greatest concerns" in the use of email as a method of service of process are security concerns: "typically messages sent via a normal e-mail service are unencrypted, may be intercepted by third parties, and can be modified because there is no digital signature to guarantee their inalterability."[3]

There has, however, been only lacklustre progress towards the widespread use of electronic methods of communication in connection with the Convention, in part because of continuing concerns about the security of these methods. The purpose of this paper is to suggest how central authorities may consider the question of whether or not to adopt e-mail for use in transmitting and receiving documents to and from other central authorities.

The approach of the paper is non-technical. We begin with an overview of what we mean by security.[4] We illustrate key security concepts using the example of postal mail—a traditional method of transmitting documents that is universally accepted. Then we turn to the security of email. We canvass the available technologies for securing email but note the low rate of adoption of some of them. And we compare the security available using email with the security of postal mail.

---

1 See C. Kessedjian, "Electronic data interchange, internet and electronic commerce", Prel. Doc. No 7 of April 2000 drawn up for the attention of the Special Commission of May 2000 on General Affairs and Policy of the Hague Conference, The Hague, 2000 para 5.2.

2 See "Conclusions and Recommendations of the Special Commission on the practical operations of the *HCCH Conventions of 15 November 1965 on Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (20-23 May 2014), of *18 March 1970 on Taking of Evidence Abroad in Civil or Commercial Matters* and of *25 October 1980 on International Access to Justice*", available on the HCCH website at: < https://assets.hcch.net/docs/eb709b9a-5692-4cc8-a660-e406bc6075c2.pdf >.

3 Permanent Bureau of the HCCH, *Practical Handbook on the Operation of the Service Convention*, 4th Edition, The Hague, 2016, Annex 8, p. 79.

4 In principle it would be better to begin with a threat model—a discussion of the threats that central authorities might seek to protect themselves against. See P Ohm, "Sensitive information", *Southern California Law Review*, vol. 88, 2015, at p. 1125, 1172-73 (discussing "threat modeling"). Here, though, we simply assume that central authorities are interested in the aspects of security referenced in Commission V's report.

The paper ends with a practical suggestion. Even given the low adoption rate of many key security technologies, it would be reasonable for central authorities to begin experimenting with the use of email in the transmission of documents. The paper concludes with suggestions for ways the Permanent Bureau could facilitate the move towards email.

I. Defining Security

Because we are concerned with communication of information, we look to the field of information security to define "security." The Internet Engineering Task Force, the leading Internet standards body, defines three important elements of security. First, *authenticity.* An "authentication service" is a "security service that verifies an identity claimed by or for an entity, be it a process, computer system, or person."[5] Authentication includes "verifying that the entity performing an operation is who it claims to be."[6] This is a restatement, in technical language, of what Commission V called the requirement "to *identify* beyond doubt the sender of the message."[7]

Second, *confidentiality.* A "data confidentiality service," according to the IETF, is "a security service that protects data against unauthorized disclosure to unauthorized individuals or processes."[8] According to Commission V, "confidentiality" means ensuring, "through cryptographic or other methods, that the message sent cannot be intercepted by another person."[9] "Interception" can have the connotation of unauthorized taking of a message while in transit,[10] but we shall see that an issue also arises about the confidentiality of data after transmission is complete.

Third, *integrity.* A "data integrity service" is a service "that protects against unauthorized changes to data, including both intentional change (including destruction) and accidental change (including loss), by ensuring that changes to data are detectable."[11] Commission V divided integrity into two concepts: what it called "integrity" (ensuring "that the message is not broken up in the course of dispatch"), and "inalterability" (ensuring "that no change can be made to the message, either by the addressee or by any other person").[12] But the basic concept is the same.

While there is not universal definition of "security" and there are additional concepts (*e.g.*, availability)[13] that are often considered to be components of security, for purposes of this paper, we measure the security of a communications technology by considering whether it guarantees the authenticity, confidentiality, and integrity of the message. We also limit the scope of our discussion by focusing on security *in transit.* That is, we are concerned here with the security of the *transmission,* not the security of the data once received. In other words, we assume, almost certainly incorrectly, that central authorities have perfect control of their computer servers and that their servers have no security vulnerabilities.

---

5 RFC 3365 3 (2002).

6 *Id.*

7 C. Kessedjian, *op. cit.* note 1, at para. 5.2.

8 RFC 3365, *supra* note 5, at 3.

9 C. Kessedjian, *op. cit.* note 1, at para. 5.2.

10 *Merriam-Webster's Collegiate Dictionary*, (11th ed.).

11 RFC 3365, *supra* note 5, at 3.

12 C. Kessedjian, *op. cit.* note 1, at para. 5.2.

13 M. Lachniet, *From the Perspective of a Computer Security Consultant,* 7.

II. The Security of Ordinary Postal Mail

To set the stage, we start with the security of old-fashioned postal mail. Most transmissions between central authorities today take place via post, and the post is a universally accepted method of transmission. So it is sensible to ask just how secure transmission by post really is, and it is not sensible to rule out email as a method of transmission unless it can be shown to be perfectly secure rather than just about as secure as the post.

Suppose you are an official in the Ministry of Justice of your country, which is designated as the country's central authority. You receive an envelope containing a writ of summons, a complaint, and a request for service on the Hague Conference's model form. How do you determine that the documents are what they purport to be? How do you determine, in other words, that they are authentic?

The documents may bear some *intrinsic* indicia of authenticity. The writ, for example, may bear a raised seal or the signature of a court official. You probably also are familiar with how a writ originating in the country at issue should look from prior experience. But these are relatively weak guaranties of authenticity. Someone with the right resources and motivations could forge such a document rather convincingly.

You might also look at the envelope. The postmark provides evidence of the place of mailing, which could provide some evidence that the documents are what they purport to be. A summons purporting to be from the U.S. District Court for the Southern District of New York but mailed from Toronto might raise questions. The envelope might also have a franking mark indicating that it is official mail, which, again, could be faked by a suitably motivated wrongdoer.[14]

Thus while the documents themselves and their envelope may provide some evidence of their own authenticity, the guarantee of evidence is not particularly strong.

You may also look to *extrinsic* evidence to establish authenticity. Perhaps the courts in the relevant country make their court dockets publicly available, and you can simply compare the documents you received with the copies of the documents available online on the foreign court's website. Or perhaps you can call your counterpart at the central authority of the sending country and ask for verification that the documents are what they purport to be. Such extrinsic evidence provides much stronger—though not perfect—guarantees of authenticity. But note that these methods of authentication are available no matter what technology is used to transmit the documents. As a practical matter, we are much more interested in guarantees of authenticity that do not require such "out-of-band" verification, because the basic reason for interest in using electronic technologies to transmit judicial documents is to make the process quicker and more efficient.

Similar considerations apply to the question of the integrity of documents received through the post. The document might have features meant to make it difficult to tamper with it, and it may be difficult to tamper with a document in an undetectable way. But these are relatively weak physical protections, and a serious adversary can tamper with a document just as easily as he might forge the document altogether. Out-of-band methods of verifying that a document has not been altered are available, but they are at odds with the goal of a quick and efficient system of document transmission.

---

[14] Subject, however, to criminal penalties. See, *e.g.*, 18 U.S.C. § 1719.

The confidentiality of postal mail must be considered separately. We must consider two problems. First, how can you know that no one has opened the envelope, read the document, and resealed the envelope in transmission? Second, can you protect the contents of the document against an eavesdropper even if he does open the envelope—for example, by enciphering the documents?

The most secure forms of mailing provide some methods for detecting an opened envelope. For example, United States registered mail features postmarks placed over the flaps of the envelope, to make it easier to detect when an envelope has been opened.[15] We should take it as given that a serious adversary could defeat such measures. But in any case, international mail can be opened, even without a warrant, by customs officials.[16]

It is possible, of course, to encrypt the contents of the documents contained within the envelope, and as we will see, modern methods of encryption are indeed highly secure. But as a practical matter, encryption of the content of paper documents would be completely impractical.

III. Public Key Encryption and PKI

Email is insecure in every respect without the adoption of additional technologies. An email message is a plain text message that is not encrypted by default. Even when it is encrypted in transmission, emails likely pass through many routers and other servers as they wend their way from the sender's computer to the recipient's computer, and it is decrypted when it reaches each computer on its route. Most obviously, the email is decrypted on the computers controlled by the sender's and recipient's email service providers.

Email does not guarantee the authenticity of messages or guarantee their authenticity by default. A sender can put any email address in the "From" field in the header of his message. Any of the computers on the route between sender and receiver can alter a message before forwarding it to the next server on the route.

To solve such problems, modern email systems make use of public key encryption. In public key encryption, each user has a *public* key, which can be freely distributed to the public, and a *private* key, which must be kept private. The keys are related mathematically to each other in a way that we will not describe here. A message may be encrypted using the desired recipient's public key, and only a person in possession of the corresponding private key will be able to decrypt it. Similarly, a message may be signed using the sender's private key, and anyone with the corresponding public key will be able to verify the signature. The important features of the system are that a message encrypted with a public key can be decrypted only with the private key (and, correspondingly, that a message signed with a private key can be verified with the public key), and that it is infeasible using present technology to derive the private key from the public key.[17]

---

15 See *International Mail Manual,* 334.2.

16 See 19 U.S.C. § 1583.

17 See Emerging Technology from the arXiv (2019), "How a quantum computer could break 2048-bit RSA encryption in 8 hours", *MIT Technology Review*, available at: <https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/> (May 2019) (noting the "huge amount of time it would take for a classical computer" to decrypt a typical encrypted message, but noting the risks posed by new quantum computers).

Perhaps the main difficulty in implementing public key cryptography solutions is the problem of key distribution. How can a sender be sure that the public key she uses to encrypt belongs to the recipient? How can a recipient be sure that the public key he uses to verify a signature belongs to the person whose name is attached to it?

In practice the main approach to solving the key distribution problem is known as PKI (public key infrastructure). In PKI, public keys are signed by trusted certificate authorities. The trusted certificate authority signs the certificate only if it has taken defined steps to confirm that the public key belongs to the person whose name and email address is associated with it. The recipient verifies the certificate authority's signature using the certificate authority's public key.[18] The signature is created by using the private key to encrypt a "hash," or number uniquely representing the contents of the message. After decryption, the recipient can compare the hash to the message to determine whether the message has been altered since signature. The Hague Conference has familiarity with PKI; the technology can be used to guarantee the authenticity of e-apostilles.[19]

In order to understand how PKI can be used to secure email, it is necessary to understand the basics of the Domain Name System, or DNS. The DNS is a distributed database whose basic function is to allow a computer, called the client, to provide a domain name (for example, "www.hcch.net") to another computer, called the server, and to receive back from the server the IP address that corresponds to the domain name, so that the client can communicate with the desired computer. But in principle the DNS can be used to store arbitrary information, not just IP addresses. Several technologies now use the DNS to provide authentication and integrity protection to emails. For example, DKIM (DomainKeys Identified Mail) allows an email sender to publish a public key in the DNS and to sign an email using the associated private key. The recipient can verify the signature by retrieving the public key from the DNS and using it to verify the signature as described above. DKIM provides some assurance of authenticity, because it shows that the sender, who has used a certain email address in the "FROM" line of the email, has control of the domain name in the email address. So, for example, if I send an email to you that appears to be from "news@hcch.net," and if the email contains a DKIM signature, your computer can query the DNS and obtain the public key that the administrator of the hcch.net domain name has published. You can use that key to verify the signature, which shows that I am not simply pretending to be associated with hcch.net. [20]

Confidentiality is more difficult. The entirety of an email message cannot be encrypted, because if the header (which contains the "TO" address) is encrypted, the email service provider will not have sufficient information to get the email to where it is intended to go. The message body can be encrypted using public key cryptography as described above, and it is possible for senders to publish their public encryption keys in the DNS.[21] Many email clients, however, do not provide a user-friendly way to encrypt or decrypt message contents.

---

18 See generally S. Y. Chow, "Conceptions of Privacy and Security in a Digital World", in S. Y. Chow (ed.), *Data Security and Privacy in Massachusetts,* § 1.3.4 (2d ed. 2018).

19 See C. Bernasconi and R. Hansberger, "*Memorandum on Some of the Technical Aspects Underlying the Suggested Model for the Issuance of Electronic Apostilles (E-Apostilles)*", Prel. Doc. No 18 of March 2007 for the attention of the Council of April 2007 on General Affairs and Policy of the Conference (available on the HCCH website at: <https://assets.hcch.net/upload/wop/genaff_pd18e2007.pdf>.

20 See generally D. Crocker *et al.* (eds.), *Domain Keys Identified Mail (DKIM) Signatures,* RFC 6376 (2011). Typically sophisticated email services also make use of a second authenticating technology, Sender Policy Framework, or SPF, which is not discussed here.

21 See generally S. Josefsson, *Storing Certificates in the Domain Name System (DNS),* RFC 4398 (2006).

These technologies face some challenges. For example, can one be sure that the answer to a DNS query is itself authentic? Answers to such queries can themselves be cryptographically signed using a technology known as DNSSEC, and the public keys used to verify the signatures stored higher in the DNS hierarchy.[22] Thus, for example, the owner of the "hcch.net" domain could cryptographically sign DNS responses and arrange to have the public key stored in the ".net" top-level domain. DNS responses served by ".net," in turn, can be cryptographically signed and the public key stored in the ".", or root, domain. The root domain public key is built into most modern computer systems, allowing a user to verify the results of a DNS query cryptographically. But DNSSEC has a low rate of adoption, both in the sense that relatively few domain names are cryptographically signed and in the sense that not all DNS resolvers validate DNSSEC signatures.[23]

A similar problem exists with public key cryptography used to encrypt the contents of email messages. There is no universal PKI infrastructure commonly in use for the distribution of public keys used for encryption. [24] The most widely used method of exchanging keys is via the "web of trust" or via manual verification of the key's "fingerprint" or cryptographic hash. Keys can be distributed via the DNS, just like DKIM keys, but that method is "not a replacement for verifying … public keys via the 'web of trust' signatures, or manually via a fingerprint verification."[25] (One reason the use of DKIM is not a substitute is that a domain's DNS data are controlled by the person or entity that controls the domain name, while a key used for encryption is typically controlled by an individual email user). But neither the "web of trust" nor manual verification is an easily scalable answer, nor could one expect a typical email user to understand how to use the "web of trust," how to verify a hash, or how to publish a certificate to the DNS.

IV. A Brief Comparison

As this discussion makes clear, *when fully implemented,* public key cryptography and PKI provide very strong, mathematically demonstrable, security. With DKIM and DNSSEC properly implemented, an email recipient can have confidence that the email she receives was sent from the domain indicated in the "FROM" line and was not changed in transit. Assuming a solution to the key distribution problem and to the usability problems identified above, a message can be encrypted end-to-end, and the recipient can have confidence that only the people with access to his private key can decrypt it. However, the technologies are not simple to use and are not universally, or in some cases even widely, deployed. A security-conscious institution considering the use of email for secure communications must weigh the trade-offs. For example, DKIM is widely adopted but DNSSEC is not. Is the assurance of authenticity and integrity that DKIM provides enough in practice to meet the institution's needs, even if the possibility of "DNS spoofing" that DNSSEC is meant to avoid still exists?

---

22 See generally. Arends *et al., DNS Security Introduction and Requirements,* RFC 4033 (2005).

23 See T. Chung, *Why DNSSEC Deployment Remains So Low,* APNIC, available at: < https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/ > (Dec. 6, 2017) and D. Satola & H. L. Judy, "Towards a dynamic approach to enhancing international cooperation and collaboration in cybersecurity legal frameworks: Reflections on the proceedings of the workshop on cybersecurity legal issues at the 2010 United Nations internet governance forum", *William Mitchell Law Review,* Vol 37, 2011, p 1745, 1756 ("the rate of adoption has not been as rapid as one might ideally want").

24 P. Wouters, *DNS-Based Authentication of Named Entities (DANE) Bindings for Open PGP,* RFC 7929, § 1 (2016) (describing existing methods of key distribution).

25 *Id.*

In contrast, the postal mail has widely available and easy-to-use security features, but while they provide some security, they do not provide the demonstrably robust security that modern cryptography can provide. Again, the question is one of reasonableness. A security-conscious institution wondering whether to use email for secure communications must ask about the trade-off between widely-adopted but weak *physical* protections and poorly-adopted but strong *cryptographic* protections.

V. Recommendations

In light of the HCCH's strategic goal of "ensuring the … efficient implementation and operation of the HCCH's Conventions … through post-Convention services and assistance,"[26] which includes providing technical advice and in some cases even technical infrastructure,[27] now is the time for the HCCH to work towards making the use of email as a means of transmission under the Service Convention feasible for central authorities.

The HCCH could take some low-cost steps in this direction. It could, for example, provide training to central authorities about how to enable the security features discussed above, and explanations of what these features do and do not guarantee and how to use them properly. It could, in future Conclusions & Recommendations or in another appropriate form, remind central authorities that the Service Convention is technology-neutral, and it could actively encourage email adoption in order to interest states that themselves have an interest in maintaining best practices or in being leaders in the field.

The HCCH could also choose to take more robust, and more costly, steps. For example, the HCCH could itself operate a PKI infrastructure, issuing and certifying keys to central authorities that could be used both for authentication/integrity protection and for encryption of the contents of messages. There are significant hurdles to overcome before obtaining the trust of the major commercial web browsers and being able to act as a "root" authority.[28] A well-known and now highly-successful certificate authority, Let's Encrypt, was able to begin issuing keys before solving that problem by arranging with an established certificate authority to have its keys "cross-signed."[29] It would, however, be prudent to undertake a serious cost-benefit analysis before taking such steps.

---

26 HCCH *Strategic Plan 2019-2022,* available at: < https://assets.hcch.net/docs/bb7129a9-abee-46c9-ab65-7da398e51856.pdf > at 5.

27 *Id.*

28 See, *e.g., Mozilla Root Store Policy,* v. 2.7, available at: < https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/ > (describing process for certification by Mozilla, the publisher of Firefox).

29 See J. Aas, *Transitioning to ISRG's Root,* available at: < https://letsencrypt.org/2019/04/15/transitioning-to-isrg-root.html >.

USE OF AN ELECTRONIC PLATFORM FOR COMMUNICATION AND TRANSMISSION BETWEEN CENTRAL AUTHORITIES IN THE OPERATION OF THE HCCH SERVICE CONVENTION

BY KATERINA V. OSSENOVA [*]

As one of the most widely used Hague Conference on private international law (Hague Conference or HCCH) instruments, the *Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (Service Convention or Convention) continues to be a critical resource in facilitating service on foreign defendants and promoting access to justice. However, while the Convention is technology-neutral in its current form, its usefulness and applicability in the future depends on the embrace of modern technology. The Conclusions and Recommendations of the Special Commission on the practical operation of The Hague Apostille, Evidence and Service Conventions in 2003 emphasized the need to embrace technical developments and acknowledged that modern technologies are an integral part of life today.[30] Specifically, the Special Commission recommended that States explore ways to use modern technology to further the operation of the Service Convention, especially in regard to the electronic transmission of requests.[31]

The United States Department of Justice's Office of International Judicial Assistance (OIJA), which serves as the U.S. Central Authority for incoming requests pursuant to the Service Convention, welcomes the use of electronic and information technology in the operation of the Service Convention. Most importantly, OIJA supports the application of electronic and information technology in the transmission of requests for service and in order to facilitate communication between Central Authorities. The increased use of electronic and information technology will have a fundamental impact on the evolution of the Convention and ensure its usefulness and relevancy in the future.[32] Electronic transmission of requests may result in a number of improvements, such as: (1) modernizing the operability of the Service Convention; (2) reducing costs for Contracting States; (3) speeding up the execution of requests; (4) promoting efficiency; (5) facilitating communication between Central Authorities; and (6) improving secure transmission of documents.[33]

---

[*] Trial Attorney, Office of International Judicial Assistance, Office of Foreign Litigation, U.S. Department of Justice.

[30] "Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Apostille, Evidence and Service Conventions" (HCCH 2003) 3, 4, available at: < https://assets.hcch.net/docs/0edbc4f7-675b-4b7b-8e1c-2c1998655a3e.pdf > (2003 Conclusions). See also Permanent Bureau, "Conclusions and Recommendations of the Special Commission on the practical operation of The Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions" (HCCH 2009) 8, 39, available at: < https://assets.hcch.net/upload/wop/jac_concl_e.pdf >.

[31] 2003 Conclusions 11, 59, 62 (n 1). See also "Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Service, Evidence and Access to Justice Conventions" (HCCH 2014) 5, 39, available at: < https://assets.hcch.net/upload/wop/2014/2014sc_concl_en.pdf >.

[32] Permanent Bureau of the HCCH, *Practical Handbook on the Operation of the Service Convention*, 4th ed., The Hague, 2016, at p. 171. Available at: < https://www.hcch.net/en/publications-and-studies/details4/?pid=2728&dtid=3 > (Service Handbook).

[33] "Use of Information Technology in the Transmission of Requests under the Service and Evidence Conventions", Prel. Doc. No 9 of January 2019 for the attention of the Council on General Affairs and Policy of the Hague Conference, p. 2.

Recently, the Counsel on General Affairs and Policy of the Hague Conference in March 2019 mandated that the Permanent Bureau conduct work on developing an electronic system to "support and improve the operation of both the Service and Evidence Conventions."[34] Among the issues to be examined is what kind of international system for electronic transmission of requests could be developed.[35] While there are a few technological options for electronic transmission of requests – such as secure email and distributed ledger technology – the one I will consider here is a common electronic platform.

The HCCH defines a common electronic platform or an electronic case management system as "a system that enables casework and related workflows to be followed and managed through electronic communication of information between the individuals concerned (incl. staff, as well as parties and their representatives in some cases)."[36] A common electronic platform would be one case management system to be used by all Contracting Parties in the operation of the Service Convention. Practically speaking, a common electronic platform would allow for the submission of requests electronically from a Competent Forwarding Authority in the Requesting State to the Central Authority or Competent Authority in the Requested State.[37]

The use of such a system to transmit requests abroad would result in a number of improvements in the operation of the Service Convention. While the platform would need to be developed or tailored to the needs of the Contracting States and may be subject to a number of limitations, potential benefits could include the ability to: (1) transmit electronically all correspondence and proofs of service and the certificate through the platform; (2) correct defects before resorting to rejecting requests; (3) make payment, if applicable, directly through the platform; (4) communicate directly with all Central Authorities; (5) have a secure place to pose questions to Central Authorities and initiate a blog about news and developments in regard to service abroad or the Convention that would be of interest to all Contracting States; (6) fill out the latest version of the Hague Convention Model Form online; (7) track the status of requests online; and (8) produce reports/statistics/data as needed and make this information accessible to all Contracting States.[38]

The most important benefits of using a common electronic platform for transmission of requests pursuant to the Service Convention would be to establish standardized and consistent procedures among Contracting States, promote communication between Central Authorities, establish best practices and guidelines for Contracting States, including States who recently acceded to the Convention, and establish a mechanism for increased accountability by Contracting States in their fulfillment of Convention obligations. One of the most difficult aspects in the operation of the Service Convention is the lack of detailed information from Central Authorities on their Practical Information web pages and lack of communication or responses from Central Authorities.[39] A common electronic platform will help bridge this gap of information and facilitate and encourage communication among

---

34 See "Conclusions & Recommendations Adopted by Council" (HCCH 2019) 6, 40. Available at: < https://assets.hcch.net/docs/c4af61a8-d8bf-400e-9deb-afcd87ab4a56.pdf >.

35 *Id.*

36 Questionnaire on the Use of Information Technology in the Operation of the Evidence Convention, September 2019, Question 1.13.

37 Prel. Doc. 9, *op cit.* note 33, p. 3.

38 *Id.*, p. 5.

39 See Permanent Bureau, "Authorities" (HCCH), available at: < https://www.hcch.net/en/instruments/conventions/authorities1/?cid=17 > (last consulted on 10 April 2020). See also Service Handbook 172, 17.

Central Authorities.[40] This improvement alone would positively impact the efficiency and effectiveness of the Service Convention.

However, while the benefits of using a common electronic platform for management and transmission of requests pursuant to the Convention seem enticing, this technological option is not without challenges.

In order to address the complexity of using a common electronic platform in the transmission of requests under the Convention, it would be helpful to explain how the United States implements the Convention. As noted, OIJA serves as the U.S. Central Authority for incoming requests pursuant to the Service Convention. Executive Order 11471, Section 1, May 28, 1969, designates the U.S. Department of Justice as one of the departments to perform the functions required from the Central Authority for the Service Convention[41] and the Code of Federal Regulations, Title 28, § 0.49 on international judicial assistance, authorizes the Assistant Attorney General in charge of the U.S. Department of Justice's Civil Division to direct and supervise the functions of the Central Authority for the Service Convention.[42] OIJA also serves as the U.S. Central Authority for incoming requests for international judicial assistance in civil or commercial matters pursuant to the Hague Evidence Convention,[43] the Additional Protocol to the Inter-American Convention on Letters Rogatory, and service and evidence requests from non-Convention states received through diplomatic channels. After the Service Convention entered into force in the United States in February 1969, requests transmitted pursuant to the Service Convention were processed by OIJA and referred to U.S. Marshals Service for execution. In April 1970, the U.S. Marshals imposed a $15.00 fee for execution of a Service Convention requests. As the number of members who acceded to the Convention grew over time and as the number of requests transmitted to the United States increased in volume, it became untenable for OIJA and the U.S. Marshals Service to continue processing these requests for service.

Article 5 of the Convention instructs that a "Central Authority of the State addressed shall itself serve the document or shall arrange to have it served by an appropriate agency"[44] and Executive Order 11471 allows for additional designations.[45] In the United States, service of judicial documents is governed by the Federal Rules of Civil Procedure (FRCP), or applicable state law. FRCP 4(c) on service of a summons dictates that "any person who is at least 18 years old and not a party may serve a summons and complaint."[46] FRCP 4(c) also directs that the "plaintiff is responsible for having the summons and complaint served" and FRCP 4(e) directs that one of the main methods of service is by "delivering a copy of the summons and of the complaint to the individual personally."[47] In the United States, therefore, service of a summons and complaint is typically carried out by private process servers through personal service.

---

40 Service Handbook 174, 23.

41 Exec. Order No. 11,471, 34 Fed. Reg. 8349 (1966-1970), available at: < https://www.archives.gov/federal-register/codification/executive-order/11471.html > (last consulted on 10 April 2020).

42 28 C.F.R. § 0.49 (1973), available at: < https://www.ecfr.gov/cgi-bin/text-idx?SID=9b8fdccf3a1b66dcb59ec6c7942a0eec&mc=true&node=se28.1.0_149&rgn=div8 >.

43 The *HCCH Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*.

44 *Convention of 5 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* at art. 5, 20. U.S.T. 361, 658 U.N.T.S. 163, T.I.A.S. No. 6638, available at: < https://www.hcch.net/en/instruments/conventions/full-text/?cid=17 >.

45 Exec. Order No. 11,471 (n 8).

46 *Fed. R. Civ. P.* 4(c), available at < https://uscode.house.gov/view.xhtml?path=/prelim@title28/title28a/node87&edition=prelim >.

47 *Fed. R. Civ. P.* 4(c)-(e) (n 10).

In July 2003, the United States notified the Ministry of Foreign Affairs of the Kingdom of the Netherlands, as depositary for the Service Convention, that it was changing the way judicial assistance under the Convention is afforded to foreign tribunals and to litigants before such tribunals.[48] Specifically, the U.S. Central Authority informed the Ministry that it was assigning the service function to a private contractor, a process server who would execute the requests for service on private individuals and companies.[49] This procedural change did not imply the formal designation of a new Central Authority for the Service Convention but reflected the outsourcing of certain activities conducted by the Central Authority, which formally remains the U.S. Department of Justice. Through a public competitive bidding process, the exclusive contract to carry out the service function was awarded to *ABC Legal Services*, a process server company headquartered in Seattle, Washington.[50] ABC Legal remains OIJA's designated contractor for all requests for service on private individuals and companies received pursuant to the Service Convention, the Inter-American Convention on Letters Rogatory and Additional Protocol, and letters rogatory received through diplomatic channels.[51] Requests for service on the United States Government itself, which includes its officials (when named in an official capacity), departments, agencies, or instrumentalities are sent directly to OIJA.

ABC Legal receives requests for service pursuant to the Service Convention directly from foreign applicants. Requests are typically mailed in hard copy to ABC Legal's offices and must be accompanied by a $95.00 fee. ABC Legal mails back any proof of service, related correspondence, and original documents back to the foreign applicant once the request is resolved. OIJA follows a similar process for requests on the United States Government.[52]

The number of requests transmitted to ABC Legal under the Convention has steadily increased every year. In 2018, ABC Legal received over 8,000 requests for service in their capacity as DOJ's contractor. That number jumped to over 9,000 incoming requests in 2019. ABC Legal has accepted requests for service transmitted online, but since 2019, they have revamped their website and processes to encourage requests to be emailed or uploaded online, subject to size and formatting limitations.[53] Currently, any Service Convention request can be uploaded on ABC Legal's website, enabling the applicant to make the payment online, track the status of their request, and download the proof of service.[54] Foreign applicants are increasingly submitting Service Convention requests electronically to ABC Legal. In the latest available data, ABC Legal received the following number of requests electronically, largely from the following countries:

---

48 Treaty Database, "Convention on the service abroad of judicial and extrajudicial documents in civil or commercial matters" (Verheid.nl), available at: < https://treatydatabase.overheid.nl/en/verdrag/details/004235_b#United States of America > (last consulted on 10 April 2020).

49 *Id.*

50 ABC Legal, "Overview" available at: < https://www.abclegal.com/international-service-of-process > (last consulted on 10 April 2020).

51 Permanent Bureau, "Declarations/Reservation/Notification" (HCCH 28 January 2020), available at: < https://www.hcch.net/en/instruments/conventions/status-table/notifications/?csid=428&disp=resdn > (last consulted on 10 April 2020).

52 Office of International Judicial Assistance, "Service Requests" (United States Department of Justice 6 April 2020), available at: < https://www.justice.gov/civil/service-requests > (last consulted on 10 April 2020).

53 ABC Legal, "Frequently Asked Questions", available at: < https://www.abclegal.com/international-service-of-process/faq > (last consulted on 10 April 2020).

54 ABC Legal, "Hague Service Convention", available at: < https://www.abclegal.com/international-service-of-process/hague-service-convention > (last consulted on 10 April 2020).

- 2016: 101 online submissions, mostly from France, Germany, and China
- 2017: 748 online submissions, mostly from France, Vietnam, and Canada
- 2018: 991 online submissions, mostly from France, Canada, and Vietnam
- 2019: 1911 online submissions, mostly from Brazil, France, and Canada.

It is important to add that in the United States, outgoing requests pursuant to the Service Convention are transmitted abroad directly by persons and entities within the United States competent to forward service requests, such as any court official, any attorney, or any other person or entity authorized by the rules of the court. As such, outgoing requests for service pursuant to the Convention are not transmitted abroad through OIJA or its contractor, but directly from a Competent Authority in the United States to the Central or Competent Authority of the Requested State.

How the United States implements the Service Convention domestically demonstrates a fundamental challenge on the use of a common electronic platform, namely the issue of access. When Contracting States require all outgoing and incoming requests to be sent through their Central Authorities only that State's Central Authority would have access to the platform. This will allow the Central Authority to transmit requests abroad to other Central Authorities but also to receive incoming requests. However, for States that allow other Competent Authorities to transmit requests abroad, the number of entities who require access to the platform increases. In addition, when those Competent Authorities include private sector entities – such as process servers, attorneys, or *huissiers* – the access issue also concerns private versus public sector access to the platform.[55] In a likely scenario, a *huissier* in France would need to have access to the platform to transmit a request to ABC Legal in the United States and ABC Legal would need to have access to the platform to receive the documents and return subsequent communications. For outgoing requests from the United States to be transmitted abroad, access to the platform would need to be provided to any Competent Authority in the United States, which would include thousands of attorneys, clerks of court, and process servers. While a common electronic platform would be beneficial for Central Authorities in the operation of the Convention, who has access to the platform and striking a balance between public and private sector access to the platform remains a key question.[56]

Use of a common electronic platform means that documents are prepared electronically and submitted electronically through the platform.[57] However, an additional challenge exists since documents in many countries would still need to be printed by the Requested State's Central Authority. Although service by email is certainly a method of service that is gaining traction, in many countries, including in the United States, personal service remains the preferred method of service.[58] Currently, ABC Legal's sole method of service for Service Convention requests is through personal service, which requires hard copy documents to be personally served on the individual. When requests are submitted electronically, ABC Legal still needs to print a complete set of the documents, which are then mailed to the process server who will personally serve them on the intended individual. Issues to consider are formatting considerations and the size and volume of requests. Central Authorities would receive requests for service that may be extremely voluminous and in a variety of formats. The Central Authority would need to undertake the costly and time-consuming task of printing all such submissions if personal service is preferred or required.

---

55 Service Handbook 173, 20.

56 Prel. Doc. No 9, *op cit.* note 33, p. 4.

57 Service Handbook 171, 13.

58 Service Handbook 169, 2. See also Prel. Doc. No 9, *op cit* note 33, p 6.

Other issues related to the use of a common electronic platform include the need for countries to accept and standardize the use of digital/electronic signatures and dispensing with formalities like requiring original documents to be returned with the proof of service. The cost of either building or tailoring an existing electronic case management system could be significant and it is unclear who would be responsible for the initial cost of the system or its maintenance costs. Countries, and governments, vary greatly in terms of their use of technology and ensuing specifications so developing one common system would likely present system operability and compatibility challenges.

Last, but not least, would be security and privacy concerns. Requests for service of judicial and extrajudicial documents often include sensitive and personally identifiable information. Use of a common electronic platform would mean confidential and sensitive information is accessible through one common system. Security would need be paramount to ensure the system is protected against unauthorized access. Ideally, the system would be limited to the most critical users, but as described above, due to how some countries, like the United States, implement the Convention, access to the platform would need to be provided to thousands of potential users. One option would be to have differing levels of access to the system, depending on the nature of the user and whether access to the system was for the purpose of transmitting a request for service or retrieving a submitted request for service.

Privacy issues are also just as critical and concerning if considering a common electronic platform. Use of a system or database by OIJA that stores personal information must comply with the E-Government Act of 2002, the Federal Information Security Management Act, and various other privacy regulations. The European Union's General Data Protection Regulation is one of the toughest privacy and security laws in the world, although many countries are enacting similar laws. Use of a common electronic platform by Central Authorities, and others who would require access, would mandate that the system used satisfies privacy and security laws and regulations around the world.

While there are a number of important benefits Contracting States would gain from the use of a common electronic platform for the transmission of Service Convention requests, the limitations and challenges at this time would surpass the benefits. My recommendation would be to instead prioritize using secure email for transmission of requests and work toward improving communication among Central Authorities.

REFLECTIONS ON THE USE OF DISTRIBUTED LEDGER TECHNOLOGIES FOR THE PURPOSE OF THE HCCH SERVICE CONVENTION

BY EMMA VAN GELDER[*] AND ERLIS THEMELI

It is undeniable that the *Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (the Convention) was and still is very successful. Its success is reflected in the large number of countries that have signed the Convention. Most importantly, it is a success that the time needed to transmit judicial and extrajudicial documents across borders has been reduced thanks to the innovations introduced by the Convention. These innovations have created standardised procedures between Contracting Parties and have provided for the creation of Central Authorities in each jurisdiction which receive and process requests from abroad. In a way, the Convention got rid of the archaic procedures in favour of a more slender and modern procedure. But when it comes to the use of technology, the drafters of the Convention lived in a world where postal services were the only way of transmitting documents. Document transfer innovations were yet to come.

The development of digital technologies and high-speed internet has made the use of paper documents redundant in many situations. Since 1965, when the Convention was concluded, courts have embraced the use of digital technologies to communicate with their users. The use of telephone, fax machines, emails or other cable and wireless communication technologies is common practice in many jurisdictions now. Most importantly the internet has created opportunities to instantly exchange documents across large distances between courts and court users. This raises the question of how the Convention should adapt to the use of new technologies. Which technologies are feasible for the purposes of the Convention? We do not try to analyse all the technologies and their implications for the Convention. This would require a different approach. We identify distributed ledger technology (DLT) as a technology that promises to improve remote communication by increasing certainty about document content and origin. This paper first briefly introduces DLT, then discusses the expected benefits and limitations of DLT and how it can support the operation of the Convention.

I. An overview on the distributed ledger technology

Before delving into DLT, it is important to briefly describe some features of computers and computer networks in order to better highlight the benefits of DLT. Computers are both machines that create and edit digital documents, and storage facilities for such digital information. When drafting documents, most computers would place a digital marker on the file which may allow readers and other users to trace the author or subsequent editors of the document. While this feature is useful, it can be easily manipulated, and it is not often used to trace changes and authorship of documents. To overcome this, electronic signatures or document encryption are commonly used. Electronic signatures guarantee that the author of the document is the one that signs the document and that no other changes have been made subsequently. While electronic signatures solve the issue of the document's authorship, achieving a significant level of document integrity may be difficult to achieve.

[*] PhD candidate at the Erasmus Graduate School of Law, Erasmus University Rotterdam.

When computers are connected in a network, they can send and receive documents between each other. A network may allow users to access information in any of the computers part of it, or it may allow non-network members to access certain documents or information stored in it. A classic example of this is the network of computers in an office. They allow colleagues to work and share work in a safe environment without fear of outside interferences. These networks often are connected to the World Wide Web – a network of networks that creates the internet – which may allow external parties to access them. Large networks require servers to regulate network access, communication, and information traffic. In addition to their regulatory role, servers store data about the network or data that network participants decide to upload there.

Network participants rely on the security of each other's server for the integrity of the information shared and the identity of the person that last edited the information. Many go by the maxim "*I trust the information stored in one server if I trust that server.*" Several solutions are used by server administrators to secure access and stored data, as well as the identity of the persons that accessed or edited the data. However, information stored in servers is vulnerable to attacks from hackers and ill-intentioned network participants. When it comes to the service of judicial or extrajudicial documents abroad, trust between Central Authorities, identity of the authors and editors of the document, and document integrity are of vital importance. If any of these three values is compromised, the service of process will be compromised as well. Distributed ledger technologies may increase document security and traceability, and as a result may be a solution to improve communications security in the digital world.

Distributed ledger are technologies that share the same database among all network participants. Participants are known as *nodes*, while the databases are referred to as the *ledgers*. Nodes maintain a consensus protocol which verifies and approves changes to the ledgers. A ledger can be changed only if all the nodes have approved the change, or in some cases if the majority of the nodes have approved it. This step does not require human intervention, it happens automatically for every node if the protocol has been respected. If consensus between nodes has been reached, the ledger is changed within all nodes. The creators of the network or its participants can approve new participants as nodes. These are known as *permissioned DLT*, and often the participants in these networks know each other. Networks where anyone can be a node and frequently users do not know each other's identity, are referred to as *permissionless DLT* (or public DLT). One type of permissionless DLT is blockchain, which is the technology that gave rise to cryptocurrencies. The term derives from the fact that the data is stored within 'blocks' and each block is cryptographically linked with a hash function to the other block, forming a 'chain'.

There are several benefits, but also drawbacks, of DLT over centralized databases. First, in DLT information is stored among its nodes, which means that information must be changed in all the nodes (or in many) to take effect. By comparison, it is sufficient for a hacker to enter a centralised network to change the information. This quality of DLT offers security.

Second, the scattered nature of the ledgers can cause undetectable breaches in the system. In centralised databases, an administrator oversees access to the server and monitors attempts to breach it, thus running a security protocol. In DLT networks, hackers may target a single node without any of the participants noticing it. And while hackers may not alter the ledger, they may read or copy its content. On the one hand this is a positive characteristic because it makes documents saved in DLT immutable, on the other it makes it prone to system breaches. One way to solve this would be to implement cryptographic security systems as part of the DLT, which brings us to the third point.

Third, DLT may upgrade its security protocols by using cryptographic techniques to maintain the security of the database. Cryptographic security, however, requires a considerable amount of computational power and therefore of energy. For example, blockchains used to maintain the bitcoin network are considered to use one percent of the world's energy consumption.[59]

Fourth, data can be broken into chunks that are stored encrypted at different nodes. This renders hacking and changing the document impossible, because the hacker would need to change all the ledgers in all the nodes to change the document. As accessing the node and then breaking the encryption of the ledger is a difficult task in itself, doing so for every ledger is impossible. Yet, a well organised hacker may attempt to create several nodes in a system in order to fraudulently reach a consensus in his or her favour. Such tactics are, however, not possible in permissioned DLT and hard to achieve in permissionless DLT. Nevertheless, this has only been a theoretical possibility so far.

II. Distributed ledger technology and public institutions: some examples

The use of distributed ledger technologies is nothing new for public institutions. This section provides some examples of such uses which may serve as inspiration for using DLT to modernize the operation of the Convention. Since 2008, the government of Estonia has been experimenting with DLT in order to improve its e-government services.[60] The citizens' personal healthcare, judicial and financial data, and also corporate data, are encrypted and saved on digital ledgers which can be accessed and edited by authorised public officials or concerned members of the public. This system offers several benefits.

First, the data is stored in a safe manner. Hence, the data are encrypted, which makes it difficult for unauthorised people to read it. Also, the data are distributed among nodes, which makes it difficult for unauthorised people to access and acquire it in the first place. Second, DLT allows for a detailed tracking of data, their editing and origin. Within the DLT, documents are equipped with a stamp which cannot be altered without the consensus of other nodes. In other words, if a wrongdoer wants to breach the protocol and alter a document, he cannot do it because he cannot get the permission from the other nodes. Third, given the distributed nature of the data, the system can function under constant external attack, unless enough nodes are incapacitated by the attack. The distributed nature of the ledgers is important also for the safekeeping from corruption or digital damage of the data stored. Even if the data is damaged in a node, other nodes serve as backups.

Another example of the use of DLT within a public institution is that of the UK's Food Standards Agency (FSA), who established a Food and Distributed Ledger Technology collaborative group. In 2018, the FSA started using DLT to track the route of meat produced in a cattle slaughterhouse, starting from the slaughterhouse until the consumer.[61] The FSA used DLT as a regulatory tool in order to ensure compliance in the food sector. In general, inspecting the chain of production of the food industry requires many inspections and

---

59 Legislative Budget Board Staff, "Overview of Blockchain and Distributed Ledger Technology for State Government Functions", *Legislative Budget Board Staff Reports* – ID: 4830, (April 2019), available at: < http://www.lbb.state.tx.us/Documents/Publications/Staff_Report/2019/5191_Blockchain_Distributed_Ledger.pdf > (last consulted on 6 March 2020).

60 Tom Macaulay, "How governments around the world are using blockchain" (Computerworld, 19 September 2019), available at: < https://www.computerworld.com/article/3412304/how-governments-around-the-world-are-using-blockchain.html > (last consulted on 6 March 2020).

61 "FSA trials first use of blockchain", available at: < https://www.food.gov.uk/news-alerts/news/fsa-trials-first-use-of-blockchain > (last consulted on 6 March 2020).

collection of results, with DLT this process can be faster and more secure. In this FSA pilot, the type of DLT used was a permissioned DLT, as only the FSA and the slaughterhouse can access it.

The same idea has been raised in Uganda, where the government supports MediConnect to explore the use of DLT to track prescription medicines from manufacturers until it reaches pharmacies and patients, in an effort to combat counterfeit drugs.[62] With DLT, more transparency can be achieved for every transaction within this chain.

Moreover, in China, DLT-based traceability is used on a large-scale. Two Chinese start-ups, Hyperchain and China Xiong'an Group, unveiled a new DLT based platform that tracks donations in order to enhance transparency and accountability within charity organizations in the midst of the COVID-19 outbreak in Wuhan.[63] This traceability enables an accurate storage of relevant records concerning each donation, including cash amounts and materials, and the distribution of these to the right people.

In the United States of America, some states consider the use of DLT to track applications for obtaining construction permits or carrying other communication with the public. In addition, some states intend to use DLT to register property before the land registry office.[64]

These examples illustrate that DLT excels at tracking documents and the contents recorded on them, their creation date, authorship, and editing. As such, DLT does not need intermediary technologies and the exchange of security certificates, while servers do need them. For users, public services that uses DLT offer real-time information about the status and whereabouts of documents and applications, as well as transparency about the integrity of the document.

From these examples we distinguish two ways in which public institutions use DLT. On the one hand, they use DLT to transmit documents in a secure and controlled way. On the other hand, they use the technology to track the whereabouts and integrity of a document. These applications, however, have exposed some issues with the use of DLT for public services. As mentioned earlier, DLT uses a considerable amount of energy to run their complex algorithms. Despite its rapid progress, DLT is still a relatively new technology which requires further research. There are no over-the-counter products. Each country or institution should develop and run its own DLT. This can be costly, and without experienced companies available it can be hard to develop. There is a risk that DLT is only developed in wealthy countries, contributing to the digital divide problem. Digital ledger technology may make legacy technologies obsolete, obliging developers to invest in new equipment compatible with DLT.

---

62 European Pharmaceutical Manufacturer magazine, "Ugandan government to explore use of MediConnect to tackle counterfeit drugs", available at: < https://www.epmmagazine.com/news/ugandan-government-meets-wth/ > (last consulted on 6 March 2020); Anjuman Rahman, "Ugandan president to explore use of blockchain to tackle counterfeit drugs", available at: < https://www.nsmedicaldevices.com/news/uganda-blockchain-counterfeit-drugs/ > (last consulted on 6 March 2020).

63 Ogwu Osaemezu Emmanuel, "Coronavirus: Two Chinese Firms Launch DLT-Based Donations Tracking Platform", available at: < https://btcmanager.com/coronavirus-chinese-firms-dlt-donations-tracking-platform/?q=/coronavirus-chinese-firms-dlt-donations-tracking-platform/& > (last consulted on 6 March 2020).

64 "Overview of Blockchain and Distributed Ledger Technology for State Government Functions", Legislative Budget Board Staff (April 2019), available at: < http://www.lbb.state.tx.us/Documents/Publications/Staff_Report/2019/5191_Blockchain_Distributed_Ledger.pdf > (last consulted on 6 March 2020).

Despite some negative issues related to DLT, we may expect an increased use of this technology in the future. The benefits it brings to both governments and the public are increased transparency, accountability and other democratic values within society. However, abusing this technology may turn it into a dystopic oppression tool.

III. Distributed ledger technology and the Hague Service Convention

a) Possibilities

Having covered the main features of DLT and how some governments use it, it is time to explore how this technology can be used for the benefit of the Convention. As mentioned above, DLT can be used for the transmission of documents or for tracking documents. A salient benefit would be the reduction in printing costs, given that DLT can replace paper documentation with electronic documentation. Moreover, the service of process through online channels usually increases the transmission speed, in comparison to using offline infrastructure.

But before deciding to adopt DLT, Contracting Parties need to agree on setting up the necessary technology, the software to be used, the protocols and other details necessary. Agreeing on the type of technology and software to be used will ensure the interoperability of the different systems in the different countries. For obvious reasons, Central Authorities in each Contracting Party will serve as the nodes of the system, which will make the system closed and permissioned. Once this system has been established, Central Authorities may start to send documents, which will improve the accountability, transparency, and security of the process.

Contracting Parties may use DLT also to increase the security of their communications and documents' storage. Contracting Parties can set up a DLT system which can split a document in chunks that are uploaded cryptographically in the different ledgers of the network, and only the forwarding authority and the Central Authority of the requested state would be granted access to the entire document. This means that hackers and ill-intended parties would have to hack all the nodes in order to gain access to a document. When data is stored within a DLT, it is very hard to alter this. This immutability of the system can contribute to resistance against fraud and changes. Lastly, DLT can be used to track documents by applying a hash on the forwarded document. This hash, which is shared in the ledger, can show where the document is, what its status is and what the receiving authority has done with it. In this regard, DLT can contribute to the transparency of the service of documents, which in turn is often necessary for creating trust in a system to be used.

b) Challenges

The implementation of any DLT will require an agreement about the particular details to be used, the company that will implement it, the authority that will fund it and ultimately the creation of a supervising or oversight authority that will decide how to approve a new node and that is competent to monitor the overall system. Also, it is necessary to consider who will be competent to decide on issues arising from the use of DLT. To ensure the smooth functioning of a cross border DLT system it would be desirable to have some sort of international regulation, such as international minimum legal standards on DLT. Furthermore, these minimum legal standards must consist of an integrated approach comprising both technical and legal standards. The costs in this regard may be high, as it would require that Contracting Parties adapt their existing infrastructure to comply with the demands of DLT. These costs may be unaffordable and unacceptable for some Contracting Parties, and moreover, such costs can deter other States from signing the Convention.

In addition to the start-up costs, energy consumption and system maintenance may create high operational costs for Contracting Parties, which may become a hurdle for States that intend to become a party to the Convention. Also, there might be costs associated to training lawyers and bailiffs in order for them to be able to work with DLT. Some of the problems identified above, such as the vulnerability of the single nodes, may need careful consideration, but we think that authorities that administer single nodes will offer similar or higher security than they do for existing servers.

The distributed nature of the ledger may be a challenge for protecting data because data is shared among all the nodes in the network. For many data protection authorities this may be problematic because they may have strict requirements concerning the storage of data in servers located outside of their territory. Agreements between Contracting Parties may solve this situation, but this is an additional consideration before implementing DLT for the purpose of transmitting requests under the Convention, which may represent additional, novel costs.

IV. Conclusion

The advantages and potential offered by DLT cannot be denied. The examples outlined above regarding the use of DLT by Governments illustrate the acceptance and application of DLT by the public sector. Costly and time-consuming paper-based processes for the transfer of requests and service of documents can be reduced through DLT. At the same time, to ensure the inclusion of all Contracting Parties and all citizens - which is of significant importance to achieving judicial cooperation - we must take a careful and considerate approach when adopting DLT. In the end, it all boils down to safeguarding access to justice at a global level.

NATIONALLY DEVELOPED IT SYSTEMS AND THE HCCH SERVICE CONVENTION

BY FLORIAN HEINDLER

I. Introduction

The 2019 HCCH *a|Bridged* conference led to discussions on the use of electronic and information technology in the context of cross-border litigation, civil procedure and dispute resolution and, more specifically, on the *Hague Convention of 15 November 1965 on the Service of Abroad of Judicial and Extrajudicial Documents in Civil and Commercial Matters* (the "Convention"). From an Austrian law perspective, this discussion is even more topical due to the recent signing of the Convention by Austria,[65] and the soundness of electronic and information technology put in place for the national Austrian e-justice system.[66] Besides, Austria has experience with supranational e-justice pilots making use of the e-CODEX.[67] Most recently, the current COVID-19 pandemic demonstrates the importance of effecting service of process by digital means, independently of closed borders, cancelled flights, closed court buildings, or quarantined regions.[68]

This paper discusses a decentralised approach to the use of electronic and information technology in cross-border litigation, civil procedure, and dispute resolution.[69] The use of decentralised systems allows jurisdictions to continue operating in cross-border situations. Therefore, interoperable systems are required. However, making electronic and information technology systems interoperable to enhance cross-border legal cooperation is a policy choice. It is thus necessary to discuss the advantages and challenges of this approach and compare it with other solutions. The paper aims to provide a first overview on the use of interoperable nationally developed technology in cross-border situations under the Convention.

---

65 Austria signed the Convention on 22 December 2019.

66 See BMVRDJ, *Von der Lochkarte zu Legal Tech: 40 Jahre e-Justice in Österreich // From Punchcards to Legal Tech: 40 years of e-Justice in Austria* (Editions Weblaw 2018).

67 Relating to the European Small Claims Procedure (Regulation 2007/861/EC) and the European Order for Payment Procedure (Regulation 2006/1896/EC).

68 See E. van Gelder, X. Kramer and E. Themenli, *Access to justice in times of corona* (2020), available at: < https://conflictoflaws.net/2020/access-to-justice-in-times-of-corona/?print=pdf > (last consulted on 8 April 2020).

69 For technical details, see, *e.g.*, CEF Digital Connecting Europe, eDelivery Documentation, available at: < https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Documentation+eDelivery > (last consulted on 8 April 2020).

II. e-Service abroad: the importance of Articles 15 and 16 of the Service Convention

Communication via electronic and information technology rests on global systems of interconnected computer networks, such as the internet. Attempts for global regulation of the internet have not led to significant results.[70] Instead, the legal profession has overcome the paradigms of the virtual nature of the internet, its resistance to national regulation, and its extraterritoriality.[71]

Moreover, "the principle of State sovereignty applies in cyberspace".[72] Within its territorial share in the global cyberspace, States enact national rules. Cross-border litigation, civil procedure, and dispute resolution could not remain unaffected. National rules affect service via e-mail, social media platforms, and the mandatory use of legally assigned electronic post boxes. States which accept service via social media and e-mail service providers re-introduce a kind of *remise au parquet* by putting foreign nationals and persons residing abroad in danger of being considered as having been notified without appropriate service having been effected.

The law of the State in which the proceedings take place prescribes how a person has to be served.[73] Where the address of the person to be served is known to be abroad and the court of the State has additional knowledge about an electronic address, it is a matter of this State's internal law to serve this person electronically. The Convention does not oblige its Member States to serve nationals or residents of other Member States following the Convention's provisions. Neither does the Convention prejudice the application of the law of the State in which the proceedings take place.[74]

However, Articles 15 and 16 of the Service Convention, considering *remise au parquet*,[75] partly deviate from this concept and contain provisions of substantive nature.[76] Due to the technologically neutral wording of the Convention, the Convention does not require a specific form of transfer of information.[77] The aforementioned applies to Articles 15 and 16 of the Convention as well.[78] Therefore, Articles 15 and 16 of the Convention protects citizens and residents of Member States against insecure e-service methods acknowledged in various States, such as service via e-mail and social media.[79] If the

---

70 Roxana Radu most recently identified different stages of internet governance and deconstructed traditional patterns of governance analysis, see R. Radu, *Negotiating Internet Governance* (OUP 2019).

71 A. Segura-Serrano, "Internet Regulation and the Role of International Law", in A. von Bogdandy and R. Wolfrum (eds), *Max Planck Yearbook of United Nations Law* 10 (Brill 2006) 191, 200; M. Schmitt (ed), *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations* (CUP 2017) 12.

72 M. Schmitt (*op. cit.* note 71), 11-29, with further references; ECJ Case C-507/17, *Google (Portée territoriale du déréférencement)* [2019]; ignoring boundaries of territoriality in case of defamation and violation of personality rights: ECJ Case C-18/18, *Glawischnig-Piesczek* [2019].

73 Explanatory notes to the Ratification of the Convention by the Austrian Parliament, 10, available at: < https://www.ris.bka.gv.at/Dokumente/RegV/REGV_COO_2026_100_2_1654242/COO_2026_100_2_1699787.html > (last consulted on 8 April 2020).

74 P. Schlosser, *EU-Zivilprozessrecht* (3rd edn, C.H.Beck 2009) Art. 1 HZÜ para 5.

75 Recently on the *remise auf parquet* in France: *Cour de cassation*, Civ. 2e, 30 January 2020, no 18-23917.

76 HCCH, *Practical Handbook on the Operation of the Service Convention* (4th ed., HCCH 2016), note 303.

77 HCCH Conclusions and Recommendations adopted by the Special Commission on the practical operation of the Hague Apostille, Evidence and Service Conventions (28 October to 4 November 2003) (2003), Nos 60, 62-63.

78 *Op. cit.* note 76, note 303 *in fine*.

79 The Practical Handbook mentions this still with some caution, see *op. cit.* note 76 at note 98; for practice of serving via social media, see *e.g.,* Australia: *Mothership Music Pty Ltd v Ayre* [2012] New South Wales District Court 42, 14 DCLR(NSW) 118, [14]; Canada: *Knott Estate v Sutherland* [2009] British Columbia Supreme Court, AJ No. 1539; United Kingdom: *AKO Capital LLP and Master Fund Limited v*

defendant has not appeared, judgment shall not be given unless: the document was served by a method prescribed by the internal law of the State addressed, or the document was delivered to the defendant or to his or her residence by another method provided for by the Convention. Direct service is not a means provided for by the Convention if the State addressed opposed Article 10 of the Convention.[80]

In contrast, citizens and residents of non-signatories could only be protected through non-recognition of foreign decisions based on defective service.[81] On the other hand, this means that Contracting Parties of the Service Convention need to observe the internal law of the State addressed for effecting service to persons who are within the territory of the latter State.

III. Decentralised approach

The above section has shown that persons residing abroad cannot just be served through their social media profiles or random e-mail addresses, even if the law of the Member State in which the proceedings take place tolerates such practices. It follows that another solution, less anarchic, must be developed to allow direct e-service in cross-border cases. As mentioned in the introduction of this paper, jurisdictions should be able to continue operating their domestic systems as if e-service were to equal postal service.

In regards to postal service, people's homes have been assigned postal addresses. Those postal addresses have been assigned by governments instead of private organisations. In effect, every home has only one address. No service provider assigns a different postal address than others do. The system of postal addresses is a uniform system on the national level and contributes to the infrastructure of the State. Besides, and to a different degree, some national laws stipulate that service to the postal address of a person equals service to the person. Some States already have engaged in establishing a parallel infrastructure regarding e-service, aiming to have a uniform system of e-addresses contributing to the infrastructure of the State.[82]

a) National States as actors instead of multinational corporations

Basic needs for the use of electronic and information technology in e-service are accessibility, resilience, security, traceability, protection of data and privacy, the confidentiality of communication, the possibility to verify and authenticate the messages,[83]

TFS Derivatives and others [2012] High Court; United States, State of New York: *Baidoo v Blood-Dzraku* [2015] New York Supreme Court 5 N.Y.S.3d 709, 711; Netherlands: Rechtbank Amsterdam, 30 July 2009, no. 428212 / KG ZA 09-1092 WT/RV; for further references see Jan De Bruyne and Cedric Vanleenhove, 'The law in the 21st century: a Sisyphean struggle to keep up with technological evolutions?' in M. Miguel Carvalho (ed), *Law and Technology – E.Tec Yearbook* (JusGov 2018) 89, 93 et seq.

80 *Op. cit.* note 76 at note 307.

81 See Art. 34(2) of the former EU Service Regulation 44/2001/EC; R. Arenas Garcia, "Abolition of Exequatur: Problems and Solutions", in A. Bonomi and G. P. Romano (eds), *Yearbook of Private International Law XIII 2010* (Sellier 2010) 351, 368 *et seq*.

82 See *e.g.* Slovenia: Zákon no 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente), available at: < https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/305/20151101 > (last consulted on 8 April 2020).

83 With further references, see A. Kasper and E. Laurits, "Challenges in Collecting Digital Evidence", in T. Kerikmäe and A. Rull (eds), *A Legal Perspective The Future of Law and eTechnologies* (Springer 2016) 195, 219-224; S. Daoui, "GDPR, Blockchain and the French Data Protection Authority: Many Answers

and expeditious communication. Each of these elements concern distinct features and carry a specific meaning in the context of e-service. Security does not only mean that the message should reach its recipient without being broken up or altered. It also requires that the sender is identifiable to the recipient, and phishing expeditions do not endanger the use of the system. Sender identification is a rather problematic aspect of email transmission. The aforementioned might be even more problematic than the interception of email-communication,[84] which appears to be difficult in practice due to the large amount of data processed.

Furthermore, login to email postboxes is insufficiently protected through passwords, many of which are accessible through illegal databases after having been hacked or detected in phishing expeditions. To a larger extent, the same applies to service via social media platforms.

Apart from these basic requirements, e-service infrastructure must satisfy the standards of fair trial and due process of law for any citizen, including elderly people and persons with disabilities. It must be non-discriminatory and acknowledge the need to protect vulnerable groups.[85]

It is, therefore, submitted that commercial purposes that are significantly different from the requirements formulated above could become the key driver for the development of adequate electronic and information technology for e-service. It is not market dynamics that leads to the better protection of vulnerable groups or personal data. Non-discrimination, protection of vulnerable groups, accessibility, resilience, security, traceability, and protection of data are priorities of the States or based on the State's mandates. Market dynamics may vary from these priorities. The interests of the general public, therefore, should be dealt with by the States. Sufficiently strong regulation thus could only be implemented in e-service systems based on State investment, either directly or through private-public-partnerships.

b) Different speeds

States face different legal, cultural, sociological, economical, and financial obstacles in developing their e-service infrastructure. They also have different policy priorities. It is thus self-evident that the Contracting Parties to the Service Convention will progress at different speeds and with a varying level of effort. States need to be able to proceed at the pace which is most suitable for them. Some States have a centralised structure, whereas other States are federal, merely to name one instance of diversity. Offering States to make their e-service technology interoperable, once such technology exists, and to provide technical support, allows each State to adopt the appropriate measures.

Having said that, it is acknowledged that in cross-border cases, not every State needs to participate immediately in a decentralised system of interoperable, domestically developed e-service technologies. It goes without saying that States lacking a domestically

but Some Remaining Questions" (2019) 2 *Stanford J Blockchain L & Policy* < https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france > (last consulted on 8 April 2020).

84 See *op. cit.* note 76, at note 79 to Annex 8.

85 See on this aspect, B. Yuksel and F. Heindler, "Use of Blockchain Technology in Cross-Border Legal Cooperation under the Conventions of the Hague Converence on Private International Law" (University of Aberdeen School of Law Blog 2019), available at: < https://www.abdn.ac.uk/law/blog/use-of-blockchain-technology-in-crossborder-legal-cooperation-under-the-conventions-of-the-hague-conference-on-private-international-law-hcch/ > (last consulted on 8 April 2020).

developed e-service infrastructure cannot be connected. Even in supranational organisations, for instance, within the EU, the amendment to Article 14a of the proposed EU Service Regulation recast[86] demonstrates that service may be effected directly by electronic means available under the law of the Forum State for domestic service of documents. Since even within the EU, acceptance is voluntary, any further-reaching approach suggested to the Parties of the Convention would most probably fail.

Once States have developed national IT systems, they could join ongoing collaborative efforts. Clarifying technicalities could furthermore create an opportunity to discuss harmonisation and help States to improve their systems by learning about different solutions abroad.

c) Respecting the internal law of the addressed State addressed

Given that the States have been developing their national e-service solutions at various speeds, and against the background of their diverse legal, organisational, cultural, sociological, economical, and financial structures, a viable approach to handling cross-border cases lies in making these national e-service solutions interoperable. Enabling Central Authorities to continue using their nationally developed electronic and information technology when communicating with Central Authorities of the other Parties to the Convention, would most probably speed up and enhance the application of the Convention in terms of security and other basic requirements.

Yet, there is another dimension of making nationally developed e-service solutions interoperable. According to Article 5(1)(a) of the Service Convention, documents are served by a method prescribed by the internal law of the State addressed, or according to Article 5(1) (b) of the Convention, a requesting State could request a particular method for the service of documents "unless such a method is incompatible with the law of the State addressed".

Article 5 of the Convention is the central provision of the Convention. It is submitted that direct service under Article 10 of the Convention is feasible as well,[87] but several Member States have objected to Article 10. Direct service to an addressee who accepts this voluntarily is permitted, but voluntary consent in individual cases to certain e-service methods cannot replace a coherent system.

As shown above, compliance with the addressed State's internal law is vital for a State intending to use its nationally developed e-service solution in cross-border cases. The advantage of a system connecting various nationally developed solutions is that the requesting State could use its nationally developed e-service infrastructure to request the Central Authority of the State addressed and, thereby, serve on the recipient using the interoperable e-service infrastructure of both States. In doing so, the requesting State would fully respect the internal law of the addressed State, is independent of getting consent from the recipient of the message, and avoid difficulties arising from objections to Article 10 of the Convention as well as from Articles 15 and 16 of the Convention.

---

86 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) COM/2018/379 final as amended on 28 November 2019 and published in document no 14599/19.

87 It appears, thus, arguable whether – contrary to the wording – the intention of the Convention permits facilitating service of judicial documents via electronic means under Art. 10(a).

d) Preservation of national investment

Numerous States already have been investing significant means in developing national electronic and information technology put in place for their court systems. Those national investments should be preserved instead of replaced. Investments, especially, have been made in setting up infrastructure which connects people, getting them used to having an e-address registered with tax authorities, or with the post or banking system. Each State most probably undertook measures to use channels that worked well in the past, given their national tradition of serving documents. Accessibility of an e-address is the principal aspect of the success of e-service. Investments made in this respect should be preserved when it comes to communication at an international level.

IV. Service beyond residence

The Service Convention focuses on the interaction between a requesting State and a State addressed. It does not limit its scope to citizens of addressed States or its residents. Moreover, it refers to the place of service.[88] Only Article 1(2) of the Convention contains a geographical nexus, stating that the "Convention shall not apply where the address of the person to be served with the document is not known". It was simply not necessary to determine the scope. The requesting States could reasonably only address State, in which the person to be served had his or her physical address.

Nowadays this is more complex, as the requirement that the physical address of a person to be served must be known does not make sense in an e-service environment. Given the technologically neutral approach of the Convention,[89] an electronic address should be sufficient to fulfil this requirement. In continuation of the above reflections, such an electronic address, however, shall be an officially designated or confirmed address, depending on how the national law of the State addressed provides for it.

The law of the State which registered the electronic address for service governs the question of whether the person has a valid e-address in that State. Thus, the e-address assigned for service is linked to the internal law of a particular State. The aforementioned concurs with the application of the law of the State assigning a physical address, which also governs the question of whether an address of the addressee in this State exists. Similar to interconnected computer networks such as the internet, e-service addresses shall be assigned to the territory of a State to allow national rules and the Convention to be applied. An e-address that is not provided or authorized by a State to be the relevant e-address for purpose of service, as defined under the Convention, is not an address within the meaning of Article 1 of the Convention.[90] If a Swiss court decided to serve to the electronic address of a Slovenian resident assigned to this person by Slovenia under Slovenian law- it makes a case for Article 5 of the Convention. Slovenia, like many other States, declared "that the service of documents pursuant to Article 10(a), is only permitted if judicial documents are sent to the addressee by registered letter with acknowledgement of receipt".[91] It would unquestionably satisfy the rules of the Convention if the addressee is served by way of e-service to the Slovenian e-address as requested by the Swiss court, and if such service corresponds to the internal law of Slovenia which will be the case. That would still apply if the person served via the Slovenian e-address is a Belgian citizen currently residing in South

88 See *op. cit.* note 76, at note 16.

89 *Ibid.*

90 See *op. cit.* note 76, at note 98.

91 Declarations made by Slovenia on 18 December 2012 relating to Arts 8, 10, 15, and 16.

Africa. It is for the internal law of the State assigning the e-address to determine under which conditions an e-address is assigned to a person and which ceases for valid service.

This example demonstrates the importance of the reference to the law of the State assigning the e-address. Irrespective of the current address or citizenship, even persons residing in a State which is not a party to the Convention can be served under the Convention if they possess an e-address of one of the Convention's Member States. If a person has registered an e-service postbox subject to the law of a State Party, the territorial nexus necessary to assess the applicability of the Convention exists.

This approach acknowledges that States might export their e-service infrastructure and offer services to persons without having a relationship like a residence or citizenship. It recalls the idea of a country-of-origin principle. Persons registering an e-address abroad may be served at this address under the law of that foreign State. The State which assigned the e-address is the State to be addressed for service in the meaning of the Convention.

Of course, harmonizing rules for withdrawing and assigning e-addresses would be favourable. Projects like the successful UNCITRAL Model Law on Electronic Signatures would be most welcome.[92] However, it cannot be expected that States will voluntarily assign e-addresses to foreigners and persons residing abroad but rather, for example, based on tax residence, registration at a physical address, and opening of a bank account.

However, the system envisioned requires acceptance in another State when a decision must be enforced there. Should the decision of the Swiss court against the Belgium citizen served to its Slovenian e-address be enforced in South Africa, the South African Act on Enforcement of Foreign Civil Judgements could prevent recognition and enforcement in South Africa due to defective service and associated violation of the South African public policy clause. Internationally accepted standards for the withdrawal and assigning of e-addresses would prevent such difficulties. Meanwhile, claimants will prefer to effect service to an e-address of a State in which assets of the defendant are located.

[92] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, available at: < https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf > (last consulted on 8 April 2020); for its significance, see the compilation of national laws in Stephen Mason, "Table of Electronic Signature Legislation", 15 *Dig Evidence & Elec Sign L Rev* 2018, 146.

V. Communication between Central Authorities

As communication between Central Authorities is concerned, one can imagine a stand-alone electronic and information technology-based system of communication. However, even Central Authorities might be reluctant to use an international communication system (for example, if provided by the Hague Conference on Private International Law ("HCCH")) in parallel with their nationally developed systems and to copy information from one system to the other. Therefore, interoperability of nationally developed electronic and information technology must be achieved rather than providing stand-alone solutions for communication between Central Authorities. If, however, a State lacks its own electronic and information technology system, its Central Authorities would need to be connected to the decentralised system with a stand-alone component.

VI. Models for decentralised systems

Models for an international gateway, i.e., a *subsidiary system enabling semantic interoperability* of diverse nationally developed electronic and information technology, already exist. The HCCH is the first international organisation implementing this approach in the use of e-CODEX for the HCCH 2007 Child Support Convention referred to as *iSupport*.[93] Therein, a gateway between the two nationally developed systems has been established.

Some EU Member States are going to adopt this decentralised approach by focusing on making different semantics interoperable concerning the service of documents abroad. In the course of the current negotiations on the amendment of the EU Service Regulation,[94] instead of setting up EU-e-service postboxes, a choice was made to enable cross-border service directly by electronic methods available under the law of the Forum State for the domestic service of documents. The technical solution pondered in the European Proposal is a decentralised IT system made up of nationally developed IT systems, interconnected by a secure and reliable communication infrastructure (Article 3a) and with traditional means of communication to be used in the case of unforeseen and exceptional disruption to the system (Article 6). The inserted Article 14a(1) reads as follows: "Service of judicial documents may be effected directly on a person with his or her known address for service in another Member State by electronic methods available under the law of the Forum State, for the domestic service of documents […]". Even in the EU, majority requirements urged the drafters to insert concerning Article 14(1)(b) that the "addressee gave in advance express consent to use electronic means for purposes of serving documents in course legal proceedings".[95]

Service through social media, as accepted in the law of various jurisdictions,[96] is not recognised in the proposal. Service shall use qualified electronic registered delivery services within the meaning of Article 44 Regulation (EU) No 910/2014.[97] Only email is permitted if the addressee gave, in advance, express consent "to the court or authority seised […] for the purposes of serving documents in the course of those proceedings".[98]

---

93 See HCCH iSupport Section, available at: < https://www.hcch.net/de/instruments/conventions/specialised-sections/child-support/isupport1 > (last consulted on 8 April 2020).

94 COM/2018/379 final (*supra*, note 86).

95 *Ibid*.

96 See, *supra*, note 79.

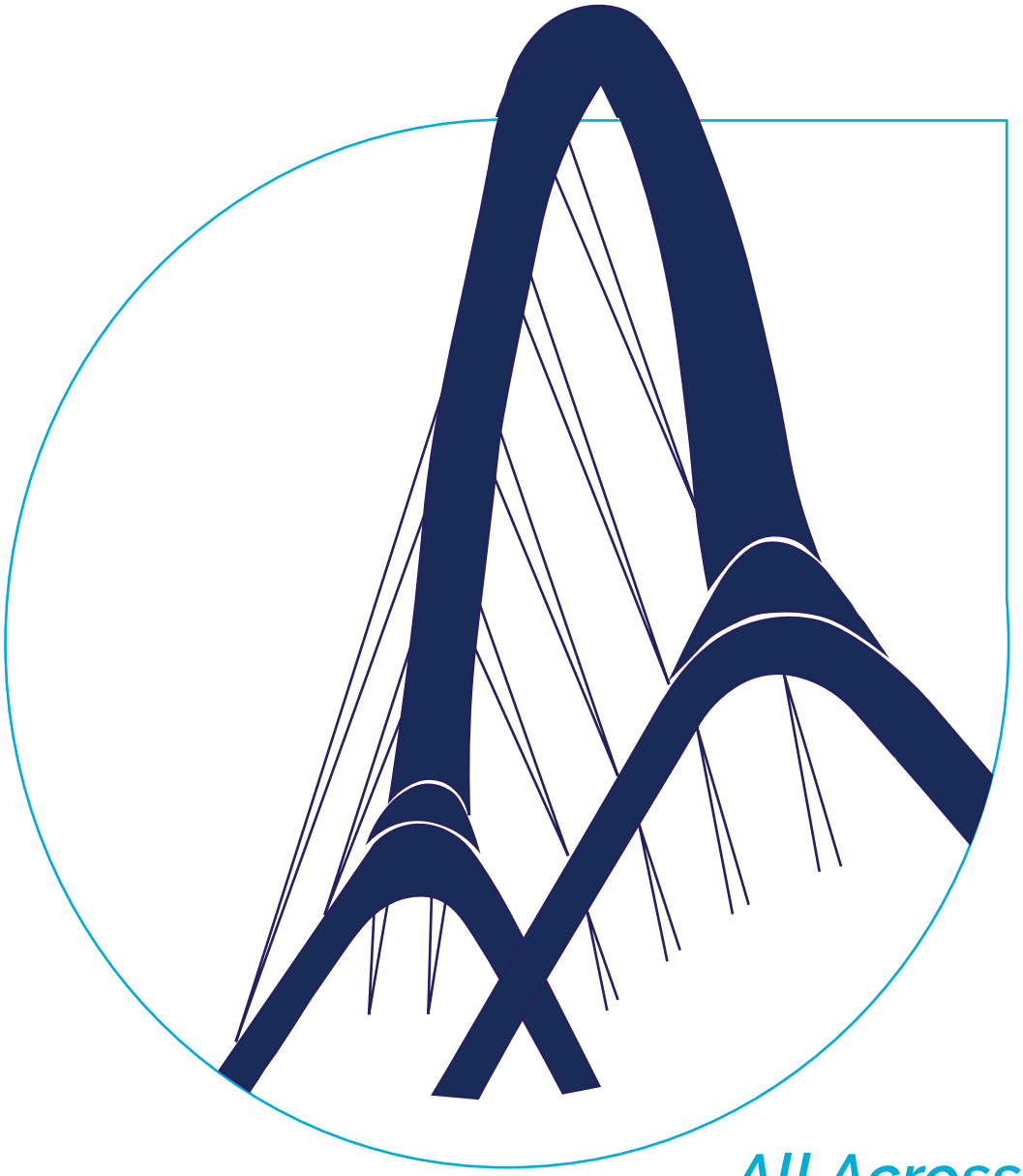
97 Regulation 2014/910/EU on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

98 Art. 14(1)(b) COM/2018/379 final (*supra*, note 86).

VII. Synopsis

As suggested concerning the internet, regulation of cross-border e-service could take the form of international law, through international instruments and the establishment of international dispute settlement bodies. This approach requires agreement about the content of such regulation. Another approach would be to rely on the dynamics of the market and self-regulation by relevant market players and rely on a framework of cross-border e-service. Yet, another solution to make cross-border e-service a viable option is to focus on making nationally developed e-service solutions interoperable. This approach is supported because the service of judicial documents is part of the system of judicial infrastructure guided by priorities to be defined by the States. These priorities, as shown above, are different from market priorities, and include non-discriminatory access, protection of vulnerable groups, accessibility, resilience, security, traceability, and protection of data. It goes without saying that these priorities could be satisfied by a stand-alone international solution as well. However, national investments could be better preserved if nationally developed systems were made interoperable. The diverse priorities, traditions in the legal culture regarding service, and public needs could be addressed. In particular, Central authorities, courts, legal practitioners, and addressees could remain within the domestic system that is familiar to them.

If we imagine a gateway between diverse national e-service systems, the technology requires a gatekeeper translating information into the semantics of the own and foreign electronic and information technology. In this function, the gatekeeper transforms the information into the semantics required by the internal law of the State addressed as it would act as Central Authority requested and serving under Article 5(1)(a) of the Convention. Therefore, the concept of Central Authorities will continue to be a story of success for international service of documents and, most probably, other HCCH instruments in the era of electronic and information technology.



The Lab:
All Across the World

In this section, judicial representatives from different regions discuss how their national service procedures currently make use of IT, or will do so in the future, with reference to systems already in place or projects currently in development.

THE LAB:
ALL ACROSS THE WORLD

BY MASTER DAVID COOK - JUDICIARY OF ENGLAND AND WALES

In this short paper I give a brief overview of recent technological developments in the courts of England and Wales. I will describe two main developments in the civil jurisdiction and describe the role which e-service currently plays. I will conclude with some general observations.

I. Technology in our courts

The jurisdiction of England and Wales is currently part way through a £1 billion reform programme[99] which aims to bring new technology and modern ways of working to the way justice is administered.

Historically the use of technology in our court system had developed in a piecemeal fashion using a wide variety of platforms most of which are now beginning to show their age and are not really fit for purpose in the 21st century. There is also the issue of access to justice. It has been widely recognised that many individuals find our court system too costly and too slow.

The reform program is wide and complex. It comprises over 50 projects across all jurisdictions (civil, criminal, family and tribunals). Many of these projects involve designing common components. The central component is known as "core case data" which is a database containing all relevant case information. Each jurisdiction will have its own interface with core case data. Examples of other components being developed are systems to upload and manage documents and to enable full video hearings to take place.

As far as the civil jurisdiction is concerned the major developments are the development of an online money claims service [OLMC] and the roll out of an e-filing and case management system for the High Court, Court of Appeal and Upper Tribunal.

Court facilities are also being upgraded, and wifi has been rolled out to all court centres along with updated facilities for video conferencing and video hearings.

II. OLMC

OLMC is a digital service for people to resolve civil money claims in a simple, accessible and proportionate way. Users are able to create an account which enables them to issue and respond to online civil money claims of less than £10,000 without the need for lawyers. New procedural rules have been developed for the system, Civil Procedure Rule [CPR] PD 51 R. For users these rules are embedded in the system which guides them through the process using a sequence of screens. By the end of November 2019, over 103,000 claims had been issued using this system and more than £6.36 million taken in court

99 See Transforming our justice system published 15 September 2016, available at: < https://www.gov.uk/government/publications/transforming-our-justice-system-joint-statement >.

fees. The average time to progress a case through to a first directions hearing using the online process is 5.2 weeks compared to 13.7 using our non-reformed services. Between now and summer 2020, the system will be expanded to increase the type of claims that can be issued, and further stages of the system will be built, enabling:

- More online negotiation and settlement;
- Uploading of evidence;
- Facilities for judges to decide cases 'on the digital papers' either at a face-to-face hearing or simply on the papers; and
- A structure for enforcing judgments.

This system is being designed and built by the Ministry of Justice using agile methodology. For those not familiar with this method, this means building small components quickly and putting them to the test in the real world, iterating and improving them in response to feedback so that the systems really work for the people who use them. Judges are actively involved at all stages of development.

In the long term, a similar system using core case data will be extended to all civil cases in the County Courts. Pilots for this system are just being implemented. The aim is to digitise the County Court.

III. E-filing CE-file

The e-filing system was developed by the Ministry of Justice in partnership with Thompson Reuters for use in the higher courts. It was introduced to the London Business and Property Courts in 2015. This is a medium to long term solution until core case data is ready to extend to the High Court. In the first quarter of 2019, the E-filing project delivered the first tranche of developments extending the existing system, to both the Queen's Bench Division (claims and appeals) and the seven regional Business and Property Courts outside London. This means registered users can now issue claims, file documents and pay court fees online.

More than 750 new users have registered to use the service, and there are already over 10,000 cases being managed using the new digital case management system. Use of the system is mandatory for represented parties but non-mandatory for litigants in person.

New procedural rules have been written to permit the use of electronic documents and court seals and to cater for time limits in view of the fact the system operates 24 hours a day (see CPR PD510).

The e-filing project team is now working on a timeline to extend the service to the Court of Appeal (Civil Division), Administrative Court, the Upper Tribunal Chambers and the Employment Appeal Tribunal.
The e-filing system will be used to case manage requests made to the Central Authority under the Hague Evidence and Service Conventions. But not yet for transmission of requests incoming or outgoing to the requesting party. However, this is a technical possibility for the future.

IV. E-Service

E-service has been possible in England and Wales since 2009 in the limited circumstances set out in CPR PD 6A, that is, the party to be served or their lawyer has indicated to the serving party that the party to be served is willing to accept e-service. This might be thought unnecessarily restrictive given advances in technology and the almost universal acceptance of e-mail as a method of commination, particularly by law firms.

However, in the United Kingdom, it is important to remember that there is no central register of citizens or e-mail addresses. For the future, there is certainly a good case to be made for extending the availability of e-service to those who are professionally represented.

It has always been possible to apply to the Court for alternative service under CPR r 6.15. Examples of methods of service which have been permitted under this rule are by fax, e-mail, and social media such as Facebook, Twitter and Instagram.

It is not envisaged that electronic service will become a primary method of service, in the near future, for originating process. However, for proceedings in OLMC and for those being managed in the electronic e-filing system, all documents and orders will be transmitted to the parties electronically by the court thus removing the need for physical service.

V. Final Observations

Market research tells us that the users of our new electronic systems appear to welcome them. There is a high degree of user satisfaction.

The benefits are clear, 24-hour access to the legal system and a reduction in the time taken to process and progress cases.

Following concerns that some people may be excluded from digital systems, we have put in place a system of digital assistance to help those who lack access to technology or who do not possess the necessary skills. However, our experience so far is that very few people have difficulty in using the new systems.

Finally, there seems to be a positive thirst from personal and professional users of our court system for technological innovation. It is fair to say that a favourable climate exists for technological innovations in cross border litigation.

Thank you.

THE LAB:
ALL ACROSS THE WORLD

BY JUDGE YOON JUNG CHOI – JUDICIARY OF SOUTH KOREA

I. Introduction

In South Korea, electronic service (e-service) is conducted through an electronic data processing system called the 'e--litigation system'. Electronic litigation (e-litigation) was first introduced by "Act on the Use, etc. of Electronic Documents in Civil Litigation, etc."[100] (E-Litigation Act)[101] in 2010 and was only available for patent cases, but gradually, over the years, it extended to other areas, and now e-litigation is used in all civil cases. E-filing is not compulsory for the parties, but the percentage of e-filings has increased rapidly due to its easy access and swiftness. In 2018, nearly 76.6% of civil cases (including family/administrative cases) were instituted through e-filing.

II. E-filing system

Any person wishing to bring an action using the e-litigation system must first register as a user on the e-filing website.[102] The verification of identity with an authentication certificate is required in this process. There are different categories for registration purposes, such as that of individual members, corporate members and agent members. Attorneys, for example, can register as agent members and file complaints on behalf of the parties. Certain government authorities and agencies are obliged by law to use the e--filing system.

After logging into the website with the registered member ID, the parties are able to file a complaint online by typing it directly or attaching the statement of claim. Documentary evidence, such as a contract or a receipt, can also be attached. Court fees should also be paid online before submitting the complaint. Once the submission is processed and stamped with a digital signature, it directly becomes a case file and a case number is automatically assigned. The party is also notified by email and text message that the complaint has been well received. Afterwards, the parties are always able to view all the documents, evidence and general information related to their case, such as the status of service of process or the date of the trial, with an electronic record viewer on the e-filing website.

III. E-service

When a plaintiff submits an electronic complaint through the e-filing website, the defendant is served a printout of the e-complaint with instructions on how to use the e-litigation system. If the defendant also registers as a user on the website and agrees with the continuation of e-litigation, e-service will be effected as of that moment. If the defendant is a government authority or agency that is obliged by law to use the e-filing

---

100 Act No. 12586, May 20, 2014.

101 Available at: < http://www.law.go.kr/lsInfoP.do?lsiSeq=153964&efYd=20141201#0000 >.

102 The e-filing website is the following: < https://ecfs.scourt.go.kr/ecf/index.jsp >.

system as mentioned above, service will be effected electronically from the outset, without the need to have the defendant's prior consent.

E-service in South Korea consists of two steps. First, a court clerk posts the e-document to be served on the e--litigation system. Second, the court clerk electronically informs by email and text message the people to be served of said event, so that they can check the document themselves. Both steps are conducted at the same time through an e-case management program used by court clerks. When a court clerk selects an e-document in the e-cabinet and clicks the '*service*' button, then the e-document is automatically posted, and a notification is immediately sent to the person to be served.

According to Article 11(4) of the E-litigation Act, e-service is deemed to have been effected when the person to be served actually checks the e-document posted on the e-filing website. However, there may be cases where the person to be served purposefully does not check it for a long time. In order to prevent this situation from arising, that same provision also stipulates that e-service is also deemed to have been effected after one week from the day of notification. Therefore, the person to be served has one week to check the e-document posted, and afterwards the e-document is considered to have been served, even though the person may not have actually checked it. If a system failure occurs, making it impossible for the parties to check the e-document, the period during which the document could not be checked because of the system failure is not counted within this one-week term.

IV. Cross-border cases and the Service Convention

If a defendant lives abroad, hard copies of the complaint should first be served to the defendant with information concerning the e-litigation system. At present, the e-filing website is only available in Korean and requires an authentication certificate to verify the user's identity. These questions make it difficult for foreigners to use the system on their own. However, if a defendant who has no difficulty with these issues and consents to e-service and e-litigation, either by himself or through his or her attorney, e-service can be effected from that point forward. Notably, if a defendant living abroad retains a Korean attorney to file a lawsuit or to defend a case, e-service might also be a very useful and easy way to make the whole process expedite and efficient. Since e-litigation is firmly grounded on the party's consent, e-service is not considered in the context of the *Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* ("Service Convention").

In terms of the Service Convention, South Korea is a Contracting Party to the Convention and the national court administration is designated as the Central Authority for receiving requests for service. Electronic judicial documents or e-filings could easily be received in electronic form, using our e-litigation system, without any technical problem. In order to do this, however, the requesting authority should first register as a member and that would require verification. The verification process is not difficult on the technical level, but there needs to be political will and cooperation among States in advance to facilitate the process.

THE LAB:
ALL ACROSS THE WORLD

BY JUDGE CARLOS VIEIRA VON ADAMEK - JUDGE AND SECRETARY-GENERAL OF BRAZIL'S NATIONAL COUNCIL OF JUSTICE

(summary prepared by Lise Theunissen based on Judge Vieira von Adamek's presentation)

During the *Lab: All Across the World* panel discussion, **Carlos Vieira von Adamek, Judge and Secretary-General of Brazil's National Council of Justice**, succinctly presented some of the technological advances implemented by the Brazilian judiciary, which could serve as inspiration for the modernisation of the international legal and judicial cooperation regime. At the outset, he stressed that security concerns should not be an impediment for using technology to improve the system

I. Background

The National Council of Justice (CNJ) was created in 2004 by a constitutional amendment and established in 2005. The CNJ, chaired by the President of the Supreme Court of Brazil and conformed by 15 members, acts as the central body of the Brazilian judiciary for administrative and financial affairs, and designs the strategic policies of the judiciary.

Due to Brazil's territorial extension, a large judicial structure, comprised of over 80,000 judges, is necessary to provide quality judicial services and to be close to the population. The court system is divided into five branches, namely the state, federal, labour, military and electoral branches. In 2018, there were over 78 million court cases, and 28 million new cases were filed, of which 80% were filed online.

II. Five electronic systems and programs by Brazil's National Council of Justice

In order to have an efficient judiciary, the CNJ has developed five electronic systems and programs to assist in the judicial process.

Firstly, the CNJ has created the **Electronic Judicial Process platform** (PJe system). The CNJ, with the contribution of several courts, developed and distributed for free a computer system for the management of cases and e-files, ending the need for hard copies and the physical presence of parties in court. One of the main pillars of the PJe is the collaborative work between courts. Currently, 76 appeal and superior courts have implemented the PJe system, replacing their own case management system. The goal is to implement this technological solution in all Brazilian courts. The PJe is the most extensive program of the CNJ with 31 million cases filed.

Additionally, the CNJ has established an Artificial Intelligence (AI) Centre for Research to develop and maintain the AI software used in the PJe system, such as the Synapsis software. The work of the AI Centre focuses on building an AI service eco-system; on providing a platform for training, hosting and distributing AI models; and on acting as an online hub for courts through a cloud-based system. The main objectives of the use of IT is to automate the work and to provide decision support tools. In 2020, the Centre is expected to start consolidating all judicial databases in Brazil to obtain structured information for the construction of AI models.

Secondly, Brazil has put in place the **National Adoption and Reception System**, an online adoption and childcare system to protect children and adolescents. The system collects and processes all relevant facts regarding the entry of children and adolescents into childcare services and leave from childcare services due to adoption or to family reintegration. Currently, there are 37.896 registered children, 1.054 children eligible for adoption and 34.477 qualified applicants.

As the software seeks to provide more effective attention to the children, the system facilitates a faster case referral and resolution, expediting the time spent under childcare services. To this aim, the system keeps a complete history of the child. The system helps to ensure that all possible solutions, such as adoption or reunification with the parents or the caretakers, are explored, and the best solution is selected.

Thirdly, the CNJ department that monitors and oversees the national prison system and the socio--educational measures' enforcement system, developed a **Program to Monitor and Oversee the Prison System**. Currently, the program has 960.800 active processes and 82,35% of the current records use the program.

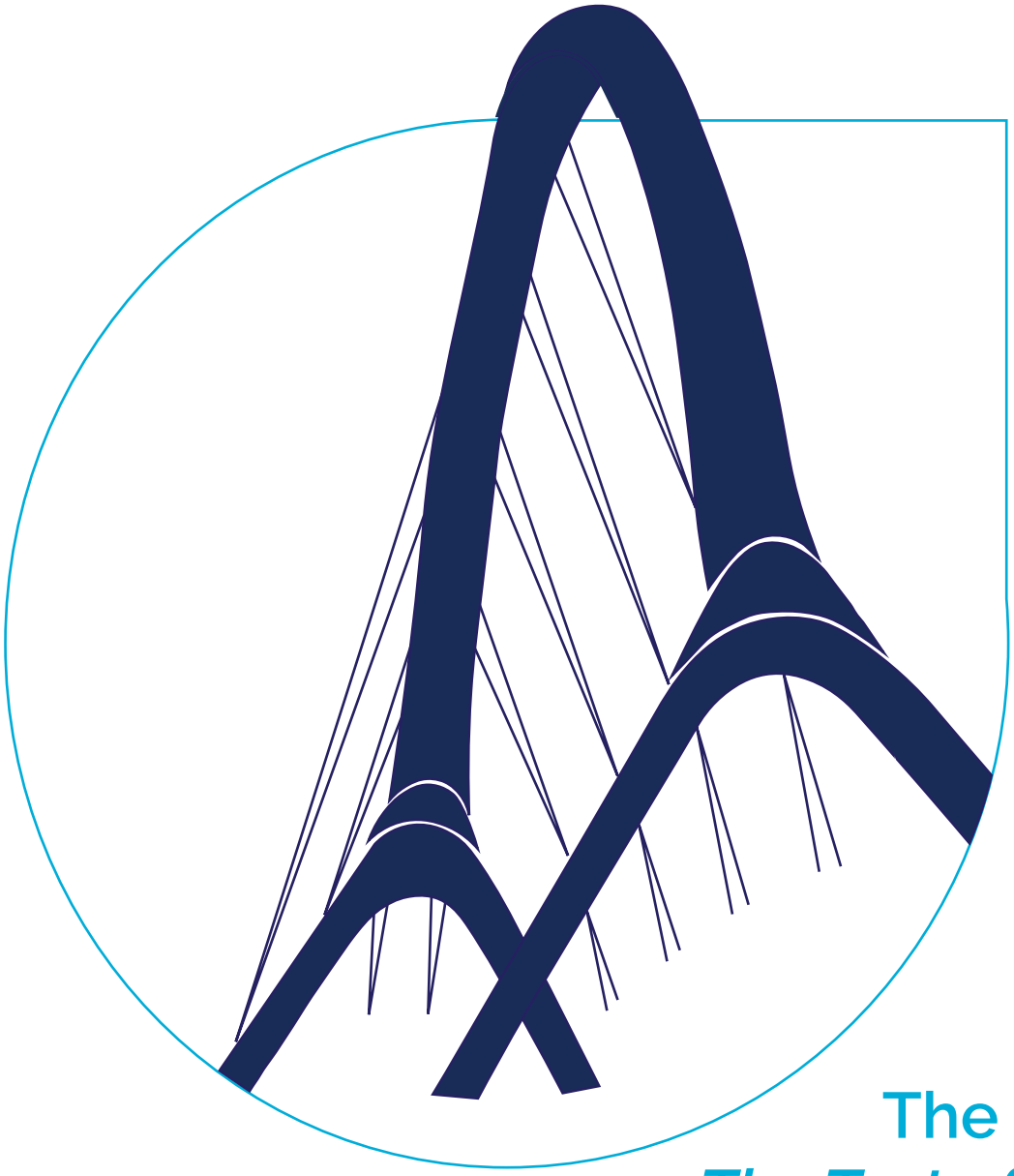
The software utilized aims to control criminal enforcement measures and gathers information on the prison system all throughout the national territory. The software provides a more efficient procedure for processing and managing data regarding the prison's population, and it can be accessed through any electronic device connected to the internet. The use of the software has the following benefits: the centralized visualization of the information of a case, the automatic calculation of the penalty (including the automatic scheduling of benefits as per the Penal Execution Law), and the electronic monitoring of the progress of deadlines, providing the status of ongoing criminal enforcement and statistical reports in real time.

Fourthly, an **Online Litigation Platform** aimed at solving consumer disputes was developed to enhance the use of technology in the judicial process.

Finally, the **National Interoperability Model (NIM)**, created in 2013 through a joint venture between the CNJ and the Public Prosecution's National Council, sets the standard for the exchange of procedural information within the judiciary. The NIM is a model for the electronic consolidation and transfer of data and procedural documents between the various judicial actors. The courts and private institutions with an interest to contribute to the development of the NIM are responsible for its implementation. The standard implementation of the model ensures the unification, inviolability and security of legal procedures, including procedural secrecy when applicable.

III. Conclusion

To conclude, Judge Carlos Vieira von Adamek stressed that these electronic systems and programs developed by the Brazilian CNJ could inspire the modernization of the current international legal and judicial cooperation system and improve service of process for all.



The Open Lab:
The Text of Tomorrow

This section is an academic examination of the HCCH Service Convention and how it will operate in the world of tomorrow.

ARE YOU BEING SERVED? DIGITISING JUDICIAL COOPERATION AND THE HCCH SERVICE CONVENTION

BY XANDRA KRAMER, ERASMUS UNIVERSITY ROTTERDAM/UTRECHT UNIVERSITY

I. Past and Present: Success of the Hague Service Convention

The proper service of documents is key to ensuring a fair trial in civil litigation. In transnational cases, judicial cooperation is pivotal to enabling the service of process. The Hague Service Convention was adopted in 1965 to secure actual notice in a timely manner, and it simplified the means of transmitting documents.[103] While its operation in practice is not without flaws and the Convention may need modernisation, it should be stressed that this Convention is one of the most successful of its kind at the global level. Despite increased complexity in transnational litigation over the 55 years of its existence, it has largely stood the test of time. To date, 76 countries worldwide have ratified the Convention, and it can still count on new accessions every year.[104] The Service Convention has also served, among others, as a model for the European Union (EU) Service Regulation.[105] Today we face the challenges and opportunities that new technologies offer in cross-border litigation and the service of process in particular. The question is whether the Hague Service Convention needs amendment to facilitate existing and new technologies of electronic service, and if so, how this can best be achieved.

II. The Service Problem in Europe and Globally

The service of documents is central both to fair and to efficient international litigation. On the one hand, a system that facilitates a speedy and efficient service is needed to avoid delays and additional costs. On the other hand, ensuring that the document reaches the addressee, in a language that the addressee understands and in time for the preparation of the addressee's defence, is crucial to guaranteeing the right to be heard and to obtain an enforceable judgment.

Research on the functioning of EU instruments on civil justice cooperation shows that the service of documents is a pervasive problem.[106] Difficulties are the result of the differences between national rules on service, the plurality of authorities involved and their different work methods, language requirements and other formalities, which result in delays in the actual service to the addressee and obtaining proof thereof. Moving from formal service channels through transmitting agencies to less costly and time-consuming postal service still creates challenges as regards the actual notice and receipt of proof. Unlike under the EU Service Regulation,[107] enabling postal service through the Hague

---

103 V. Taborda Ferreira V, "Rapport explicatif", in HCCH, *Actes et documents de la Dixième session* (1964), Tome III; HCCH, *Practical Handbook on the Operation of the Service Convention* (4th Edition, 2016), no 6.

104 Status 1 July 2020.

105 Regulation (EC) No 1393/2007 on the service of documents (EU Service Regulation).

106 *E.g.* F. Gascón Inchausti and M. Requejo Isidro, "A Classic Cross-border Case: the Usual Situation in First Instance", in B. Hess and P. Ortolani (eds), *Impediments of National Procedural Law to the Free Movement of Judgments, Vol. I* (Hart/Beck/Normos 2019), 11-30; in the same volume, X. Kramer, "Specific Instruments", 239.

107 Art 14 EU Service Regulation.

Service Convention is still voluntary, although Central Authorities now commonly use postal channels in accordance with Art. 10.[108] This may also pave the way for the use of e-mail.

Enabling electronic service of documents is not only necessary to keep up with predominant ways of communicating and working in today's society, but it also creates opportunities to diminish the apparent trade-off between efficient and secure service. Devising a proper system of e-service of documents is instrumental in increasing access to justice in cross-border litigation. Unfortunately, there is no quick fix. Although the electronic service of documents has been discussed since e-mail became an ordinary means of communication in the 1990s, e-service is still underdeveloped and not accepted in all countries.[109] Recent discussions in the European Union are exemplary regarding the considerable difficulties of e-service in the cross-border context. In May 2018, the European Commission put forward a proposal to amend the EU Service Regulation with the primary aim of increasing efficiency by introducing a virtual equivalent to postal service.[110] Since then, the proposal has been the subject of intensive discussions and has undergone a large number of amendments. However, this is not the place for analysis. Suffice it to say that discussions revolve around the difficulties of putting into place an interoperable IT system; whether electronic service should be mandatory or voluntary; and how privacy and the protection of data can be secured.

III. Making the Hague Service Convention Tech Proof

Considering the technical and legal obstacles impeding the implementation of electronic service in a regional instrument operating in a judicial cooperation system as advanced as the EU, one may wonder how it can be achieved at the global level. In the EU, the body of existing instruments on judicial cooperation, qualified electronic registered delivery services, and electronic identification, as well as the EU e-justice portal, greatly facilitates judicial cooperation, while legislation on data protection secures safety and privacy. Also, EU funding will be made available to set up decentralised IT systems facilitating e-service. These supportive measures are largely absent in the global context of the Hague Service Convention. In addition, securing safe systems that guarantee privacy and protection of personal data at the global level creates even more significant challenges. However, taking into account the crucial role of technology in society and the legal domain, and the need to increase efficiency relating to the service of documents, it is not a question of 'whether' but only of 'how' the Hague Service Convention should be made technology-proof.

The text of the Convention is plain and straightforward, and – considering the worldwide use and great diversity of legal systems – it should stay this way. If amendments are conceived to be necessary, they will primarily involve the following two. First, Art. 10(a) of the Hague Service Convention on transmission channels should clarify that postal channels would also include electronic means. This is in line with more recent conventions and EU instruments referring to written documents that also include electronic means.[111] Second, it may be considered to include a reference to an electronic address in Art. 1(2) in order to extend the scope of the Convention. A primary question is whether the possibility

---

108 Practical Handbook (*op. cit.* note 103), nos 125, 134.

109 This includes the author's home country, the Netherlands.

110 European Commission, "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents)", COM(2018) 379 final.

111 *E.g.* Art 3 HCCH 2005 Choice of Court Convention.

of sending and receiving documents through electronic means should be made compulsory. Ideally, this should be answered in the affirmative. However, this is not realistic, considering the voluntary nature of transmission by postal service under Art. 10(a) of the Hague Service Convention and the fact that even in the EU a mandatory system of electronic service is questionable. If amendments are to be made, this step should also be facilitated by practice guidelines. As global binding instruments on electronic identification and information security are lacking, these must be left to national law.

Though modernisation of the text of the 1965 Hague Service Convention may be useful, amending such a widely ratified convention is extremely cumbersome. The better option may be to establish a protocol designed to reflect on the use of technology. But even without such formal amendments or a protocol, relying on the functional equivalence of electronic documents, as is widely accepted,[112] may be sufficient when complemented by practice guidelines. The latest edition of the Practical Handbook on the Service Convention already contains a useful section on electronic service.

IV. An Instrument for Electronic Judicial Cooperation?

The last point to address is whether a more widely encompassing system involving electronic international judicial cooperation is desirable. Some issues regarding electronic documents and transmission by technological means have arisen, and not only in the context of the service of documents. They have also been discussed extensively as regards the taking of evidence and e-discovery in particular (Hague Evidence Convention),[113] as well as in the area of family law and the recognition of foreign documents (Apostille Convention). The use of electronic documents and information exchange has become standard; the first 'email trials' date back to the 1990s, and electronic devices and social media play an essential role in both civil and criminal litigation. Such an overarching instrument, be it in the form of a convention, a protocol, or model law, could set out the main principles about electronic documents, identification and security, and provide rules or guidelines for legal practice. Such an instrument could greatly benefit international judicial cooperation and extend access to justice and the rule of law in today's digitised world.

[112] For instance, in relation to written arbitration agreements under the New York Convention 1958, making use of a Legislative Note.

[113] See *e.g.* S. Mason and D. Seng (eds), *Electronic Evidence* (Institute of Advanced Legal Studies 2017); X. Kramer, "Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise", in *La Prueba en el Proceso/Evidence in the process* (Atelier 2018), 391-410.

LAUNCHING THE HCCH SERVICE CONVENTION INTO THE CRYPTO SPACE

BY FLORENCE GUILLAUME, PROFESSOR OF PRIVATE INTERNATIONAL LAW, UNIVERSITY OF NEUCHÂTEL, SWITZERLAND
AND
SVEN RIVA, PH.D. STUDENT IN PRIVATE INTERNATIONAL LAW, UNIVERSITY OF NEUCHÂTEL, SWITZERLAND

I. Service Convention and technology

The *Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (the "Service Convention") has as its main objective the setting up of a system for transmission of documents for service abroad.[114] More specifically, the Service Convention aims: "a) to establish a system which, to the extent possible, brings actual notice of the document to be served to the recipient in sufficient time to enable him to defend himself; b) to simplify the method of transmission of these documents from the requesting State to the requested State; [and] c) to facilitate proof that service has been effected abroad, by means of certificates contained in a uniform model."[115] The Service Convention contains rules of international cooperation whose purpose is to facilitate the transmission of a document from one Contracting Party to another. It does not, however, deal with the way to serve the document to the addressee, as this is a matter of domestic law.

The Service Convention was conceived at a time when the international transmission of documents could only be made by postal mail. Nonetheless, it has the particularity of allowing the transmission of documents by any appropriate means, without providing any specific method for the transmission. The primary requirement is that the transmission of a document abroad must be made as soon as possible.

The operation of the Service Convention has been reconsidered in light of the technological developments that have occurred since its adoption, so as to incorporate the possibility to transmit documents by fax, and then by e-mail.[116] It was noted during a Special Commission meeting in 2003 that "the spirit and letter of the [Convention] do not constitute an obstacle to the usage of modern technology and that [its] application and operation can be further improved by relying on such technologies."[117] For this reason, "the operation of the Convention [is] to be considered in light of a business environment in which use of modern technology [is] now all pervasive, and that the electronic transmission of judicial communications is a growing part of that environment."[118] The Special Commission concluded that "the transmission of documents internationally for the purposes of the Convention can and should be undertaken by IT-Business methods including e-mail."[119] It was thus recognized that the use of the Internet could facilitate the transmission of

114 HCCH, *Practical Handbook on the Operation of the Service Convention*, The Hague, 2016 (the "Practical Handbook"), No 9.

115 *Ibid.*, No 6, with reference to V. Taborda Ferreira, "Rapport explicative", in *Actes et documents de la Dixième session (1964),* Tome III, *Notification*, The Hague, 1965, pp. 363 f.

116 See Practical Handbook (*op. cit.* note 114), Annex 8, Nos 1-9.

117 HCCH, Conclusions and recommendations adopted by the Special Commission on the practical operation of The Hague Apostille, Evidence and Service Conventions (28 October to 4 November 2003), October 2003 (the "Conclusions and recommendations 2003"), No 4.

118 *Ibid.*, No 59.

119 *Ibid.*, No 62.

information internationally and thereby the cooperation between the authorities of the Contracting Parties. This would greatly improve the overall operation of the Service Convention.

However, the Special Commission already noted in 2003, and again in 2009, that the use of e-mail, or even fax, for the transmission of documents abroad was not yet possible in all Contracting Parties.[120] It thus appears that the transition of the Service Convention to the technological environment is difficult to achieve in practice. The recent evolution of computer technology induced by blockchain technology could favor this transition by providing a digital environment that guarantees the security requirements necessary for the application of the Service Convention.[121]

The use of electronic means for the service of documents to the addressee is of course a desirable development. Whereas technologies such as e-mail or fax could greatly benefit the Service Convention by improving the speed of delivery and simplifying the process, blockchain technology would combine those advantages while providing increased security to the electronic service of documents to the addressee. In this paper, we will explore this possibility by examining whether the use of blockchain technology for the transmission of documents abroad could improve the practical operation of the Service Convention while guaranteeing sufficient security to the Contracting Parties to the Convention. The question of the actual process of transmission will not be elaborated in this paper.

After these introductory remarks about the use of technology in the context of the Service Convention (I), a brief description of blockchain technology will clarify the main features of this new technology (II). On this basis, we will then examine whether and how blockchain technology can be used for the service of documents abroad (III). We will conclude these first academic thoughts on the use of blockchain technology to improve the operation of the Service Convention with a few practical remarks (IV).

II. Blockchain technology in a nutshell

Since the compatibility of blockchain's architecture with the Service Convention will be examined, it is necessary to briefly review the basic characteristics of this technology.[122] The following observations will use the Bitcoin[123] model as a reference to describe the technical aspects of this technology. Bitcoin is a blockchain designed as a money transfer system that works with bitcoin, the most capitalized cryptocurrency. It should be noted that other blockchains may differ from this reference model on certain technical or conceptual points.

---

120 *Ibid*., No 64; HCCH, Conclusions and recommendations of the Special Commission on the practical operation of The Hague Apostille, Service, Taking of evidence and Access to justice Conventions (2 to 12 February 2009), February 2009 (the "Conclusions and recommendations 2009"), No 38.

121 Although security requirements should not be stricter than those currently existing for paper transmission: Practical Handbook (*op. cit*. note 114), Annex 8, No 14.

122 This Chapter is inspired from F. Guillaume, "L'effet disruptif des smart contracts et des DAOs sur le droit international privé", in A. Richa/ D. Canapa (eds), *Droit et économie numérique*, Lausanne 2020 (forthcoming).

123 Hereafter, "Bitcoin" will refer to the Bitcoin blockchain and "bitcoin" will refer to the bitcoin cryptocurrency. The same logic will be followed with other cryptocurrencies and their underlying blockchains.

a) Genesis of blockchain

Blockchain is presented by specialists as a technology that is driving a revolution on the Internet by enabling the creation of a new generation of distributed and cryptographically secure computer programs. Above all, this technology is at the origin of a new low-cost money transfer system, operating without financial intermediaries, and freely accessible from anywhere in the world and to anyone equipped with an electronic device connected to the Internet (e.g., a computer or a smartphone). Bitcoin[124] is the first publicly known use of blockchain technology. It serves as a large-scale international currency where money transfers take place on a cryptographically secure distributed ledger. Bitcoin has the particularity of being, so to speak, "issued" by blockchain technology. Unlike State-issued fiat currencies, no central regulatory authority has control over bitcoin and it is not legal tender. Therefore, the bitcoin rate cannot be controlled by a State authority (e.g., a central bank). Bitcoin has profoundly changed the financial ecosystem, which has led to blockchain being labeled as a "disruptive technology."[125]

Since the launch of Bitcoin in 2009,[126] many more blockchains have been released with their own cryptocurrencies. Ethereum was launched in 2015 and its ether is the second largest capitalized cryptocurrency.[127] Ethereum differs from Bitcoin in that it pursues a different objective than simply transferring money. This blockchain has been developed in order to facilitate the implementation of a second layer of programming that allows the transfers of cryptocurrencies to be automated. The possibility of introducing a computer program, referred to as a "smart contract,"[128] which, in particular, allows a transfer of cryptocurrencies to be made conditional on a series of rules, has opened up new perspectives for the use of blockchain technology. This kind of application has attracted the attention of lawyers, as smart contracts can be used in contractual matters as a means to perform the financial obligation provided for in a contract, or even to "digitalize" a contract or to create a "digital contract."[129]

b) Basics of blockchain

Blockchain is a distributed ledger technology.[130] This is a data management model in which transactions are recorded simultaneously on a great number of computers across the world. The network of computers is organized in a peer-to-peer fashion, which means that the registry containing all transactions is distributed to all computers in the network, removing the need for a centralized record or master copies. The computers are in constant communication and continuously share the state of the blockchain.

---

124 S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, available at: < https://bitcoin.org/bitcoin.pdf > (last consulted on 16 March 2020).

125 A. M. Antonopoulos, *The Internet of Money*, Vol. 1, 2016, Chapter 1: What is Bitcoin?

126 The first block of Bitcoin (the "genesis block") was created in January 2009.

127 V. Buterin, Ethereum White Paper – A Next Generation Smart Contract & Decentralized Application Platform, November 2013, available at: < https://www.blockchainresearchnetwork.org/wp-content/plugins/zotpress/lib/request/request.dl.php?api_user_id=2216205&dlkey=LIWF7NVA&content_type=application/pdf > (last consulted on 16 March 2020).

128 The term "smart contract" was coined by NICK SZABO, "Smart Contracts": Formalizing and Securing Relationships on Public Networks, First Monday, Vol. 2, 1st September 1997, available at: < http://firstmonday.org/article/view/548/469 > (last consulted on 16 March 2020).

129 See *e.g.*, F. Guillaume (*op. cit.* note 122), (forthcoming).

130 See *e.g.*, F. Guillaume, "Aspects of private international law related to blockchain transactions", in D. Kraus, T. Obrist and O. Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, Cheltenham/Northampton, 2019, pp. 49-82, at pp. 54-56.

Blockchain is a decentralized technology entirely managed by the community of users who hold amounts of cryptocurrency. The fact that the network does not need to be managed by a central institution (e.g., a bank or any other financial intermediary) is a key feature of this technology. Unlike digital platforms such as Uber or Airbnb, blockchains can be managed independently without the intervention of an intermediary.

Blockchain works according to a system of distributed trust between users. Its use does not require trust to be placed in a central institution or in the other party to the transfer of cryptocurrencies. Each user can have a copy of the blockchain on his or her own computer and can thus check by himself or herself the validity of all the transactions carried out. The transaction register (i.e., the blockchain ledger) is indeed public. Bitcoin has introduced a paradigm shift in the financial ecosystem by transferring the trust that was placed in the central authorities (or trusted third parties) to the computer system itself.

Transactions are carried out through several stages of a decentralized consensus mechanism, which provides the trust necessary for the operation of the entire cryptocurrency transfer system.[131] The validity of a transaction is first verified by the computers on the network. They identify the accounts participating in the transaction on the basis of an electronic signature attached to each account, which is composed of a set of two cryptographic keys that guarantee the anonymity of the account holder.[132] The transaction is then integrated into a block of several transactions that are validated simultaneously by a computer or, more generally, a group of computers that have managed to find at random a sequence of digits that allows the system to validate the block. As soon as the block is validated, it is added to the chain and linked to the previous block so as to make up the chain of blocks constituting the transaction register. Computers validating transactions are referred to as "miners." They are paid both by the participants and by the system, which "issues" new units of bitcoin to pay for their work.

Within Bitcoin, all participants are treated equally. This blockchain is accessible to everyone and anyone can make transactions without being limited by State borders. The computers in the network can also be located anywhere. Bitcoin is not subject to any central authority, government, or central bank control. The network is censorship resistant as no one has the power to change the rules of the system or deny access to an individual. It is virtually impossible to exercise power or control over the Bitcoin blockchain, either by preventing transactions or by modifying transactions that have already taken place.[133] Once a transaction is recorded on the blockchain, it is time-stamped, tamper-proof, and cannot be corrupted nor deleted.[134]

---

131 There are several types of consensus mechanisms. Bitcoin uses Proof of Work (PoW), which is still the mechanism used by major blockchains.

132 Each Bitcoin user has (at least) one Bitcoin identity resulting from a set of two cryptographic keys. The person transferring bitcoin units must sign the transaction with his or her private key. The associated public key allows computers on the network to identify the user's account and to verify the validity of the transaction. The recipient's public key is embedded in the transaction so that, after it is added to a new block and validated by the minors, the recipient is able to retrieve the transferred units of bitcoin by using his or her own private key.

133 It should be noted, however, that a powerful miner (or several miners working together) can take control of Bitcoin by controlling 51% of the mining activity. The control of the mining activity would grant the power to block new transactions or double spend units of bitcoin. This attack, which is theoretically possible but considered unlikely, is referred to as the "51% attack". See K. Werbach, "Trust, But Verify: Why the Blockchain Needs the Law", *Berkeley Technology Law Journal* 2018, Vol. 33, pp. 489-552, at pp. 515-517.

134 See A. M. Antonopoulos (*op. cit.* note 125), Chapter 1.4; Legaler, Blockchain for Lawyers, 2018, available at: < https://www.legaler.com/wp-content/uploads/2018/12/Blockchain-for-Lawyers-eBook.pdf?utm_medium=email&utm_campaign=eBook%20Delivery&utm_content=eBook%20Delivery+&utm_s

c) Access to blockchain

The basic blockchain characteristics described above took Bitcoin as a reference model. This blockchain is a permissionless computer network, meaning that anyone can access it to make transactions at any time and from any location, without the need for permission. Bitcoin is also open source, which means that anyone has access to its software code and any computer developer can make improvement proposals to the network[135] or reproduce the software code to run a new blockchain. Ethereum, as well as many other blockchains, are similar open networks.

Some blockchains deviate from this reference model by being managed by a central authority. This type of blockchain is usually developed by a State, a company or a bank, which retains control over the system and manages access rights. These permissioned blockchains are not open networks: access is subject to authorization and the code is usually not open source.[136] An example is the (future) blockchain Libra from Facebook.

Unlike permissionless blockchains, which guarantee (at least in theory) the anonymity of users, permissioned blockchains typically require users to provide identification. Furthermore, this blockchain model is not censorship resistant as the system is controlled by a central authority. Moreover, unlike the Bitcoin reference model that has been deployed internationally, permissioned blockchains can be bounded by State borders. For example, the central authority can allow access to the blockchain only to persons residing in a particular State. This model usually limits the number of computers in the network, in particular the number of miners, and restricts their location within the territory of one single State. When the nodes running a blockchain are contained within the borders of a single State, the security of the whole network is compromised. The integrity of a permissioned blockchain may be completely at risk, for example, when the State in which the nodes are located declares any use of a blockchain illegal in order to preserve its national economy, prohibits mining activity for environmental reasons, or orders a general shutdown of the Internet[137] due to disturbances on its territory. Permissioned blockchains offer, paradoxically, a lower level of security than permissionless blockchains.

There is a fundamental conceptual difference between permissionless and permissioned blockchains. The launch of Bitcoin is part of an ideology that sees blockchain technology as a means of freeing oneself from the power of States and financial intermediaries.[138] The initial objective was to create the foundations for a new, self-sustaining economic model, by setting up a payments system (Bitcoin) over which governments and central banks could not exercise control. By reintroducing a trusted third party into the system, permissioned blockchains create an environment that loses its open access and neutrality, presents a risk of censorship, is not public, and is not necessarily cross-border. The more nodes exist in the network and the more decentralized the power over the network is, the safer a blockchain can be considered. Permissionless blockchains

ource=CM&utm_term=Click%20Here%20to%20Download%20eBook > (last consulted on 16 March 2020), p. 11; WERBACH (note 133), pp. 523 f.

135 Program updates are done by Bitcoin Improvement Proposal.

136 It is, of course, also possible to launch "mixed", partially open blockchains, for example by providing an authorization system to access them while leaving the code open source.

137 Recent events have shown that Internet shutdowns are becoming more and more frequent, in particular for political reasons.

138 S. Nakamoto (*op. cit.* note 124).

that follow Bitcoin's model are, for this reason, considered by purists to be the only "true" blockchains.[139]

III. Blockchain technology for the service of documents abroad

Blockchain technology is a major step in the evolution of information technology that cannot be ignored. Any plans to create a new system of international service of documents must take this recent technological development into account.

a) What improvements could blockchain make?

The Service Convention is part of a set of international conventions which are fundamentally aimed at ensuring access to justice across the world and facilitating the conduct of international civil proceedings. More specifically, this Convention aims to set up a system which ensures the service abroad of documents in a simple, efficient, and secure way that makes it easy to prove that the documents have been properly served. It is worth examining how blockchain technology could fulfil these fundamental objectives pursued in the context of the international service of documents.

Blockchain technology has the advantage of being extremely secure, and once information is put on a blockchain, it is time-stamped and tamper-proof. These two basic features of blockchain technology meet the essential conditions required for the transmission of documents for service abroad. Furthermore, the information stored on a blockchain could be easily accessible to authorities from anywhere in the world. Authorities could take immediate notice as the system would be accessible twenty-four hours a day, seven days a week. The use of blockchain technology would thus increase security, efficiency, and speed in the international system of service of documents set up by the Service Convention.

Considering the above, the use of blockchain technology for the transmission of all the documents that must be served abroad under the Service Convention could greatly benefit all Contracting Parties. If Contracting Parties were to jointly use blockchain technology in order to serve documents abroad, they would be operating on a widely accessible and secure network distributed across the world.

b) Permissioned or permissionless blockchain?

If the use of blockchain technology is considered in order to improve the operation of the Service Convention, the development of a permissioned blockchain would most likely be the first option examined. In this way, full control over the nodes of the network could be retained and the entire system could be maintained by the Permanent Bureau of the HCCH, a Contracting Party, or a central body to be determined. A permissioned blockchain is understandably the first type of blockchain that comes to mind when planning the development of such a system as part of the operation of an international convention.

However, while the need for control over the network by an authority seems evident in this context, the centralization of a permissioned blockchain poses security risks. This is

---

[139] Andreas Antonopoulos has defined the five pillars of a "real" blockchain, according to which a blockchain must be open, borderless, neutral, censorship resistant, and public. See A. M. Antonopoulos, The Five Pillars of Open Blockchains, 11 May 2019, available at: < https://www.youtube.com/watch?v=qlAhXo-d-64 > (last consulted on 16 March 2020).

due in particular to the limited number of nodes involved in the validation process of the blocks containing information and the centralization of their location. Unlike Bitcoin, which runs on an extremely large network of nodes that can be freely joined by users all across the world, a permissioned blockchain limits the number of nodes, which usually results in a small and centralized network. This centralization makes the network more prone to attacks, and information can be more easily corrupted as an attack would have to be launched on a limited number of nodes.

In addition, if all nodes are located in the same State, security risks are all the more increased. We could indeed imagine the possibility that access to the network, or to the Internet in general, could be restricted for any given reason in the State that hosts the nodes that validate the operations on the blockchain. A permissioned blockchain could also carry the risk of being censored by that government. In those two cases, there would be a risk that the entire system of international service of documents would be blocked.

By contrast, the use of a permissionless blockchain would significantly reduce security risks and would provide Contracting Parties with the full benefits of this new technology. The system would be fully decentralized, that is to say that data would be encrypted and then securely recorded in multiple places at the same time without a central data store and without any master copy. The multiplication of nodes, which could be located anywhere in the world, would provide the necessary degree of security to guarantee the availability and integrity of the information. All Contracting Parties could always have access to the information at any time, as a permissionless blockchain would not centralize control over the system in the hands of a particular State or a limited number of States. In addition, due to the distribution of data, the information stored could not be tampered. Those elements are essential when it comes to securely transmitting electronic data in a confidential manner at the global level.

Furthermore, by choosing to run the system on a permissionless blockchain, existing blockchains such as Bitcoin or Ethereum could be integrated in the data transmission process. This would significantly reduce development and operating costs as the most sensitive element of the system would be, so to speak, outsourced to an existing network which entails very little operating costs.

In our opinion, developing a permissioned blockchain would make as much sense as if a State were to create a private network similar to the Internet in order to share information at the international level.[140] Indeed, a permissioned blockchain would be a mere private network comparable to the Internet of the first age. The use of a permissionless blockchain as a new channel of transmission of documents in the context of the Service Convention would be the best way to provide Contracting Parties with a cost-efficient system that guarantees the integrity and availability of information.

However, we have to admit that relying on a permissionless blockchain for the data transmission process would result in a significant change in the operation of the Service Convention, as the system that would be used for the transmission of documents abroad would be partially outside the control of State authorities. The use of a decentralized technology means that States would no longer need to trust other States to establish a channel for communication and certification of information. But rather, States would trust blockchain technology to ensure the availability, authenticity, and integrity of the information issued and received. Furthermore, States would be bound by the available

[140] It should be noted, however, that some States are increasingly claiming the right to control and regulate the Internet. A permissionless blockchain would clearly run counter to this trend as it would not allow a top-down control of the system by governments.

technology offered by the chosen blockchain serving as the underlying network for the transmission of documents abroad. States would have no means to directly improve technical characteristics of the Bitcoin or Ethereum blockchain, such as scalability. This, however, would not mean a revolution in the way States operate. For example, State authorities commonly use the Internet as a means to transmit confidential information, even if they do not have full control over the network.

The use of a permissionless blockchain does not mean that the data transmitted in the context of the Service Convention would be accessible to all: encryption can guarantee the confidentiality of information. It is possible, for example, to use blockchain technology to create digital identity cards that are certified by a State with a digital seal. The system allows the information to be restricted so that only specific data is available. Similarly, access to information may be limited for each step of the transmission process of a document by determining what information is available and to whom. Confidentiality would therefore be ensured even if data was transmitted on a permissionless blockchain.

There are multiple possibilities to combine permissioned and permissionless blockchains, or even to combine blockchain technology with other systems, in order to take advantage of the characteristics of this new technology while obtaining various degrees of control over the system and distribution of data. Further research into blockchain technology could lead to finding a system that would provide the right levels of safety and control in order to meet the specific needs of Contracting Parties in the context of the Service Convention.

c) Does blockchain comply with the rules of law?

Relying on blockchain technology for the transmission of documents in accordance with the Service Convention would only be possible if the resulting system would conform at least to the principles of non-discrimination, technological neutrality, and functional equivalence. These three principles, which were first adopted in the UNCITRAL Model Law on Electronic Commerce, are considered fundamental when examining the compatibility of an electronic technology with the rules of law.

Under the principle of non-discrimination, the use of electronic means of communication shall not be discriminated against.[141] Therefore, the transmission of a document should not be denied legal effect, validity, or enforceability solely on the grounds that it took place on a blockchain. The use of blockchain technology does not preclude the transmission of a "written document" since the information is accessible so as to be usable for subsequent reference.[142] According to the principle of non-discrimination, the electronic transmission of the request for service, which consists of the model form and the documents to be served, must be considered as valid. Similarly, the requirement for an "original document" is met if there is a reliable assurance as to the integrity of the information from the time when it was first generated in its final form and if that information can be displayed to the person to whom it is to be presented.[143] Blockchain technology makes it possible to generate information that is time-stamped and tamper-proof, which clearly meets the requirements set out by the Service Convention as regards the formal requirements relating to the documents to be served. The use of blockchain technology

141 See *e.g.,* Art. 5 and Art. 11 of the UNCITRAL Model Law on Electronic Commerce; see also Art. 8 of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

142 See *e.g.,* Art. 6 of the UNCITRAL Model Law on Electronic Commerce.

143 *Ibid.,* Art. 8.

can guarantee a higher level of security with greater efficiency and speed than the channels of transmission that are currently in use, in particular as regards the identification of the source and the content of the documents transmitted.

The Service Convention does not specify how the transmission of documents is to be performed, leaving room for the use of modern technology. From today's point of view, the Service Convention follows the principle of technological neutrality (even if this was not intended at the time of its adoption). The neutrality of the rules of the Service Convention makes it possible to take account of technological developments without the need for a revision of its text. The opportunities provided by the drafting of the Service Convention should be seized to make the most of modern technology. The use of new technologies should be considered in order to improve the operation of the Service Convention, in particular if the transmission process can be made faster.[144] A paperless transmission of documents would definitively foster the efficiency of international service of documents. The use of a technology such as blockchain, which permits instant transmission of documents from one State to another, would significantly improve the usefulness of the Service Convention.

The Special Commission proposed to examine each channel of transmission of documents provided for in the Service Convention by taking into account an approach based on the principle of functional equivalence as well as the objective pursued by the channel and its relevant requirements.[145] According to the principle of functional equivalence, the transmission of documents by electronic means may be regarded as equivalent to the transmission in paper form if it fulfils the same purposes and functions.[146] For example, the interpretation under the functional equivalence approach of the term "postal channels" found in Article 10(a) of the Service Convention allows us to consider that this channel of transmission could include fax, e-mail, SMS or the posting of a message on a website.[147] Likewise, the requirement of transmission of the judicial document or a copy in duplicate under Article 3(2) of the Service Convention must be interpreted according to the functional equivalence approach when the transmission is carried out by electronic means. Indeed, "[a]s a document transmitted by electronic means can usually be duplicated (copied and printed out) at any moment and an unlimited number of times, the requirement of a copy or duplicate will be satisfied by the sending of a single message".[148]

In accordance with the functional equivalence approach, the purposes and functions of the requirements set out in the Service Convention for the transmission of documents abroad should be examined in order to determine whether transmission via blockchain can fulfil those purposes and functions. For example, the "signature" of a document serves two essential functions: to identify the author and to confirm that the author agrees with the content of the document.[149] Blockchain technology respects these essential legal functions of a signature, as the use of a set of two cryptographic keys makes it possible to identify

144 See Practical Handbook (*op. cit.* note 114), Annex 8, No 11 f.

145 *Ibid.*, Annex 8, No 8.

146 See Art. 9(2) of the United Nations Convention on the Use of Electronic Communications in International Contracts: "Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference."

147 However, Contracting Parties have divergent views on this topic. See Practical Handbook (*op. cit.* note 114), Annex 8, No 35-37.

148 *Ibid.*, Annex 8, No 18.

149 See *e.g.,* the UNCITRAL Model Law on Electronic Signatures (2001). See also Art. 7 of the UNCITRAL Model Law on Electronic Commerce, and Art. 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts.

with certainty the sender of the message and to indicate that the sender approves the information contained in the message.[150] The Special Commission has already acknowledged that requests for service may be converted from paper into electronic form by scanning, or issued directly in electronic form, and signed in both cases by means of an electronic signature.[151] Those examples show that the principle of functional equivalence allows us to interpret the Service Convention in such a way that service of documents abroad can be achieved by using blockchain technology, without the need to revise the text of the Convention.

IV. Facing a new reality

Blockchain technology has all the characteristics necessary to simplify the service of documents abroad and improve the operation of the Service Convention. As of today, blockchain is probably the most suitable technology for transmitting documents abroad with efficiency, security, and speed. This technology has the potential to take the Service Convention out of an ancient world of papers and borders and propel it into the digital space.

The service abroad of documents using blockchain technology could probably be easily adopted in some States that already have a widespread use of computer technology. But it has already been observed that the transmission of documents by fax or by e-mail is not possible in all the Contracting Parties.[152] The fact that there is currently a discrepancy between Contracting Parties in the way in which they put into practice the channels of transmission provided for under the Service Convention does not seem to be a real obstacle to the adoption of blockchain technology. In countries facing difficulties in using electronic means for transmitting documents in accordance with the Service Convention, it is quite conceivable that the implementation of a new system for the operation of the Convention could be less complicated than in other countries that already use electronic means for the service of documents abroad. It may be easier to directly adopt a new technology than to deviate from a well-established practice. For example, in some countries, people have moved directly from a cash-based payment system to a smartphone payment system without ever switching to credit cards. Since a blockchain can be accessed with existing electronic devices connected to the Internet, such as a smartphone or a computer, the adoption of this technology for the service of documents abroad might turn out to be easier than one might think. This transition would be summarized in developing a user-friendly interface running on blockchain technology. This should be possible without too many practical difficulties, in particular if it can be carried out in a cost-efficient manner.

Contracting Parties that have a long-established practice for the transmission of documents under the Service Convention may be more reluctant to switching to a new channel of transmission. For example, in the field of legalization for foreign public documents, Switzerland is one of the first signatory States of the Apostille Convention that has been applied in this country since 1973. As of today, Swiss authorities do not use the electronic apostille register regardless of the obvious practical advantages it offers. In practice, a paper document on which the apostille is placed is indeed still required in most cases. However, Switzerland is not recalcitrant to the use of the Internet to facilitate communication between litigants and the authorities. Electronic communication with civil

150 See *e.g.,* Art. 6 of the UNCITRAL Model Law on Electronic Signatures: digital signatures based on cryptography enter into the scope of application of this model law.

151 See Practical Handbook (*op. cit.* note 114), Annex 8, No 13.

152 Conclusions and recommendations 2003 (*op. cit.* note 117), No 64; Conclusions and recommendations 2009 (*op. cit.* note 120), No 38.

courts has been allowed for many years, which enables service via electronic means.[153] However, even if e-mails are broadly used in Switzerland, litigants rarely use this means of communication and remain attached to paper when it comes to communicating with each other and with civil courts. These examples show that the implementation of a new system can be challenging, and it can only be achieved if users are willing to use it, especially when the system being changedworks.

The use of a new technology requires a change in mentality. The establishment of a global system of service of documents via blockchain could only work if all the parties to the Service Convention agree to give up on the use of paper and join this new electronic system. The greatest challenge would certainly not be the development and implementation of a new system, but its adoption by Contracting Parties. The revolution brought by blockchain technology is that the less the system can be controlled and the more distributed the data is, the more secure the network becomes. This new reality could initiate a paradigm shift in international civil proceedings if States were to recognize that security and integrity are not necessarily linked to centralization and control, but rather to decentralization of power and distribution of data. The transmission of documents to be served would no longer be hampered by State borders if documents could freely transit to their recipient on a distributed global network. This would significantly facilitate and secure international civil proceedings. However, such improvements can only be reached if both States and litigants switch to a new way of thinking.

153 See Art. 139(1) of the Swiss Civil Procedure Code (SR 272): "With the consent of the person concerned, summonses, rulings and decisions may be served electronically. They must bear an electronic signature […]."

IS THE SERVICE CONVENTION READY FOR EARLY RETIREMENT AT AGE FIFTY-FIVE? OR CAN IT BE "SERVICEABLE" IN A WORLD WITHOUT BORDERS?

BY LOUISE ELLEN TEITZ [*]

Turning fifty-five in the United States is often an age for reflection on past accomplishments, for looking to the future and trying to resolve uncertainties, and sometimes even for early retirement. The question is what is the role for the Hague Service Convention in this age of technology?[154]

The completion of the Service Convention in 1965 was not only a major milestone for the Hague Conference, it was also a definitive time for the United States and its relationship with the Hague Conference. It was the first convention during which the US participated actively as a member in the HCCH, and when the US ratified the convention, it was the first multilateral treaty it signed onto with respect to international judicial procedure.[155] The Service Convention also appears to be the first HCCH convention to have a Special Commission to focus not on amendments or a protocol, but on using the existing machinery of the convention more effectively – a model that has been followed with other HCCH conventions.[156] Special Commissions for the Practical Operation of a convention have become a mainstay with conventions and post-convention services being a practical way to increase efficiency and consistency in application and practice.[157]

---

[*] Professor of Law, Roger Williams University School of Law, Bristol, Rhode Island. She served as First Secretary at the Hague Conference from 2011-14. The author gratefully acknowledges the research assistance of Tatiana Maria Gomez, RWU Class of 2021. Thanks also to Hans van Loon, former Secretary General of the Hague Conference and Prof. David Stewart, Georgetown Law School.

[154] The current Secretary General, Dr. Christophe Bernasconi, has been very instrumental in incorporating and addressing new technologies for older conventions, as seen in his work with the even older Hague Apostille Convention from 1961 and the creation of an electronic apostille program, e-App.

[155] *HCCH Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters*, available at: < https://www.hcch.net/en/instruments/conventions/full-text/?cid=17 > (hereinafter Service Convention). Congress approved U.S. participation in the Hague Conference and UNIDROIT on December 30, 1963 (P.L. 88-244), discussed in S. Exec. Rep. No. 6, 90th Cong., 1st Sess. 5-6 (1967).

[156] HCCH, Report on the Work of the Special Commission on the Operation of *the Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (1977) 2 ("This was the first time that a Special Commission had met within the Conference in order to discuss the operation of a Hague Convention.")

[157] See *Actes et Documents de la quatorzième Session: Miscellaneous Matters (1980)* at Tome I-70 ("The fourteenth session […] expresses the wish that the Secretary General of the Hague Conference may convoke at regular intervals Special Commissions to study the practical operation of Conventions and Recommendations […]"). The first convention that seems to have created an explicit provision for the convening of a Special Commission at regular intervals was the Hague Convention on Protection of Children and Cooperation in Respect of Intercountry Adoption Art. 24, available at the following address < https://www.hcch.net/en/instruments/conventions/full-text/?cid=69 >. However, even before this Convention, there were earlier Special Commissions for the Service, Evidence, and 1980 Child Abduction Conventions. Most modern conventions provide for future review in their text. *See, e.g.,* HCCH 2005 Choice of Court Convention, Art. 24, June 30, 2005, available at: < https://www.hcch.net/en/instruments/conventions/full-text/?cid=98 > (hereinafter Choice of Court Convention); *HCCH Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters*, Art. 21, available at: <https://www.hcch.net/en/instruments/conventions/full-text/?cid=137> (hereinafter Judgments Convention).

There has been a significant amount of discussion and writing about ways to integrate new technologies into the Service Convention, ranging from using email to blockchain, as well as on some of the attendant concerns raised by the use of technology, such as security and fairness.[158] Setting aside new technologies, how should we "retool" the text and its existing language and dress it up for the new world of e-technology? The Convention was drafted in a time when borders mattered in a world that was based on respect for territoriality and sovereignty.[159] How do we take a text from paper into the world of borderless cyberspace and electronic communications? How do we give "functional equivalence" and go from "mail" under Article 10(a) to email and beyond?[160] Or take a brick-and-mortar address and replace it with the functional equivalent of an email address or website?[161]

158 See generally D P Stewart and A Conley, "E-Mail service of foreign defendants: Time for an international approach?", *Georgetown Journal of International Law*, vol. 38, 2007, p 755; F. Guillaume, Panelist Remarks at the HCCH aBridged: Innovation in Cross-Border Litigation and Civil Procedure Conference (11 December 2019) (discussing blockchain technology and fairness concerns), available at: <https://www.hcch.net/en/instruments/specialised-sections/service/hcch-a-bridged/>; F. Conley, "Service with a Smiley: The Effect of E-Mail and Other Electronic Communications on Service of Process", *Temple International and Comparative Law Journal*, vol. 11, 1997, p 407; M. O. Eshleman and S. A. Wolaver, "Prego Signor Postino: Using the Mail to Avoid the Hague Service Convention's Central Authorities", *Oregon Review of International Law*, vol. 12, 2010, p. 283, 311-315 (discussing the possibility of service by "electronic 'postal channels,'" like email); R. J. Hawkins, "Dysfunctional Equivalence: The New Approach to Defining "Postal Channels" Under the Hague Service Convention", *UCLA Law* Review, vol. 55, 2007, p 205.

159 The text of the Convention has an explicit provision and reference to infringing on sovereignty or security as a grounds for refusing to make service. Service Convention, *supra* note 155, Art. 13. This argument has been used by the German government in refusing class action service in cases such as the US suit against Bertelsmann in connection with Napster where Bertelsmann sought an injunction against service under Art. 13. Petition of Bertelsmann A.G., Bundesverfassungsgericht Germany [2003] 2 BverfG 1198 (25 July 2003). A translation by Andreas Lowenfeld appears in his book, *International Litigation and Arbitration* (3rd ed, 2006) 256. The availability of the Service Convention in class actions was specifically endorsed in the 2009 Special Commission: "The SC notes that the Convention is applicable to a request for service upon a defendant in a class action." HCCH, Conclusions and Recommendations of the Special Commission on the Practical Operation *of the Hague Apostille, Service, Taking of Evidence, and Access to Justice Conventions* (2009), available at: <https://assets.hcch.net/upload/wop/jac_concl_e.pdf> (last consulted on 21 April 2020). See also T. Folkman, "Case of the Day: Rockefeller v. Changzhou SinoType" (Letters Blogatory, 13 April 2020) available at: <https://lettersblogatory.com/2020/04/13/case-of-the-day-rockefeller-v-changzhou-sinotype> (last consulted on 20 April 2020) (discussing sovereignty as a goal of the Service Convention in the context of a recent California decision).

160 One of the earliest examples of legal attempts to deal with the concept of functional equivalence between actual writing and electronic form was in UNCITRAL's Model Law on Electronic Commerce (1996) designed to avoid discrimination between electronic and written text. "The MLEC was the first legislative text to adopt the fundamental principles of non-discrimination, technological neutrality and functional equivalence that are widely regarded as the founding elements of modern electronic commerce law." United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Commerce", available at: <https://unictral.un.org/en/texts/ecommerce/modellaw/electronic_commerce> (last consulted on 21 April 2020).

161 For United States cases wrestling with the problem of fitting together electronic forms of communication and the Service Convention, *see e.g., Luxottica Grp S.p.A. v. P'Ships & Unincorporated Ass'ns Identified on Schedule "A"*, 391 F. Supp. 3d 816 (N.D. Ill. 2019) (deeming service by email to defendants in a contracting state insufficient and thus granting defendant's motion to dismiss due to plaintiff's non-compliance with the Service Convention); *Keck v. Alibaba.com, Inc.*, 330 F.R.D. 255 (N.D. Cal. 2018) (denying a motion to allow service by messaging services provided by Alibaba.com and Aliexpress.com); *NOCO Co. v. Shenzhen Anband Tech.,* No. 1:17CV2205, 2018 U.S. Dist. LEXIS 44545 (N.D. Ohio Mar. 19, 2018) (granting a motion to serve defendant in a contracting state by email and Amazon's message center); *Lipenga v. Kambalame*, No. GJH-14-3980, 2015 U.S. Dist. LEXIS 172776 (D. Md. Dec. 28, 2015) (granting a motion to serve a defendant in a contracting state by email and Facebook messenger); *Rio Props. V. Rio Int'l Interlink*, 284 F.3d 1007 (9th Cir. 2002) (allowing email service in a case involving a defendant from a non-signatory country to the Service Convention).

One can see the tensions when one looks at the Service Convention, past and future—taking a sort of Janus approach. The Service Convention chapeau speaks of its goals of making sure the addressee has timely notice (avoiding *notification au parquet*) and of improving mutual judicial assistance by simplifying and expediting procedures. Indeed, in 1965, the use of the Central Authority to facilitate diplomatic boundaries was "modern." The goals for the Service Convention included meaningful and timely notice while "simplifying and expediting the procedure."[162] But in 1965, there was also a strong sense of sovereignty and concern with not violating the territory of others. How do we balance these goals and still maintain the integrity of the Convention — that is, the desire for efficient notice and yet respect for territoriality? The former goals can be accommodated perhaps by an "interpretation" of the text as discussed below, but the latter sovereignty concerns may require something more formal in the form of hard law, or at least something more solid than soft law.

I. Options for a Facelift for a Middle-Aged Text

I want to explore several potential ways to "update" the Service Convention, starting with the hard-law options and moving down the spectrum towards less binding soft-law.

Let's start with hard-law and the possibility of a protocol that would address service by new technologies. The most recent use of a protocol in HCCH conventions is with the 2007 Maintenance Convention, but that protocol was negotiated at the same time as the actual convention. The idea of a protocol, albeit one of narrow scope, negotiated fifty-five years after completing a convention, raises all the fears of opening a Pandora's box, especially since the number of member states in the HCCH when it was negotiated was only twenty-three, while today it is eighty-five, and is truly global.[163] Even a minimalist approach to textual changes could be met with skepticism.

On the soft-law side, this Convention already has a new Practical Handbook, although it is not focused on the new technologies issue, at least to the exclusion of non-electronic mechanisms.[164] One could see a more focused and perhaps a bit aspirational product, such as a "Guide to Good Practice" with acceptable practices, perhaps produced at a Special Commission, and including suggested or model language for legislation for individual Contracting States.[165] One could include the Special Commission Conclusions and Recommendations for dealing with new technologies from the last two Special Commissions in 2009 and 2014.[166]

---

162 Service Convention, *supra* note 155.

163 For a timeline showing membership growth by year, see 'Membership Growth' (*Hague Conference on Private International Law*), available at: <https://assets.hcch.net/docs/e11314e9-9453-4f06-b159-fa86d450f9ea.pdf> (last consulted on 19 April 2020).

164 HCCH, *Practical Handbook on the Operation of the Service Convention*, 174-201 (4th ed. 2016) (hereinafter Practical Handbook) (discussing information technology in the context of the Service Convention, including service by electronic means).

165 This approach was used in part in connection with the 1980 Child Abduction Convention Special Commission Part II in January 2012 when there was a lack of consensus for a protocol dealing with the "grave risk" basis for non-return, and a compromise provided for a Guide to Good Practice on Article 13 (1)(b). See HCCH, *1980 Child Abduction Convention Guide to Good Practice: Part VI Article 13(1)(b)*, available at: < https://www.hcch.net/en/publications-and-studies/details4/?pid=6740 >.

166 HCCH, "Conclusions and Recommendations of the Special Commission on the Practical Operation of the Hague Service, Evidence, and Access to Justice Conventions" (2014), available at: < https://assets.hcch.net/docs/eb709b9a-5692-4cc8-a660-e406bc6075c2.pdf > (last consulted on 20 April 2020); HCCH, "Conclusions and Recommendations of the Special Commission on the practical operation of *the Hague Apostille, Service, Taking of Evidence, and Access to Justice*

Perhaps one option is a middle ground of a "Legislative Note" — harder soft law or soft hard law, depending how one views it — as illustrated by the approach taken by UNCITRAL when it, too, had to deal with allowing for electronic technologies in the New York Convention on Recognition and Enforcement of Foreign Arbitral Awards, dating from 1958.[167] The New York Convention contains a requirement of an "agreement in writing" in Article II paragraph 2 and Article VII paragraph 1. The Legislative Note of 7 July 2006 provides an interpretation of these two Articles and the requirement of a "writing", which serves to modernize the text which originally had been designed for traditional means of contracting, but should now be read to incorporate electronic transactions.[168]

This Legislative Note type of approach is not totally alien to the Hague Conference. One example is that in contemplation of the 1986 Sales Convention, there was a Diplomatic Session in 1980 declaring that at the time of negotiation of the 1955 Hague Convention, consumer sales were not as such identified and envisaged, and thus recommended that the Convention should not prevent States from applying special rules for consumer sales.[169] This Declaration and Recommendation was adopted at the Diplomatic Session, meaning it had the official weight of all member countries (then twenty-seven), rather than just their experts.[170]

II. Interpretation—The Other Side of Updating a Text

The other approach to "updating" the Service Convention is to do so through interpretation to reach a "functional equivalence" as discussed in the Practical Handbook.[171] I like to think of it as the "evil stepsisters' approach" in *Cinderella* — trying to squeeze a size 38 foot into a size 35 glass slipper.

Many jurisdictions, including some courts and scholars within the US, have eagerly embraced the interpretation solution to updating the text, construing "postal channels" in Article 10 to include courier services and electronic mail.[172] Many jurisdictions have adapted

---

Conventions" (2009), available at: < https://assets.hcch.net/upload/wop/jac_concl_e.pdf > (last consulted on 20 April 2020).

167 See United Nations Commission on International Trade Law, "Recommendation Regarding the Interpretation of Article II, Paragraph 2, and Article VII, Paragraph 1, of the Convention on the Recognition of Foreign Arbitral Awards" (7 July 2006), available at: < https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/a2e.pdf > (last consulted on 20 April 2020).

168 *Id.* The Legislative Note says it is issued "considering the wide use of electronic commerce," and recommends that the "circumstances described" in Article II, paragraph 2 and Article VII, paragraph 1, not be read as "exhaustive". *Id.* The New York Convention's language contemplates that an "'agreement in writing' shall include an arbitral clause in a contract or an arbitration agreement, signed by the parties or contained in an exchange of letters or telegrams." United Nations Commission on International Trade Law, *Convention on the Recognition and Enforcement of Arbitral Awards* (1958).

169 *Actes et Documents de la Quartorzieme Session: Miscellaneous Matters (1980)*, Tome I, at I-62.

170 *Declaration and Recommendation Relating to the Scope of the Convention on the Law Applicable to International Sales of Goods, Concluded June 15th 1955* (1980). This Declaration was adopted by the XIVth Session in 1980. It declared that the Convention "does not prevent States Parties from applying special rules on the law applicable to consumer sales", and recommended that States Parties "which apply special rules on the law applicable to consumer sales, inform the Permanent Bureau of this fact." *Id.* The Diplomatic Session also adopted a draft text on the law applicable to such consumer sales, but this never made it to a finished convention.

171 The HCCH's "functional equivalence" approach would include "information technologies such as e-mail or fax" as postal channels under article 10(a) so long as states have not objected to the methods, and the documents are "sent by postal agencies." Practical Handbook (*op. cit.* note 164), at 177.

172 *Ibid.*, at 177-180 (discussing the interpretation of "postal channels" to include electronic services like email in both scholarly literature and caselaw). For U.S. cases interpreting "postal channels" to include

their service procedure under the Convention to fit new technologies for the domestic part of the process, as of the moment that the Central Authority has received the request. Indeed, it is ironic that the Convention itself is much more rigid than the internal systems of so many countries which have embraced e-technologies. But in the age of electronic commerce, concerns with security and authenticity are often more significant than speed, especially when borders are being crossed. One wants to be certain that an electronic service is actually received as sent and actually opened, in keeping with the spirit of the Service Convention and its concern with avoiding *notification au parquet*.[173]

Besides interpreting the existing text to accommodate new technologies, some forms of interpretation seek to make the Convention inapplicable to transactions involving the virtual world, as opposed to brick-and-mortar addresses, as the Convention is not applicable when the address of the person is unknown.[174] New technologies also may exacerbate the problem of parties bypassing the Convention through an interpretation of the jurisdictional requirement of having "occasion to transmit a judicial or extrajudicial document for service abroad."[175] While it has been generally agreed that this determination is one of national law, as discussed below in more detail, some countries are creating flexibility that in effect amounts to exclusion of the Convention by applying domestic law.[176] Similarly, courts in some countries are slow to see an "objection" by a country when interpreting Article 10's availability of service by mail (or electronic mail).[177] Some countries and courts are encouraging the waiver of service, either by procedural rule[178] or by contractual agreement, leaving weaker parties to face a possible electronic *notification au parquet*. Looser and broader interpretation means more exclusion from the requirements of the Convention, which may also lead to increased friction among sovereigns.

courier services or email, see, *e.g., TracFone Wireless, Inc. v. Hernandez*, 126 F. Supp. 3d 1357 (S.D. Fla. 2015) (finding that service on a defendant by FedEx delivery is done through a postal channel); *Lexmark Int'l, Inc. v. Ink Techs. Printer Supplies, LLC*, No. 1:10-cv-564, 2013 U.S. Dist. LEXIS 200012 (S.D. Ohio Aug. 21, 2013) (finding both courier service and email service are appropriate under Article 10(a), thus implying that they are both postal channels); *NOCO Co. v. Khaustov*, No. 1:19 CV 196, 2019 U.S. Dist. LEXIS 151413 (N.D. Ohio Sep. 5, 2019) (allowing service by email to a defendant in a signatory country).

173 See *Melia v. Les Grands Chais de France*, 135 F.R.D. 28 (D.R.I. 1991) [hereinafter *Melia*]; V. Taborda Ferreira, "Explanatory Report on the 1965 Hague Service Convention", in HCCH, *Actes et documents de la Dixième session (1964)*, tome III, *Notification*, available at: < https://assets.hcch.net/docs/b6304b87-d5ee-4020-8587-c22ae19ec002.pdf >. See also S. Exec. Rep. *supra* note 155 for a discussion on the importance of avoiding *notification au parquet* as a reason for supporting the U.S. participating in the Service Convention.

174 Service Convention, Art. 1 states: "This Convention shall not apply where the address of the person to be served with the document is not known." Service Convention, *supra* note 155.

175 Service Convention, *supra* note 155, at Art 1.

176 See *Melia, supra* note 173; *Volkswagenwerk Aktiengesellschaft v. Schlunk*, 486 U.S. 694, 699 (1988) [hereinafter *Schlunk*]. *See also infra* notes 188-191 and accompanying text.

177 Many courts in the U.S. have said that service by email or other electronic means is proper even if a country party to the Service Convention has objected to service by postal channels, so long as there is no explicit objection to service by the electronic method used. See, *e.g., WhosHere, Inc. v. Orun*, Civil Action No. 1:13-cv-00526_AJT-TRJ, 2014 U.S. Dist. LEXIS 22084 (E.D. Va. Feb. 20, 2014) (allowing service by email, Facebook, and LinkedIn for a defendant in Turkey because Turkey objected to service by postal channels, but not to service by email or social media); *FTC v. PCCare247 Inc.,* 2013 U.S. Dist LEXIS 31969 (S.D.N.Y. Mar. 7, 2013) (allowing service by email and Facebook messenger for a defendant in India, as India, although it had objected to service by postal channels, had not specifically objected to either method); *Gurung v. Malhotra*, 279 F.R.D. 215 (S.D.N.Y. 2011) (allowing service by email to a defendant in India because India's "objection to postal channels does not amount to an express rejection of service via electronic mail.").

178 See *Fed. R. Civ. P.* 4(d) for an example in the U.S.

III. Increasing Role for Hague Service

Ironically, as virtual environments suggest fewer applications of traditional concepts under the Service Convention, two newer conventions dealing with cross-border conflict resolution highlight the significance of appropriate and deferential service. The Choice of Court Convention ("COCA") in its text highlights the importance of service and notice, and provides a discretionary basis for non-recognition under Article 9 when the form of service in the requested State "is incompatible with fundamental principles of the requested State concerning service of documents."[179] This represents a carefully negotiated provision that reflected the strong concerns of some delegations that service must be made under the Service Convention when applicable (since it is exclusive) and the failure to abide by the Service Convention could provide a basis for non-recognition. This same language, voiced by the same delegations, led to the incorporation of the defense into the 2019 Judgments Convention.[180] This requirement, incorporated into both COCA and Judgments, means that the way one modifies or interprets service under the earlier Service Convention will impact newer conventions, and thus any interpretation has broader implications. The Service Convention will remain an example of what is an acceptable way to serve—what would be "[compatible] with fundamental principles in Contracting States."

IV. Taking Stock of the Convention in the United States

I want to make a few comments on the current status of the Service Convention in one Contracting State, the United States. While the US Supreme Court has affirmed that the Convention is exclusive where it applies,[181] many US courts, both federal and state, have been interpreting, bypassing, or ignoring the Convention for many years, and not always due to the question of new technologies.[182] As discussed below, the new technologies have

---

179 HCCH 2005 Choice of Court Convention, *supra* note 157, at Art. 9(c)(ii).

180 Judgments Convention, *supra* note 157, at Art. 7(1)(a)(ii).

181 *See Schlunk*, *supra* note 176, at 699; *Water Splash, Inc. v. Menon*, 137 S. Ct. 1504, 1507 (2017). See also L. E. Teitz, "Will the Supreme Court Finally Resolve an Almost 30-Year Split Among Circuits on Service of Process Abroad Under the Hague Service Convention?", *Preview of US Supreme Court Cases*, vol. 44, 2017, p 198.

182 Judge Weis, a federal appellate judge, was lamenting this aspect in 1992 when he commented:

"In the absence of energetic judicial direction, the bar has attempted to avoid the Convention's procedures and, instead use the more familiar domestic methods.
[...]
[I]n a recent proposal for amendments to the Rules [of Civil Procedure], the [Advisory] Committee itself drafted an informal waiver procedure that would have bypassed the Convention in a significant number of cases."
Joseph F. Weis, Jr., "Service by Mail—Is the Stamp of Approval from the Hague Convention Always Enough?" (1994) 57 *Law & Contemp. Probs.* 165, 165-66 (1994) (footnote omitted).
For a more recent view, see M. Gardner, "Parochial Procedure" (2017) 69 *Stanford L. Rev.* 941, 996 where the author suggests that "[F]ederal courts are consistently applying the Service Convention." The author, however, does detail "a line of cases that do not require compliance with the Service Convention even when it applies." *Id.* at 998. The article extensively details case law from the last fifteen years and suggests that the application has shown a non-parochial approach, although several of the cases cited do reflect a lack of respect or awareness of the Convention, a situation that is probably also found in state court decisions which are not included in her analysis, since the focus is on the federal rule. *Id.*
Perhaps one of the factors that increases both awareness of and use of the convention is the availability of information and status tables on the HCCH website, making information available that was hard to find twenty years ago. See generally HCCH, available at: < https://www.hcch.net/en/home >.
Ted Folkman's "Letters Blogatory" blog is an excellent source of cases concerning the Service Convention and reflects the wide range of approaches taken by courts, primarily in the US, but

exacerbated some of the problems with a virtual world without borders, but the underlying assumptions about the Convention's purpose of assuring actual notice that is simple and expeditious are in tension with underlying notions of sovereignty and territoriality.

US judges and lawyers frequently assume that, if the form of service is not explicitly prohibited under declarations under Articles 8 and 10,[183] service is permitted under new technologies, such as email and even Facebook,[184] failing to consider that the use of the new technology did not exist when the last objections were made. Other misconceptions surround the construction of Federal Rule 4(f) and its cascading options under (f)(2) and (f)(3) of additional forms.[185] Another way to avoid having to make service under the Convention is the broad reading of "address unknown" with the result that service is outside the scope of the Convention, recent examples of which have included Chinese e-commerce sellers.[186]

A large number of US state and federal cases avoid the use of the Convention through a broad construction of domestic (state) law to define when service is complete (and therefore not "transmitting abroad" and not triggering the Convention).[187] This determination is almost always based on US state law, which is often interpreted as not requiring the actual "formal service" to be made abroad but sufficient when on a local agent, as seen in the *Schlunk*[188] case itself. A broad extension of this construction is seen in many cases of "substituted service" as in *Melia Chairs*[189] a well-known case where the Rhode Island federal court found that service on the Secretary of State, as required when a foreign unregistered company is doing business in the state, did not trigger the Convention, even though the Secretary of State had to mail a copy of the summons and complaint to France, not just under state law but for basic due process concepts— reminiscent of the *notification au parquet*. US federal proposed legislation, the Foreign Manufacturers' Legal Accountability Act of 2009 and 2011, also tried to avoid Hague service by requiring certain foreign manufacturers who imported products into the US to have a designated agent for service in the US.[190] Like contractual waiver, there would appear to be limitations to these approaches other than just domestic requirements of due process and the practical limitation of not having the resulting domestic judgment recognized outside the US. Of course, for so many years, US litigants and creditors have assumed that foreign assets can be found in the US, frequently true but in the age of virtual currency, becoming less so.

reinforces the inconsistency in application. See generally Ted Folkman, "Letters Blogatory: The Blog of International Judicial Assistance", available at: < lettersblogatory.com >.

183 Countries must also communicate this opposition under Art. 21. Service Convention, *supra* note 155, at Art. 21.

184 See *supra* note 177.

185 See M. Gardner (*op. cit.* note 182), at 999-1002.

186 See, *e.g., Keck v. Alibaba.com, Inc.*, No. 17-cv-04572-BLF, 2018 U.S. Dist. LEXIS 128396 (N.D. Cal. July 31, 2018) (allowing electronic service by email and Aliexpress.com's messaging system on Chinese defendants with unknown physical addresses).

187 See *infra* notes 188-189.

188 *Schlunk*, *supra* note 176. For a discussion of the role of sovereignty and fiction in the context of service, see D. Rendleman, "Comment on Judge Joseph F. Weis., Jr. Service by Mail—Is the Stamp of Approval from the Hague Convention Always Enough?," *Law and Contemporary Problems*, vol. 57, 1994, p 179.

189 *Melia*, *supra* note 173. See also L. E. Teitz, *Transnational Litigation* (Michie 1996); Weis (*op. cit.* note 182), at 174-75.

190 Foreign Manufacturer's Legal Accountability Act of 2011, H.R. 3646, 112th Cong. (2011), available at: < https://www.govtrack.us/congress/bills/112/hr3646 > (last consulted on 20 April 2020); Foreign Manufacturer's Legal Accountability Act of 2009, S. 1606, 111th Congress (2009), available at: < https://www.govtrack.us/congress/bills/111/s1606 > (last consulted on 20 April 2020).

A similar approach can be seen in the use of a contractual "waiver" of service (and submission to jurisdiction) or parties agreeing that service shall be made at a local address. The validity of the contractual waiver approach as a way to avoid service under the Convention was just upheld by the California Supreme Court in its decision in *Rockefeller Technology Investments (Asia) VII v. Changzhou Sinotype Technology Co.* where a contractual agreement to receive notice by FedEx by a Chinese corporation was viewed as sufficient under California law to exclude the application of the Convention.[191] The problem with this waiver is that it creates tension between ensuring efficient and actual notice and the role of sovereignty. The notion of sovereignty that went without debate in 1965 also appears in some portions of the Convention, such as Articles 8, 10, and 13 as to the requested State.[192] At the time, sovereignty was taken for granted and the focus was on allowing speedy and efficient actual notice, avoiding the slow diplomatic channels, or worse yet, lack of meaningful notice at a meaningful time to a defendant. But respect for sovereignty seems to have been lost by parties working around the Service Convention with an exclusion or a waiver. As Ted Folkman has argued, sovereignty is not the parties' right to waive.[193]

If one takes the concept of contractual waiver further, are there no limits on whether waivers can be used to say that you are not transmitting documents abroad and therefore not under the Service Convention? The ability to mandate waivers becomes much more problematic if one extends the holding of *Rockefeller Technology* from sophisticated businesses to non-negotiated agreements and ones with weaker parties, such as consumers. Would the US Supreme Court uphold the waiver as a matter of Convention law, as opposed to one of basic due process notice? Arguably, Justice Brennan's concurrence in *Schlunk* at least would suggest that the Convention does set some limits on what domestic law can do.[194] Does the sovereign in the requested state have a right to limit who can waive notice and on whose territory? Of course, the requested state can always refuse the judgment, as is often the case when a US creditor goes to export a US judgment where the initial service in the underlying case was not made according to the Service Convention. And then we are back to the problem of domestic law construction eviscerating the application of the Convention and interfering with global harmonization.

---

191 No. S249923, 2020 Cal. LEXIS 2091 (Apr. 2, 2020). For a thorough analysis of the decision, see T. Folkman (*op. cit.* note 159). For a discussion of *Rockefeller* after the intermediate court decision and the use of contractual local agents to avoid Hague Service requirements, see J. F. Coyle, R. J. Effron and M. Gardner, "Contracting around the Hague Service Convention", *Davis Law Review* Online, vol. 53, 2019, p 53.

192 It also appears in connection with the limits placed on the requesting state in connection with default judgments under Arts 15 and 16.

193 See, *e.g.,* T. Folkman (*op. cit.* note 159). "[A] *defendant* can waive objections to service by post all day long, but the objection isn't there for the benefit of the *defendant*, it's there for the benefit of the state. It is not for the defendant to waive." *Id.* (emphasis supplied).

194 I am indebted to Hans van Loon, former Secretary General, for his thoughts about waiver and weaker or protected parties and for calling my attention to Brennan's concurrence. In his concurrence, Brennan states that:

> the assumption that the Court imputes to the Rapport [the explanatory report of the Service Convention] is inaccurate; as noted above, *notification au parquet* was typically deemed complete upon delivery to the local official. See *supra*, at 709, and n. 1. Any requirement of transmission abroad was no more essential to formal service than is the informal arrangement by which a domestic subsidiary might transmit documents served on it as an agent for its foreign parent. See, *e. g.*, 3 Actes et Documents 169. Thus, if the Court entertains the possibility that the Convention bans *notification au parquet* under all circumstances, *ante*, at 704, it can only be because (notwithstanding the Court's stated analysis) the Convention, read in light of its negotiating history, sets some substantive limit on the forum state's latitude to deem such service "domestic."
>
> *Schlunk*, *supra* note 176, at 713 (Brennan, J concurring).

V. Conclusion

From a US perspective, one can predict that the Hague Service Convention may see more limited use in outgoing cases, at least in commercial cases, given the narrower adjudicative jurisdictional bases post *Goodyear*[195] and *Daimler*[196] (e.g., no more "general doing business" jurisdiction) and narrower construction of specific jurisdiction after *Nicastro*.[197] There will be fewer cases where courts have adjudicative jurisdiction in the US over foreign defendants, and those foreign defendants will often have agents or subsidiaries which would be able to accept service within the US, removing the case from the Convention as there is no transmission abroad. On the other hand, the Service Convention will have increased importance when the US ratifies the Choice of Court Convention and when the Judgments Convention becomes effective, both of which provide the possibility of discretionary non-recognition on the basis of service "incompatible with fundamental principles of the requested State concerning service of documents."[198]

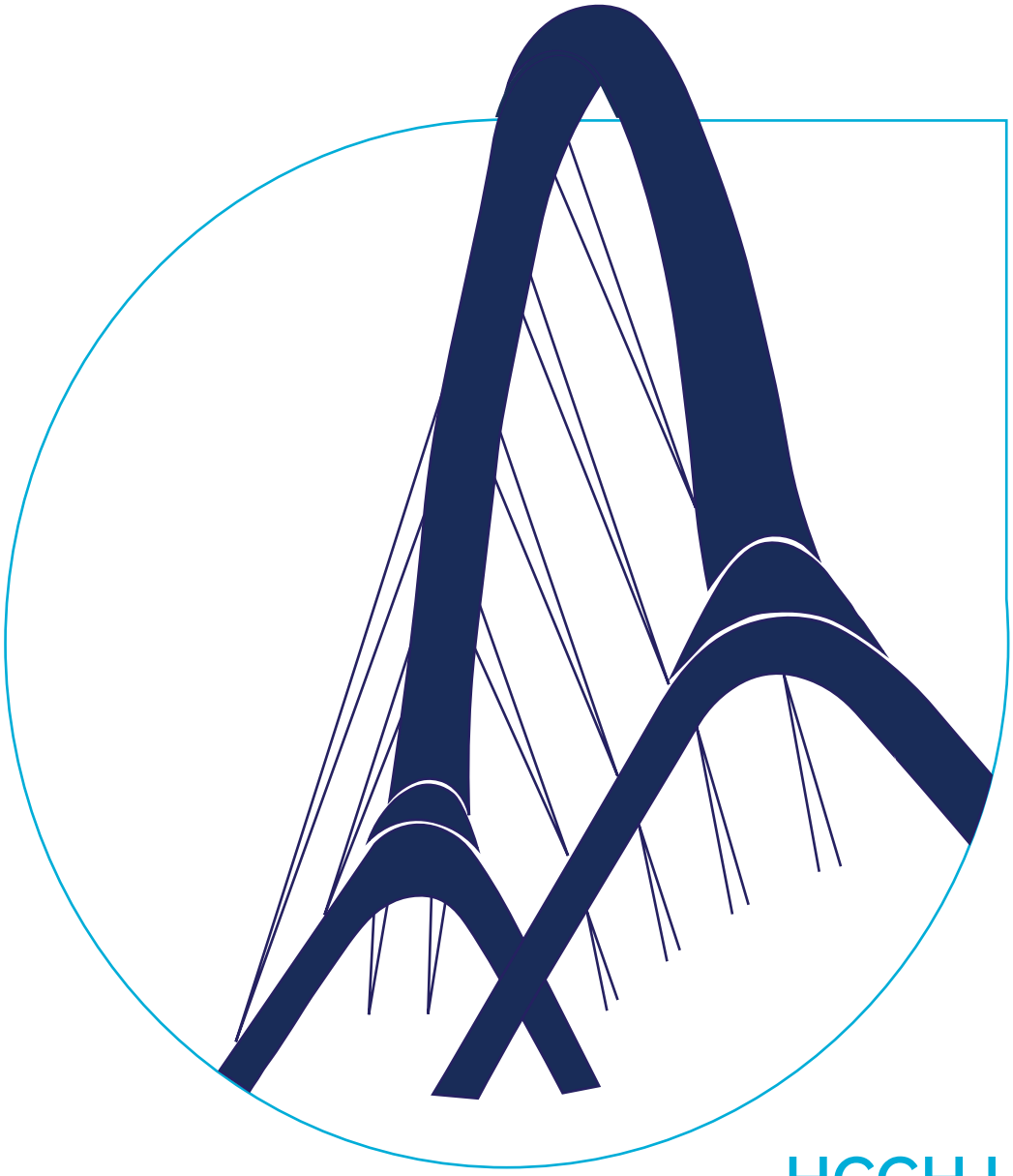
The Hague Service Convention was made for a world of paper and borders — and if sovereignty is still an important underlying value of the Service Convention, new interpretations may not meet that need. There may be a need for a soft hard-law or a legislative interpretation that allows and encourages new technologies when shown to be safe, secure, and effective in a world that lacks sovereign boundaries and is indeed limitless.

195 *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915 (2011).

196 *Daimler AG v. Bauman*, 571 U.S. 117 S. Ct. 746 (2014).

197 *J. McIntyre Mach., Ltd. v. Nicastro*, 564 U.S. 873 (2011).

198 HCCH 2005 Choice of Court Convention, *supra* note 157, at Art. 9(c)(ii); Judgments Convention, *supra* note 157, at Art. 7(1)(a)(ii).



HCCH Unplugged

This section collates the summary opinions of our speakers on specific topics arising from the use of information technology in the operation of the HCCH Service Convention.

KNOWING ME, KNOWING EU:
SECURITY AND DATA PROTECTION

BY MARIE VAUTRAVERS

Two years ago, the European Commission submitted a legislative proposal[199] for the revision of the Regulation 1393/2007 *on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters* (the "2007 Service Regulation"). This Regulation is applicable to cross-border service of documents and supersedes the *Hague Convention on the service abroad of judicial and extrajudicial documents in civil and commercial matters* (the "Service Convention") within the European Union (EU). In view of facilitating and accelerating the cooperation in relation to the cross-border service of documents, the Commission intended to take a major step towards the broader use of electronic means and pursued two key objectives directly linked to the digitalisation of procedures:

- **Mandatory use of electronic means for the transmission of requests** and other communications between competent authorities;
- Introducing **electronic cross-border service** of documents.

The new EU Regulation has not yet been adopted: the European actors responsible for the adoption of new instruments (the Commission, the Council of the EU and the European Parliament) are currently wrapping up the negotiations. However, the work conducted within the EU might already bring new prospects and help identify the challenges of electronic communication for the operation of the Service Convention. Because the 2007 Service Regulation is in many ways almost identical to the Service Convention (only better!), many of the questions regarding digitalisation addressed in the European context are also relevant in the context of the Service Convention, subject to the necessary adaptations.

I. Mandatory electronic transmission of requests

The 2007 Service Regulation provides that the document to be served is transmitted directly by the competent authority of the requesting State to the competent authority of the requested State, excluding the intervention of a central body or of any intermediate authority.

As indicated above, the proposal for the revision of the 2007 Service Regulation aimed, inter alia, at eventually obliging Member States to use electronic means for all transmissions between competent authorities. EU Member States consider overall the use of electronic transmission as an overriding objective and do not dispute its benefits. However, the technical and legal means required to attain this objective, and in particular the level of security and data protection that is needed and/or expected in the use of cross-border electronic communication, were the subject of much discussion and debate. The result of these discussions has been that striking a balance between the need for a flexible and cost-effective solution on the one hand, and the obligation of security and data protection on the other hand, cannot easily be done.

[199] Available at: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0379 >.

It is in light of these conflicting requirements for flexibility and security that the European experts have reviewed the three main technical options available as regards the architecture of electronic communications.

a) A common IT platform

A common IT platform, meaning a unique IT system to which all participating authorities would connect, is generally considered as a highly secure solution, which does not entail actual transmission of data between different national systems. The authority of State A uploads a document on the common platform and grants access to the competent authority of State B, which in turn connects to the platform to download the document. Only competent authorities would have access to the platform and their access would be restricted to the documents they are requested to serve. For instance, in the case of the EU, all the data is stored on the Commission's server (in Luxembourg). As a result, a common platform comes with strong guarantees in terms of data protection.

Such a platform has also proven to be cost-effective for a community of users coming from different countries. It entails only the development and the implementation of a single IT system, irrespective of the number of participating States and results in a single investment. In an EU context, the European Commission would have had the financial responsibility for its development and maintenance.

However, the use of an IT platform might not be as secure as it appears at first glance: one single point of access also means one single point of potential failure. Once hacked, it gives access to most, if not all, data.

Additionally, the use of a platform for cross-border communications is much more complicated when it comes to providing a legal framework, from a data protection perspective, as it entails several layers of responsibilities. In the European context for instance, the European Commission would likely have been responsible for the development and maintenance of the platform, and would therefore have had a joint responsibility in the control of the data stored on the platform. Since the European Commission is not involved in any step of the actual transmission of judicial documents, it did not wish to take on new heavy responsibilities for the protection of data, and naturally wished to leave this to the States or competent authorities. Similarly, the Permanent Bureau would likely not be willing to bear any responsibility regarding data protection in the operation of the Service Convention.

b) Secure emails

Some experts considered secure email as the closest technology to the current everyday practice of the competent authorities for service. Secure email is highly flexible and easily accessible for competent authorities - regardless of the development of their own national system. Regular email is already broadly used to exchange documents under the 2007 Service Regulation or the Service Convention.

In terms of security, however, other experts considered this technology to be unreliable, especially in a cross-border context: using secure email does not guarantee the successful delivery of a message.

Exchanging requests and information via secure email also places the responsibility for security on each and every individual involved in the email communication. Although the exact number of competent authorities for service in Europe is not known, it is safe to assume that there are thousands of them. As an example, France counts around 4000 competent authorities: 1000 courts and 3000 *huissiers de justice* (bailiffs).

In the context of secure email, common security safeguards and access rights must also be correctly implemented at the local level, *i.e.* on every computer sending or receiving secure emails. This is a lot to control and coordinate. Such a decentralised architecture therefore increases the risk of diluting responsibilities and of inappropriate use.

c) Decentralised IT system

In the end, subject to the final version of the text (which, at the time of publication remains under discussion), Member States have favoured the implementation of a decentralised IT system. The decentralised IT system consists of a secure communication infrastructure connecting existing national IT systems and making them interoperable. This solution allows participating States to keep using their own national IT system, and whatever security and technical standards they have opted for.

In terms of security, the risk of the whole system being hacked is very low, as security failures in one State do not affect the entire network. Between national systems, the common communication infrastructure ensures the integrity of the document, the accurate identification of the sender and recipient, as well as the exact time and date of delivery.

At present, the EU envisages using the e-CODEX technology to connect all national systems: this technology has been developed to cater for reliability, security and interoperability while respecting the efforts and investments made in national IT systems. For those Member States that do not have an existing IT system, or that do not want to invest in the adaptation of their IT system, one single common IT system will be developed by the Commission to send and process requests for service of documents.

In terms of data protection, each State would retain entire responsibility of the data processed. Additionally, a specific data protection provision included in the Regulation would ensure that personal data will *"be processed lawfully, fairly and in a transparent manner"*, according to Article 5.1 of the well-known General Data Protection Regulation (GDPR)[200], and would provide the necessary legal basis for the processing of data. Additional implementing legislation will properly define the responsibilities of the different actors.

The use of a decentralised IT system will ensure the implementation and use of secure means of transmission, while each State will continue providing for the security of their own system and the adequate protection of personal data. It does not require any delegation of responsibilities from States to the European Commission and allows for a secure framework. In the context of the Service Convention, the use of any similar decentralised IT system might likewise offer major benefits for Contracting States and relieve the Permanent Bureau of the Hague Conference of any responsibility in the actual operation of the Convention. It would, however, likely require the prior development of common software for those Contracting States that do not have their own national system or do not have the capacity to connect it to the common infrastructure.

The overall discussion on the means of communication between competent authorities relates primarily to practical, technical and cost issues. Defining security standards for the electronic service of documents itself (as opposed to electronic transmission), raises additional questions in relation to procedural law and procedural public policy, which are known to be much more sensitive issues.

---

[200] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

II. Allowing a new method of service: electronic cross-border service

The Service Convention does not provide for any specific method of service. The actual service of a document is always executed under the law of the Requested State/State of destination, with the exception of Articles 8, 10(a) and 5(1)(b), which allow for the application, under specific conditions, of the law of the Requesting State. Contrary to the Service Convention, the 2007 Service Regulation has introduced one alternative common method of service: service by postal mail with an acknowledgement of receipt. In line with this first innovation, when revising the Service Regulation 11 years later, the introduction of cross-border electronic service appeared as an available and attractive option. However, because a great number of EU Member States had not yet introduced electronic service of documents in their own legal system, or were only in the process of doing it, it was found more appropriate to *allow* for such a method of service, if provided for in the law of an EU Member State, rather than to *introduce* it as a standalone alternative method for service.

Direct electronic service (by email for instance) is probably the quickest and simplest method of service, since it does not entail any intermediate action between the sender and the recipient.

However, in the context of electronic service and particularly of email, the exact conditions of service are not established with certainty, thanks to the intervention of a third party (the receiving competent authority or the postal service). In case the defendant fails to enter into appearance, courts may request some or all of the following evidence, in relation to the service of the document instituting proceedings, but also other procedural documents or additional claims, which have proved difficult to obtain in the context of service by email:

- The accurate identification of the parties to the electronic communication;
- The exact date of sending and delivery of the document;
- The proof of the integrity of the attachment.

We all know that emails are unreliable and may be deceiving. We can delete an email and pretend we did not receive it. We can change the content of that email, including the date, the recipient and the attachments. We can access the inbox of someone else (ex-spouse, business partner, colleague…), then respond to and/or delete an email. There is no way of tracking this and no secure record of the messages received for the court or the parties. Sensitive data relating to third parties is stored in regular mailbox, which can be easily hacked.

To overcome those shortcomings and build appropriate security and data protection safeguards, European Member States have agreed on establishing certain conditions and limitations to the electronic service.

First, the recipient will need to consent to the service by email in advance. This is particularly relevant in the context of the GDPR, as it is a non-negotiable condition to the lawful processing of data.

Second, documents instituting proceedings should be excluded from the scope of electronic service, as this document is the cornerstone of judicial proceedings. If it is not served correctly, or not served at all, and if the identity of the parties or the date of service is not sufficiently proven, it may lead to the annulment of proceedings, or the refusal of recognition and enforcement of the decision.

Finally, the definition of the minimum level of security that is expected from the electronic service of a document has given rise to lengthy discussions that are still ongoing. Some Member States have a very demanding set of security requirements as regards

electronic service of documents, while others already permit the service of some documents by email. To ascertain whether the delivery of the document was effected and the date on which this occurred (one of the primary flaws of service by email), an acknowledgement of receipt signed by the addressee was introduced as an additional condition. As for the use of email to serve documents, one possible way forward would be to allow some Member States to object to service by email in whole or in part, or to allow them to specify conditions.

The question then becomes how an objection to, or limitation upon, service by email can be effectively crafted in a specific territory. When the service is dematerialised, and there is no geographical connecting factor, the court will have no idea of the physical location of the recipient at the time of receiving the email. This will necessitate a thorough common understanding of all aspects and concepts involved, but this is another story!

Disclaimer: the information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

THE IMPORTANCE OF SERVICE OF PROCESS

BY AASHNA BHIKHARI

Although service of process might seemingly be a "highly technical and not very thrilling legal field,"[201] the importance of a well organised system of service of documents cannot be understated. In civil proceedings, the principle of *equality of arms* implies that each party must be afforded a reasonable opportunity to present his or her case - including evidence – under conditions that do not place him or her at a substantial disadvantage *vis-à-vis* his or her opponent.[202] Equality of arms is one of the aspects underlying the concept of *fair trial*. Such equality implies the right for the parties to have knowledge of and to comment on all evidence adduced or observations filed.

The European Court of Human Rights (ECtHR) has highlighted the importance of said principle in the case *Grozdanoski v. FYROM.*[203] In that case, the Northern Macedonian Government asserted that certain proceedings were fair as the parties were given an equal opportunity to present their case. The ECtHR had a different opinion. According to the applicant, the Government had failed to provide any evidence that a copy of the appeal on points of law had been communicated (served) to him. The lack of a proof of receipt in the casefile supported his arguments:

> *"*In the absence of any evidence of service, the Court is unable to accept the Government's argument that the appeal and the request were ever served on the applicant. [...] The Court considers that procedural failure prevented the applicant from effectively participating in the proceedings before the Supreme Court. Article 6 § 1 of the Convention is intended, above all, to secure the interests of the parties and those of the proper administration of justice [...]. In the present case, respect for the right to a fair trial, guaranteed by Article 6 § 1 of the Convention, required that the applicant be given an opportunity to have knowledge of, and to comment upon the [...] appeal and the public prosecutor's request. Consequently, there has been a violation of Article 6 § 1 of the Convention.*"*[204]

As illustrated above, service of documents plays a vital role in preserving the principle of procedural equality. The above example is not exceptional. In many countries, backlogs in courts and in enforcement proceedings are caused by the incorrect service of documents or the failure to do so at all. For this reason, in a substantial number of countries (e.g. France, Belgium or the Netherlands) legal professionals, known as judicial officers, are involved in the service of judicial and extra judicial documents. The judicial officer guarantees that the service of documents is done appropriately. Prior to servicing the documents, the judicial officer corroborates the domicile of the recipient, and only once the judicial officer is convinced that the domicile of the recipient is correct, the document is

---

201 Centre for European Constitutional Law, the International Union of Enforcement Agents, and the Aristotle University of Thessaloniki, "Comparative Report", *ENABLE – Enabling dematerialized access to information and assets for judicial enforcement of claims in the EU* (NUMBER 721331), available at < https://access2just.eu/wp-content/uploads/2019/02/COMPARATIVE-REPORT_final.pdf >

202 *Dombo Beheer B.V.* v. *the Netherlands*, ECtHR 27 October 1993, no. 14448/88, and *Stran Greek Refineries and Stratis Andreadis v. Greece*, ECtHR 9 December 1994, no. 13427/87.

203 *Grozdanoski* v. *the Former Yugoslav Republic of Macedonia*, ECtHR 31 May 2007, no. 21510/03.

204 *Ibid.*

served. The judicial officer may be liable (on both criminal and civil grounds) for any damages stemming from the service of documents if done incorrectly. In those legal systems where the judicial officer is involved, the service of documents is challenged only in exceptional cases.

These guarantees should not be lost in the process of digitising the service of judicial and extra-judicial documents!

I. E-service of judicial and extra judicial documents

The electronic transmission of documents is commonplace these days. Yet, when it comes to the e-service of documents, countries have different levels of progress. Between 2016 and 2018, the *International Union of Judicial Officers* (UIHJ) conducted an assessment on the status of e-justice in the enforcement system of 8 EU member states.[205] The study found that, among these member states, some countries fully accepted e-service of documents, and that they had legislation in place to that effect. However, there are certain legal conditions that need to be fulfilled prior to effecting e-service, namely, the document needs to carry an e-signature and service can only be done by judicial officers. Also, the recipient must have expressly accepted such method of service in advance.

In summary, the study shows that e-service of documents depends on the existence of an e-signature and the consent of the recipient for such kind of service. A document can be served electronically, provided that the following conditions are fulfilled:

- The circumstances of the case must allow for this;
- The recipient of the document to be served (a private individual or a legal entity), must hold an "electronic judicial address" or, failing so, an "elected electronic address for service." In the latter case, express prior consent – which can be obtained through dematerialised means – is required.

With regard to the service of documents, most procedural complications arise when the recipient cannot be located at the (registered) address or does not have a registered address at all. Such situation should be avoided when it comes to e-service of documents. A scenario in which all citizens have one mandatory "official e-address" for service purposes is still utopic.

To ensure legal certainty, the requirements mentioned above are a *conditio sine qua non*. The principle of *legal certainty* requires certain guarantees on the service of documents, and these guarantees should extend to the e-service of documents. Having a minimum acceptable level of security regarding the e-service of documents is crucial.

What does this mean in practice? It is important that there is an authentic source for all records of service, i.e. that all notifications are recorded in an official registry, along with all the necessary additional information. This could be done by establishing an e-service platform. This platform could function as a communication system, through which the requests for service could be forwarded to the territorially competent and available judicial officer. The platform could also register the moment in which the recipient has been electronically served. In case a receipt of service is not received within a certain period, service would still need to be effected in the "traditional" manner.

[205] Source with author.

Turning to cross border e-service of documents, it should be noted that States do not need to domestically develop infrastructure for e-service. As way of example we have the Service Regulation 1393/2007 regarding the cross-border service of documents within the EU, which is being currently evaluated. One of the objectives of the review is to allow, in the future, e-service of documents using the e-CODEX infrastructure.

II. Conclusion

Presently, e-service of documents is not common in most countries. Thus, it is not an option to serve all documents exclusively through electronic means. Both on a national and a cross border level, the following barriers preclude that service is effected exclusively through electronic means:

- **Technical barriers** resulting from incompatible technical standards at the national level, lack of inter-operational databases, lack of inventories and publicly accessible information allowing the identification and selection of judicial officers, limited use of digital signature nationally and in cross border communication, lack of validated databases, the need for security of electronic exchanges, data protection and other concerns.
- **Legal barriers** related to the highly diversified national frameworks in relation to the status, role, competences of judicial officers and the lack of alternative means to verify documents' authenticity.[206]
- **Informational barriers** resulting from insufficient information available on the competent judicial officers, debtor's domicile or location of property.
- **Linguistic constraints** in accessing information, communicating, monitoring and obtaining feedback on the enforcement proceedings.
- **Cost constraints** resulting from different tariffs, delays and the need to translate necessary documents to the official language of the receiving Member Party.
- **Barriers resulting from the limited trust** in dematerialized exchanges and enforcement from the part of authorities and citizens.[207]

[206] See for example: Study No. JAI/A3/2002/02 on making more efficient the enforcement of judicial decisions within the European Union: Transparency of a Debtor's Assets Attachment of Bank Accounts Provisional Enforcement and Protective Measures, 2004.

[207] UIHJ Position paper "Judicial officers in the middle of e-Justice", April 2010, available at: < https://uihj.com/archive-uihj/en/ressources/10149/01/position_paper_uihj-e-justice-en.pdf >.

YOU'VE (STILL) GOT MAIL: POSTAL CHANNELS IN THE 21ST CENTURY

BY BRODY WARREN

I. Introduction

As it approaches its 55th anniversary,[208] it is fair to say that the *HCCH Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (Service Convention) has truly stood the test of time. It is the most successful multilateral instrument on the subject, having enjoyed continuing interest from States across the globe since its adoption.[209]

Yet as digitisation of judicial processes garners widespread support and technological advances propel society forward, it is not unsurprising that the so-called "technology-neutral" drafting of the Convention would become the subject of further discussion.[210] What may be surprising is that a seemingly straightforward term hidden in a sub-paragraph of an Article in the middle of the Convention has become a likely candidate for ensuring that the Convention can keep pace with technology in the 21st century. Yet this is the case with the term "postal channels" enshrined in Article 10(a).

II. "Postal Channels": A History

In order to understand the use of the term and its origins, an examination of the term in its original context is required:

> *Provided the State of destination does not object, the present Convention shall not interfere with –*

---

208 While the Convention was adopted on 28 October 1964, the final Convention carries the date of the first signature(s), 15 November 1965. For more on the adoption of the Convention during the Tenth Session, see HCCH, *Actes et documents de la Dixième session (1964)*, Tome III, *Notification*, The Hague, Imprimerie Nationale, 1965.

209 Within five years of its entry into force, the Convention had 16 Contracting Parties across four continents. At the time of writing, the Convention counts 76 Contracting Parties, with its five most recent accessions being from States across four continents. For the full list of Contracting Parties to the Convention, see the "Updated List of Contracting Parties", [hereinafter "Status Table"] available on the Service Section of the HCCH website, < www.hcch.net > (last consulted on 27 April 2020).

210 In September 1999, the Permanent Bureau organised, in collaboration with the University of Geneva, a roundtable to consider the issues of private international law raised by electronic commerce and the Internet. Commission V of the Geneva Roundtable had as its specific assignment a review of the repercussions of new means of electronic commerce on the operation of the Service Convention. The Commission's findings were published by the Permanent Bureau in a Report by C. Kessedjian, "Electronic Data Interchange, Internet and Electronic Commerce", which was included in Prel. Doc. No 7 of April 2000 for attention of the Special Commission of May 2000 on General Affairs and Policy of the Hague Conference. The use of technology was also subsequently discussed during the 2003, 2009 and 2014 meetings of the Special Commission (SC) on the practical operation of the Service Convention and referenced in the Conclusions & Recommendations (C&R), which are available on the Service Section of the HCCH website. See C&R Nos 4, 59-64 of the 2003 SC; C&R No 55 of the 2009 SC; C&R No 20 of the 2014. See also, Permanent Bureau of the HCCH, *Practical Handbook on the Operation of the Evidence Convention*, 3rd ed., The Hague, 2016, (hereinafter "Service Handbook"), Annex 8, pp. 167-201.

> a) *the freedom to send judicial documents, by* **postal channels**, *directly to persons abroad […]*[211]

The term "postal channels" is not defined elsewhere in the Convention, nor does it even appear in any other Article. The Explanatory Report to the Convention is equally silent on the term and contains no reference to Article 10(a) specifically.[212] All that can be gleaned from the Explanatory Report is that the three alternative channels in Article 10 (*i.e.* paragraphs *a)*, *b)* and *c)*) were considered to be *direct* channels of transmission.[213]

Fortunately, the text of Article 10(a) is identical to that which was presented to the Tenth Session in the draft Convention, together with which the Special Commission had provided its own report.[214] This report provides some additional guidance, namely that:

- the reference to "persons" encompasses both legal and natural persons (and their legal representatives if applicable);
- the drafters had expressly rejected the notion that postal channels should be restricted only to registered mail; and
- that the term "postal channels" encompasses service by telegram;
- in the absence of an objection from the State where service is to be effected, service by postal channels need only be valid under the law of the forum.[215]

Although this may prove useful in the subsequent analysis of the application of postal channels to new technologies, conspicuously absent from the report is a definition. This is of particular interest because the French equivalent, "*la voie de la poste*", appears not only in the 1965 Convention,[216] but also in the corresponding provisions of its predecessor Conventions on Civil Procedure: the HCCH Conventions of 1954, 1905 and 1896.[217] This demonstrates that the term was used for over 60 years without a comprehensive definition being articulated, which may suggest that it was so well understood among the delegations present at the Tenth Session that a definition seemed superfluous.

This was likely because, between the late nineteenth and mid-twentieth centuries, the notion of *la voie de la poste* had remained largely unchanged – a State-owned or State-associated service that would ensure the transfer of mail from A to B – the original postal channel.

---

211 Art. 10 (emphasis added). The full text of the Convention is available on the Service Section of the HCCH website.

212 V. Taborda Ferreira, "Rapport explicatif", [in French only], in *Actes et documents de la Dixième session (1964)*, Tome III, *Notification*, The Hague, Imprimerie Nationale, 1965, pp. 363 *et seq.* (hereinafter "Explanatory Report").

213 *Ibid.*, pp. 373-4.

214 V. Taborda Ferreira, "Rapport de la Commission spéciale" [in French only], in *Actes et documents de la Dixième session (1964)*, Tome III, *Notification*, The Hague, Imprimerie Nationale, 1965, p. 74 *et seq.* (hereinafter "Report of the 1964 SC").

215 *Ibid.*, p. 90.

216 See Art. 10(a) of the French version of the Convention, available from the Service Section of the HCCH website.

217 Art. 6(1) of the *HCCH Convention of 1 March 1954 on Civil Procedure*; Art. 6(1) of the *HCCH Convention of 7 July 1905 on Civil Procedure*; and Art. 4(1) of the *HCCH Convention of 14 November 1896 on Civil Procedure.*

Even in instances where postal services have been privatised, in whole or in part, their historical links to the State and the equivalence of the service provided would seemingly leave little doubt as to their inclusion within the scope of postal channels.[218]

With the continued growth and diversification within the postal sector over the years, there has been a proliferation of private courier services offering postal services – often an expedited service at a premium.[219] The use of such services has been deemed to be the equivalent of a postal channel for the purposes of Article 10(a) by the Special Commission on the practical operation of the HCCH Service Convention.[220]

However, if entrusting the transmission of a document to a private company in the paper world is considered to fall within the scope of the term postal channels, why should entrusting the transmission of a document to a private company in the online world be any different?[221] This is a question the drafters of the Convention could not possibly have contemplated and one which illustrates that the application of postal channels in the 21st century may be more fraught with complexity than first thought.

III. Universal Agreement?

At this juncture, it is relevant to note the work of the Universal Postal Union (UPU), an international organisation established well before the first HCCH Convention.[222] The UPU Congress regularly adopts iterations of the Universal Postal Convention providing comprehensive guidance on postal services worldwide, the most recent of which was adopted by the Istanbul Congress on 6 October 2016 and entered into force on 1 January 2018.[223]

In particular, Article 37 of the Universal Postal Convention provides for four main electronic postal services: electronic postal mail, electronic registered mail, the electronic postal certification mark and the electronic postal mailbox.[224] First, electronic postal mail is "an electronic postal service involving the transmission of messages and information by designated operators."[225] Second, electronic registered mail is the "secure electronic postal service with proof of sending and proof of receipt, and a secure communication channel to authenticated users."[226] The third, the certification mark is less relevant to the broader

---

218 Consider, for example, the designated postal service providers in Japan, Netherlands, and the United Kingdom. For more information on these and other designated postal service providers, see Universal Postal Union, "Status of postal entities", available at: < http://www.upu.int/en/the-upu/status-of-postal-entities/about-status-of-postal-entities.html > (last consulted on 27 April 2020).

219 Such as the international courier companies: FedEx Corporation; Dalsey, Hillblom and Lynn (DHL) International GmbH; and United Parcel Service (UPS), Inc.

220 C&R No 56 of the 2003 SC, *op cit.* note 210. See also, Service Handbook, *op cit.* note 210, paras 253 *et seq*.

221 For example, if the transmission were entrusted to companies such as: Google LLC, Facebook, Inc., Apple Inc., Amazon.com, Inc., and the Microsoft Corporation.

222 The Universal Postal Union was established in 1874 and, at the time of writing, has 192 Members. See Universal Postal Union, "About UPU", available at: < http://www.upu.int/en/the-upu/the-upu.html > (last consulted on 31 July 2020).

223 Universal Postal Convention, in International Bureau of the Universal Postal Union, *Convention Manual*, Berne, Universal Postal Union, 2018, Art. 40.

224 *Ibid*., Art. 37.

225 *Ibid*., Art. 37(1.1) and corresponding Regulations *37-001 Hybrid mail*, *37-002 Facsimile-based services*, *37-003 Text-based services*.

226 *Ibid*., Art. 37(1.2) and corresponding Regulation *37-005 Postal registered electronic mail*.

discussion of postal channels, but is essentially a digital authentication of an electronic event, such as postal transmission.[227] Finally, the electronic postal mailbox allows for the sending, delivery and storage of electronic messages and information while ensuring that both the mailers and addressees are appropriately authenticated.[228]

Each of these electronic postal services serves a different purpose, yet three common themes emerge: first, that the recipient or addressee has effective notice (and that this is verifiable); second, that the transmission is secure; and third, that the transmission is completed expeditiously. These are all assurances which the Service Convention too, seeks to provide; assurances which, given the growing number of electronic alternatives available, can be facilitated (or even better achieved) with the aid of technology. Against this background, why is it that we are so reluctant to move away from the idea that paper can be the only form of original?

IV. Analogy vs Application

In order to assess the extent to which information technology can be used in facilitating the operation of the Convention more broadly, a "functional equivalence" approach is advocated.[229] This involves an examination of the aims of the relevant channel of transmission and an assessment of whether the requirements can be satisfied when electronic means are employed.

Looking to the requirements imposed by Article 10, of note is the fact that the State of destination must not have objected to the use of the channel in question on its territory. In this respect, while there are a majority of States which accept service by postal channels, there are still a large number which do not, as well as some who will accept it provided certain conditions are met, for example translation requirements and/or the use of registered mail.[230]

In the absence of an objection from the State of destination, the second relevant consideration is that by "not interfering with the freedom" Article 10(a) does not affirmatively authorise the use of postal channels, but instead requires only that it be permitted under the law of the forum.[231]

An important clarification in this context is that what must be permitted by the law of the forum is actual service by mail, which is to be distinguished from, for example, transmission under the main channel of the Convention, where the request for service is transmitted to the Central Authority for subsequent execution.[232] The negotiation history confirms that Article 10(a) was conceived as a direct channel under the Convention,[233]

---

227 *Ibid.*, Art. 37(1.3) and corresponding Regulation *37-004 Electronic postal certification mark*.

228 *Ibid.*, Art. 37(1.4) and corresponding Regulation *37-006 Postal electronic mailbox*.

229 Service Handbook, *op cit.* note 210, Annex 8, para 8. See also, para. 35, for a discussion of functional equivalence in the context of postal channels.

230 At the time of writing, 40 Contracting Parties to the Convention have not objected to the use of postal channels under Art. 10(a), 31 Contracting Parties have objected, and a further 5 Contracting Parties have qualified objections, *i.e.* will allow it under certain circumstances. To view the declarations or reservations made by a particular Contracting Party, see the Status Table, *op cit.* note 209, in column entitled "Res/D/N/DC".

231 Report of the 1964 SC, *op cit.* note 214, p. 90.

232 See, *e.g.* Arts 3 and 5 of the Convention.

233 In both the Explanatory Report (*op cit.* note 213) and the Report of the 1964 SC (*op cit.* note 214), Art. 10(a) appears under a heading "*Autres voies directes*", which translates to "Other direct channels".

meaning that transmission using postal channels is only completed once service itself is effected. Therefore, no distinction is to be drawn between sending and serving in the context of postal channels, an approach which has been confirmed by both the Special Commission[234] and State practice.[235]

In addition to these aspects unique to Article 10(a), when adopting an approach of functional equivalence to assess any potential use of information technology, the four fundamental conditions enshrined in Article 1 of the Convention must also be fulfilled. First, whether the relevant case is a *civil or commercial matter* and whether the documents to be served are *judicial or extra-judicial* in nature.[236] These are questions which can be resolved in the same manner irrespective of whether information technology is implicated. However, the same cannot be said for determining whether there is a *transmission abroad*[237] and whether the *address* of the person to be served is known.[238]

The latter two conditions give rise to a number of practical questions. For example, where the law of the forum determines that "there *is* occasion to transmit […] abroad",[239] how far into the technology should courts go to determine that the document was transmitted "abroad", that it reached the State of destination, or that did not pass through other States? Similarly, in the digital world, what kind of "address" would be sufficient for the purposes of the Convention? And if, under either the law of the forum or the law of State of destination, an electronic address is sufficient for the purposes of accurately locating and identifying the addressee, should this not be enough to satisfy the known address condition in Article 1(2)?

While these and other related questions may be unresolved, it is nonetheless advisable to adopt pragmatic approach when assessing the relevant conditions in a technological context.

V. Conclusion

In the context of the Service Convention, adherence to the textual requirements remains paramount, yet an open and modern reading would certainly facilitate the way that technology can be leveraged to improve its day-to-day operation, especially in relation to traditional notions of location and transmission.

As the old adage goes, necessity is the mother of all invention, a notion which has only been reinforced during the global COVID-19 crisis. The pandemic may have forced the transition to digitised judicial processes sooner than expected in some jurisdictions, but it may just be the push that was necessary to collectively rethink our approach to information technology and the law.

Ultimately, while we may have to get a little creative with the Convention text for the sake of technology, if the last century is anything to go by, postal channels – in all their forms – are here to stay.

---

234 C&R No 55 of the 2003 SC, *op cit.* note 210.

235 See, *e.g.* resolving the question in the United States, the decision of the United States Supreme Court in *Water Splash, Inc. v. Menon* 137 S. Ct. 1504 (U.S. 2017). For more information on the history of jurisprudence in the United States, see, Service Handbook, *op cit.* note 210, paras 270 *et seq.*

236 Art. 1(1) of the Convention.

237 *Ibid.*

238 Art. 1(2) of the Convention.

239 Art. 1(1) of the Convention (emphasis added).

TRENDING ON SOCIAL MEDIA?
YOU'VE BEEN SERVED!

BY CHRISTINE KALIBBALA

Ole, Ole, Ole Ole!!! A popular chant associated with sporting events and notably found on various social networking sites throughout the world during the football world cup in 2018. Football is no doubt one of the most popular, if not the most popular sport in the world, with people from different cultures, backgrounds and regions being able to communicate or cheer their respective teams with common chants. It has been said that sport has the ability to unite people and social media has further aided in uniting people by allowing people across the globe to simultaneously witness or experience live events in their own countries notwithstanding diverse time zones. Billions of people around the globe are users of various social networking sites, for example *Facebook, Instagram, Twitter, LinkedIn* and *WeChat,* to name a few. These social networking sites are available in numerous languages with millions of users. By way of example, *Facebook* is available in over 100 languages in numerous countries, India has 269 million users, the United States has 180 million users and Brazil has120 million users; *Twitter* is available in over 30 languages in numerous countries, the United States has 59 million users, Japan has 45 million users and the United Kingdom has 16.7 million users. *WeChat* is available in over 20 languages, China has the most users, approximately 900 million users, with other countries such as Vietnam, Japan and Australia having 100 million users combined. On review of the figures, one is confronted with the magnitude and prevalence of social media in the lives of people around the world. Bearing in mind that there are also numerous other social networking sites (that cater for diverse interests) with a fair number of users across all continents further bolsters the assertion of such magnitude and prevalence.

Society's technological advances, therefore, cannot be denied. Such advancements have led to the evolution of numerous sectors due to many reasons but one being the fact that technology facilitates cross border interactions. For the purposes of this piece, I shall focus on advancements in the legal sector, particularly service of process. The trend toward electronic service is a logical step forward in the evolution of civil procedure. It could be argued that the step forward in the evolution by necessary implication requires an analysis of social media as a prime method of service. In particular, where litigious matters of a cross border nature are concerned, it would be of value to explore the feasibility of service of process via social media. Exploring the feasibility will require a holistic outlook analysing the practicalities, challenges and advantages of effecting service in this manner. What better way to explore the feasibility than the Service Convention,[240] due to its global reach in that there are 76 contracting parties comprising of countries that have some of the highest numbers of users of social networking sites in the world. The contracting parties comprise of both common and civil law legal systems indicating diversity and hence a comprehensive outlook. Furthermore, the preamble of the Service Convention states that the aim of the Service Convention is to improve organisation of mutual judicial assistance for the purpose of service of process by simplifying and expediting the procedure. I argue that social media does, or alternatively has the ability to, simplify and expedite the procedure, notwithstanding the absence of explicit provisions in the Service Convention authorising service by such means. The absence of such explicit provisions is unsurprising as the environment within which we find ourselves today differs significantly to the one when the Service Convention was drafted.

---

[240] *Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters*, 1965.

It would be prudent to focus specifically on the alternative channels of service, in particular, Article 10 (a) as arguably this is the article one could rely on to justify service of process via social media. By way of example, we could consider a plaintiff in the United Kingdom who wishes to institute proceedings against a defendant in Tunisia, within a matter of seconds, information can be transmitted and received via social networking sites which is the epitome of simplicity and expedition. Some of the most popular social networking sites, particularly those mentioned above, have features which provide for the attachment of documents, provide pertinent information, for example, the date and time when documents are sent, the time when they are delivered as well as the time when they are accessed or read. If it can be argued that under the functional equivalence approach[241] service by email could fall within the ambit of Article 10(a), then why not social media, as social networking sites have similar features and in fact in certain cases are more advanced than email.

Having canvassed the practicalities, one has to consider some challenges and advantages. One obvious challenge is that numerous States have objected to alternative channels of service and specifically Article 10(a). This is an indication that States are reluctant to explore unconventional methods of service. Furthermore, security measures and privacy settings are also challenges that one must consider. In the case of the former, proof that the account holder is that of the defendant is key, it would have to be determined with a reasonable degree of certainty that a considerable amount of information contained in the profile such as occupation or location, matches information known about the defendant sought to be served. In the case of the latter, as technology evolves, many people feel the need to regularly alter their settings with the view of limiting who can access their profiles and to what degree. Therefore, if a defendant has privacy settings which prevent the plaintiff from obtaining key details to prove that the defendant regularly visits the site, this could be problematic because, in order to establish timeliness of notice via social media, there must be evidence of the defendant's use of the site, such as status updates, connecting with other users or similar activity. That being said, no method of service be it conventional or unconventional is without flaws. In my view, the advantages, however, outweigh the challenges, and I base this on the premise that there is, in my opinion, strong evidence to suggest that service via social media complies with due process considerations (specifically notice and an opportunity to be heard). As litigious matters in their very nature have victors and losers with serious ramifications, due process is indispensable and hence an integral part of civil procedure notwithstanding the legal system (be it common law or civil law).[242] With reference to the case in point regarding the defendant in Tunisia, service by social media arguably meets the due process considerations as it is possible for the defendant to be given adequate notice of the proceedings, to decipher the information at ease and is afforded an opportunity to respond appropriately to the allegations. Therefore, provided the defendant maintains a social media page on the specific website, the profile on the social media page is that of the defendant and the defendant regularly accesses the account, an assertion that due process has been complied with is surely not unfounded.

---

241 Permanent Bureau of the HCCH, *Practical Handbook on the operation of the Service Convention* (Service Handbook), 4th edition, 2016, Annex 8 Section D, para. 35.

242 *Baidoo v. Blood Dzraku* 5 N.Y.S.3d 709 (N.Y. Sup. Ct.2015), where a state court granted permission to serve the defendant solely via Facebook, holding that service by such a networking site, albeit novel and non-traditional, if certain procedures were followed, was reasonably calculated to provide notice and thus would comport with due process considerations under the circumstances of that case.

There is traction in domestic systems as far as service via social media is concerned, which indicates progress.[243] Such progression from a cross border perspective (with reference to the Service Convention) would in my view not only be welcomed but is vital in order to circumvent being stagnant. It would thus be remiss not to move with the times because as sure as it is that night follows day, social media is here to stay!

[243] *CMC Woodworking Machinery (Pty) Ltd v. Pieter Odendaal Kitchens* (unreported), High Court, 3 August 2012 (South Africa) Judge Steyn, para 2: "changes in the technology of communication have increased exponentially and it is therefore not unreasonable to expect the law to recognise such changes and accommodate them".

LEGAL DOCUMENTS AND CHAINS OF BLOCKS: TRANSMITTING AND STORING LEGAL RECORDS VIA DLT

(SUMMARY PREPARED BY THEOPHILUS EDWIN COLEMAN BASED ON MADI SAKEN'S PRESENTATION)

During the *Unplugged: NewTech* session, **Madi Saken**, Senior Legislative Coordinator of the Blockchain & Data Center Industry Association of Kazakhstan, talked about the possibilities and challenges posed by Distributed Ledger Technology (DLT) in relation to handling legal records. He first explained the general operation of DLT and provided examples of its application. Then, he contrasted the potential benefits with the challenges associated with this technology. Finally, he concluded that DLT has a great potential to impact the way we store and transmit information.

I. Background

Blockchain and DLT have proven to be promising technologies for recording transactions, including legal records. The main features of blockchain and DLT, unlike traditional databases, are the immutability of data (thereby preventing falsification) and the automation of records. These technologies are designed to track all records of transactions, as well as any changes in the system, since these records are synchronised across the network and visible to every party in that network.

The two salient technological features of blockchain and DLT are the distributed network, and the encryption of data. In a distributed network, a database is comprised by the information stored in different servers (nodes) which are synchronized and conform a network, as opposed to replicating or copying the database from one server into other servers. Importantly, DLT permits that every transaction is stored efficiently in such a way that all these new records are stored according to specific programming rules, synchronized across the nodes; therefore, data is considered immutable as it is not subject to unilateral modification.

The use of blockchain and DLT in the context of a multi-party system, such as the one within the HCCH 1965 Service Convention, has good prospects. For instance, these technologies can aid in the transmission and storage of legal and other judicial documents by enabling each server of a contracting Party to the Convention to come together and form a blockchain network. Using such a system for transmitting and storing legal documents has its own specific benefits and promises. Some of the problems include, but are not limited to, issues of data processing, access or security.

II. Applicability of blockchain to the HCCH 1965 Service Convention

a) Scope of the technology

Mr Saken clarified that blockchain only deals with transactional information that is transmitted and stored in a particular system, *i.e.* a certain event or fact, and its time-stamp. Accordingly, it is important to realize the purpose and the most feasible use of DLT in the near future. One of the challenges in the context of the Convention is ascertaining the substance of the document that is being transmitted or stored in the system. That is to say that validating the characteristics of a document or whether a document complies with certain standards, such as model forms, would hardly be possible at present, even when in the future Artificial Intelligence may help sort this; the focus thus should be on recording communicational transactions.

b) The problem of data access

Another challenge of using blockchain will be data access, especially regarding confidential documents. This would require the need to provide a complex multi-level 'access right list' for the parties. That is to say, there should be an identification of all the users that will have authority to deal with certain documents, such as state officials and the parties to the proceedings. This implies that the question of granting access rights should be administered by each state party of the blockchain. However, this may lead to some challenges.

The crucial question is how a multi-party blockchain should work when most parties have their own data security regulation and would most likely insist on a secure integration with their closed-circuit governmental information systems. The current trends show the development of private blockchains and so--called nodes clustering, *i.e.* when some part of a set of information within a network is visible only to a certain party. Cluster blockchain might be the future for such multi-party systems. However, giving each party the right to have its own closed-circuit without granting access to certain information to another party, would mean that parties would have to put in place a complicated storage and transmission architecture, and mark some information as visible to some parties and other information as not visible to other parties.

c) Problem of delivery

The main issue is whether blockchain can properly record the facts connected with the delivery of documents in light of Article 6 of the Convention, which requires effective proof of delivery, along with the time, place, methods and identity of the addressee. It could be challenging for a blockchain system to meet these requirements, especially regarding validation of the circumstances of delivery as required by the Convention.

Therefore, physical delivery would be a challenge for the whole blockchain system, which value is based on transactions within a digital environment. Perhaps, all the chain of communication could be done digitally, from the transmission of the request to the services of process itself. However, that would require a permanent intermediary such as a party that owns a standard database containing the legitimate contact information and identity of the addressees.

In the future, using a DLT-based digital channel for transmitting documents may show its key benefits, such as:

- credible time-stamped records at each or most of the stages;
- deeply synchronized storage and transmission of information;
- possibility to trace back where problems arise, if any;
- reduction of time, costs, etc.

The positive trend in this regard is that some countries have legally adopted and institutionalized communication through electronic means. For example, obligatory mobile registration can be helpful in terms of using mobile phones as tools for authenticating the identities of addressees. The same could work in terms of email, if there are legitimate emails for all the addressees. Moreover, there is a trend in certain industries to rely on the internet of things to record circumstantial information.

Some additional questions concern who would administer this complex architecture or who would bear the costs.

III. Conclusion

Madi Saken concluded his presentation by explaining that the adoption of blockchain technology is received with skepticism in many industries, due to the complications associated with implementing blockchain systems.

However, there are good prospects regarding the transmission of data and legal records, including, for example, the possibility that the information, facts or transactions recorded within the blockchain system is used in a court of law in a way that such information would not need to be proved and could automatically be recognised by the judicial authorities. Even though the use of blockchain has its own open questions, positive trends in the business industries illustrates how this technology could change the way information is stored, transmitted, and communicated.

BRIDGING THE DIVIDE:
THE ROLE OF A SCANNED AND PRINTED DOCUMENT

BY ELLEN M. GILLEY[*]

The inaugural HCCH a|Bridged conference challenged its speakers and audience to examine the opportunity electronic and information technology offers service of process abroad under The Hague Service Convention (the "Service Convention").[244] In many respects, the messages were optimistic—they charted how technology can be leveraged to advance the Service Convention's goals of efficient, timely, and secure service of process,[245] and they explained how the impersonal aspects of technology could be softened through the involvement of people.[246]

As is often the case, the stumbling block to using technology in legal practice is not technology, but the law. To fully benefit from technology, policymakers and lawmakers must wrestle with how and when the law will catch up with the innovations of the day. However, the events of 2020, most notably the COVID-19 global pandemic, has highlighted a different question: how can technology be used right now, within the constraints of the current legal framework, to reduce human-to-human contact? While we must ask the aspirational questions of how to fully embrace technology, we must not lose sight of practical considerations and immediate needs. It is from this perspective that I evaluate the role of technology on service of process abroad.

I. Context – The Service Convention

The Service Convention innovated service of process through the use of Central Authorities, which are agents physically located in each of the signatory states that execute service of process on individuals or entities in their jurisdiction. This is preserved in the Service Convention's "main channel" of transmission.[247] Broadly, service of process under the main channel operates as follows: (1) the institution that has authorized service of process (such as a court) sends the request to the Central Authority located in its state (the "Requesting State"); (2) the Central Authority of the Requesting State sends the formal request to the Central Authority where the intended recipient has a known address (the "Requested State"), and (3) the Central Authority of the Requested State executes service of process according to its internal laws.

Ellen Gilley is an Associate at Ropes & Gray LLP and also lectures on topics of international law. She thanks Secretary General of the HCCH, Dr. Christophe Bernasconi, and Dr. Gérardine Goh Escolar for the invitation to present at the conference. She also thanks Monica Mleczko, an Associate at Ropes & Gray LLP, for her invaluable research.

244 The *HCCH Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* (hereinafter "Service Convention").

245 For example, Emma van Gelder and Madi Saken addressed the role of distributed ledger technology ("DLT") for service of process abroad, and Christine Kalibbala addressed the potential for service of process by social media.

246 Aashna Bhikari provided her insight on the need for personal service of process from her experience as a Dutch Judicial Officer.

247 Service Convention, Art. 5(1).

When the Service Convention was enacted in 1965, each step of international service of process required physical delivery of hardcopy documents because borders were fixed, and geographical points had to be physically crossed. As a result, service of process developed and still operates in a geographically dependent framework.

II. The Technological Opportunity – e-Service

However, now this method of physical delivery is unnecessarily burdensome. As a snapshot, between 2009 and 2013, there were approximately 37,000 known requests under the Service Convention.[248] As Katerina Ossenova discussed in her presentation, this means a single Central Authority can be handling hundreds of thousands of pages of documents.

Technology, specifically cloud-based computing, can reduce the paper, time, and human-to-human contact of physical delivery with electronic service of process (or "e-Service"). Through email or DLT or other cloud-based services, the request and documents can travel to the intended recipient via both Central Authorities all by pressing buttons.

III. The Legal Constraint – Choice of Law

Nothing in the text of the Service Convention prevents us from using technology in transmitting documents through this main channel, and the Service Convention itself has been deemed technology neutral.[249] However, before advocating for full use of e-Service, we must address a threshold choice of law question: what law governs proper execution of e-Service?

The Service Convention governs the *transmission* of service of process abroad, but the *execution* of service of process is determined by domestic or municipal law, specifically, the law of the jurisdiction where the intended recipient has a valid address.[250] Physical delivery neatly fits this paradigm, as physical delivery must occur in the jurisdiction where the address is located. Like the law, it is *geographically dependent*. However, e-Service is not tethered to a specific location or jurisdiction because accessing or receiving cloud-based documents, such as through email, can be done anywhere. It is *geographically independent*.

For example, imagine a resident of France is served via email. Although she has a physical address in France, she might receive the email while in Spain, and the location of her email server, if even ascertainable, could be in another country, such as the United States. In this relatively simple illustration, three different jurisdictions have been implicated, and, as of now, we do not know whether the law of France, Spain, or the United States would govern execution of service of process.

---

248 HCCH, Synopsis of Questionnaire (2014), p. 20.

249 HCCH, Electronic Data Interchange (2000), pp. 27-28.

250 Service Convention, art. 5(1) (requiring that the methods be either "prescribed by [the Requested State's] internal law for the service of documents" or not "incompatible with the law of the [Requested State.]" This is consistent with international principles of service of process more generally, which look to the law where service is executed to determine proper service of process.

This is not an academic question. Ensuring we can point to a set of laws upon which to judge effective service is crucial. It is crucial for the proper functioning of civil litigation, upholding a defendant's due process rights, and respecting the sovereign rights of a state to regulate service of process in its jurisdiction. Before e-Service is used across borders, these choice of law rules must be developed.

IV. The Practical Solution – Scanned/Printed Documents

In the meantime, technology can—and must!—be leveraged to make the process more efficient and, as 2020 has shown us, to reduce human-to-human contact. My proposal is to use technology that can bridge the geographically independent framework of cloud computing with the geographically dependent framework of the law. That requires nothing more sophisticated than a scanner and a printer:

The original, hardcopy request for service of process can be scanned and electronically sent to the Central Authority of the Requesting State.

That scan can be electronically sent to the Central Authority of the Requested State, reducing the time and effort of hard-copy delivery.

Once received, the request can be printed and served according to the domestic laws of the Requested State.

By hitting "print," the request is taken from the cloud, where it is untethered from geography, and grounded in the same jurisdiction as the intended address. Transforming electronic documents to hardcopies may be a common, even outdated, technological process, but it makes the applicable law clear. It is a practical, interim solution while we solve the policy question of when and how the law will adapt to e-Service.

FROM PHYSICAL LOCATION TO ELECTRONIC ADDRESS: OMNIPRESENCE IN THE ERA OF THE INTERNET

BY NICOLÁS LOZADA PIMIENTO

According to the United Nations,[251] over 1,5 billion people lack meaningful access to justice for civil, administrative or criminal matters, and 4,5 billion people are excluded from the opportunities the law provides.

Partly, this is because cumbersome procedures and excessive formalities still abound in legislations around the world. In Civil Law countries, many of the procedures in force nowadays do not differ much from those of Roman Law. Bringing cases is not only time consuming and subject to rigid rules, but also extremely expensive.

I. The use of electronic service in comparative law

Online Dispute Resolution (ODR), i.e. the use of electronic means for case managing and decision-making, has been widely promoted as a feasible response to this lack of access to justice and a means to expedite and improve judicial proceedings.[252] Legislations around the world have started to steer in the direction of incorporating ODR into their own processes.

Colombian legislation, for example, provides that communications between parties and tribunals may be conducted by e-mail both in civil procedure and civil arbitration[253].

According to Article 23 of Colombian Arbitration Statute[254], every single procedural step,[255] including hearings, may take place electronically. In particular, all communications may be served electronically. E-mail is even allowed to serve the writ of summons or commencement of proceedings.

With email, locating a defendant becomes easier. Claimant does no longer need to know in advance his defendant's physical address. Nor is it required to have an officer of the court to undertake the task of locating and servicing a person.

---

251 *Justice for All,* Report of the Task Force on Justice, April 2019, page 11. Available at: < https://reliefweb.int/sites/reliefweb.int/files/resources/task_force_on_justice_report_conf_version_29apr19_1_1_1_compressed.pdf >.

252 Report of Working Group III (Online Dispute Resolution) on the work of its twenty-second session Vienna, 13-17 December 2010, Available at: < https://undocs.org/en/A/CN.9/716%20 >.

253 It is allowed also in the article 103 of General Process Code of Colombia, which regulate the civil procedure and works for all process that does not have a special regulation. Available at: < http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html >.

254 Available at: < http://www.secretariasenado.gov.co/senado/basedoc/ley_1563_2012.html >.

255 This includes electronic hearings, submission of memoranda, servicing of opening of procedures and even judicial decisions.

Although a claimant does need to know his defendant's email address, all companies must register an official electronic address for judicial purposes in public databases. Many individuals have also registered email addresses, although this is not mandatory. Defendants with registered addresses are presumed to receive communications in such address and can be legally served in such manner.

This is not just a Colombian trend. This is the standard the world is now adopting as in the Spanish legislation[256] and the European Union, more generally.[257]

II. Electronic Service and the 1965 Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters ('the Service Convention')

Article 1 of the Service Convention states that it "shall not apply where the address of the person to be served with the document is not known'.'[258] Given that Article 1 defines the convention's scope - in the negative - the convention does apply if the address of the person to be served is known.

Furthermore, according to Article 10(a) of the Convention, it provides that if the State party does not object, it is possible to transmit judicial documents or serve the initiation of a judicial procedure "*by postal channels, directly to persons abroad*".

A case can be made under Public International Law that the terms *'address' and 'postal channels'* included throughout the Convention are open terms, including both physical and electronic forms.

For this purpose, a good starting point is article 31 of Vienna Convention on the Law of Treaties, which provides the general rule of treaty interpretation: "*A treaty shall be interpreted in good faith in accordance with the* **ordinary meaning to be given to the terms** *of the treaty in their* **context** *and in the light of its* **object and purpose."**[259] (emphasis added).

a) Ordinary Meaning of the Words

Following its ordinary meaning, if a word has more than one meaning, its interpreter should accept as valid both meanings unless the treaty itself restricts this wide interpretation. If the provision does not distinguish, the interpreter should not distinguish either.

---

256 In Spain, the article 41 of the *Law on the Common Administrative Procedure of Public Administration* allows the electronic notification. In addition, the same law states some exceptional matters where this type of notifications is prohibited, available at: < https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10565-consolidado.pdf >.

257 The EU has implemented the e-Curia free application, which allows the parties to exchange procedural documents with the Registries by exclusively electronic means. Since its establishment in November of 2011 this method has been remarkably successful, as evidenced by the increase in the number of access account holders, available at: < https://curia.europa.eu/jcms/jcms/P_78957/en/ >.

258 Art. 1 of *The Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial*, Available at: < https://www.hcch.net/en/instruments/conventions/full-text/?cid=17 >.

259 Available at: < https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf >.

Apart from the regular definition of *'address'* as a *place* where a person may be communicated with, the Merriam Webster Dictionary also includes "*the designation of an account from which one can send or receive e-mail.*"[260] '*Postal,'* for its part, is defined as '*related to the post,'* which in turns is, among others, defined as *"something (such as a message) that is published online."*[261]

The International Court Justice (ICJ) has endorsed a "wide sense" interpretation in its *jurisprudence constante*. In *Lybia vs. Chad* and *Australia vs. Japan*, for example, it indicated that ordinary meaning of the words was sufficient to interpret a term.[262] Therefore, scientific or *specialized* definitions are not accepted unless it is a complex term.[263]

In short, physical and electronic addresses; as well as regular and online postal channels should be permissible under a wide interpretation of the Service Convention.

b) Today's context

An interpretation in context considers the text of a treaty by updating its provisions into the current circumstances. Technologies historically unavailable at the time of conclusion of a treaty, must be contemplated in the current interpretation of a treaty.

Interpreting the 1965 Service Convention according to today's context means recognizing that almost the entirety of the world's business communications no longer takes place via regular postal service, but online.

An interpretation in context would, therefore, embrace the prevalence of digital communications and would allow for electronic servicing.

c) The Efficiency Purpose

Moreover, in the light of its object and purpose, an interpreter should look into the true objectives pursued by a treaty to reveal its true meaning.

In its preamble, the Service Convention signatories expressed their desire "*to create appropriate means to ensure that judicial and extrajudicial documents to be served abroad shall be brought to the notice of the addressee in sufficient time*", with the aim to "*simplifying and expediting the procedure.*"[264]

The best way to ensure that documents and procedures are served in a simple and expeditious way is by allowing the use of electronic servicing. E-mailing is simple (there is no need for duplicates), takes a few seconds to be completed (as opposed to months), can be easily traceable from origin to destination (without intermediaries), and its integrity is certifiable with the common-use technologies.

---

260 Merriam-Webster Dictionary, available at: < https://www.merriam-webster.com/dictionary/address >.

261 Merriam-Webster Dictionary, available at: < https://www.merriam-webster.com/dictionary/post >.

262 Territorial Dispute (Lybian Arab Jamahiriya v. Chad) Judgment, ICJ. Decision 03/02/1994, p. 4.

263 Whaling in the Antarctic (*Australia v. Japan; New Zealand intervening)* Judgment, ICJ. Reports 2014, p 226, para 82.

264 Preamble, *HCCH Service Convention.*

Electronic servicing would also be in line with an increasing body of international treaties and soft law expressly leaning towards the validity of electronic communications; especially, the UN Electronic Communications Convention, Article 8.[265]

III. Final Remarks

Using the technology that surrounds us in the Internet Era and applying it to dispute resolution will result in faster and more efficient procedures.

In the current context of the Hague Service Convention, and in light of its object and purpose, it is possible to envisage electronic service if "address" is interpreted as "electronic address" and "postal channel" is interpreted as "e-mail."

This open and modern interpretation would be aligned with the trend adopted in legislations around the world acknowledging that it is considerably easier, simpler and more effective to locate a person online than it is physically. After all, one could say "not a single leaf of a tree moves without the internet knowing."

This does not, however, means that the gateway is closed to regular servicing by other official channels provided for in the Service Convention. Regular service can and should be available for people without access to Internet and whose email address is not known or unreliable.

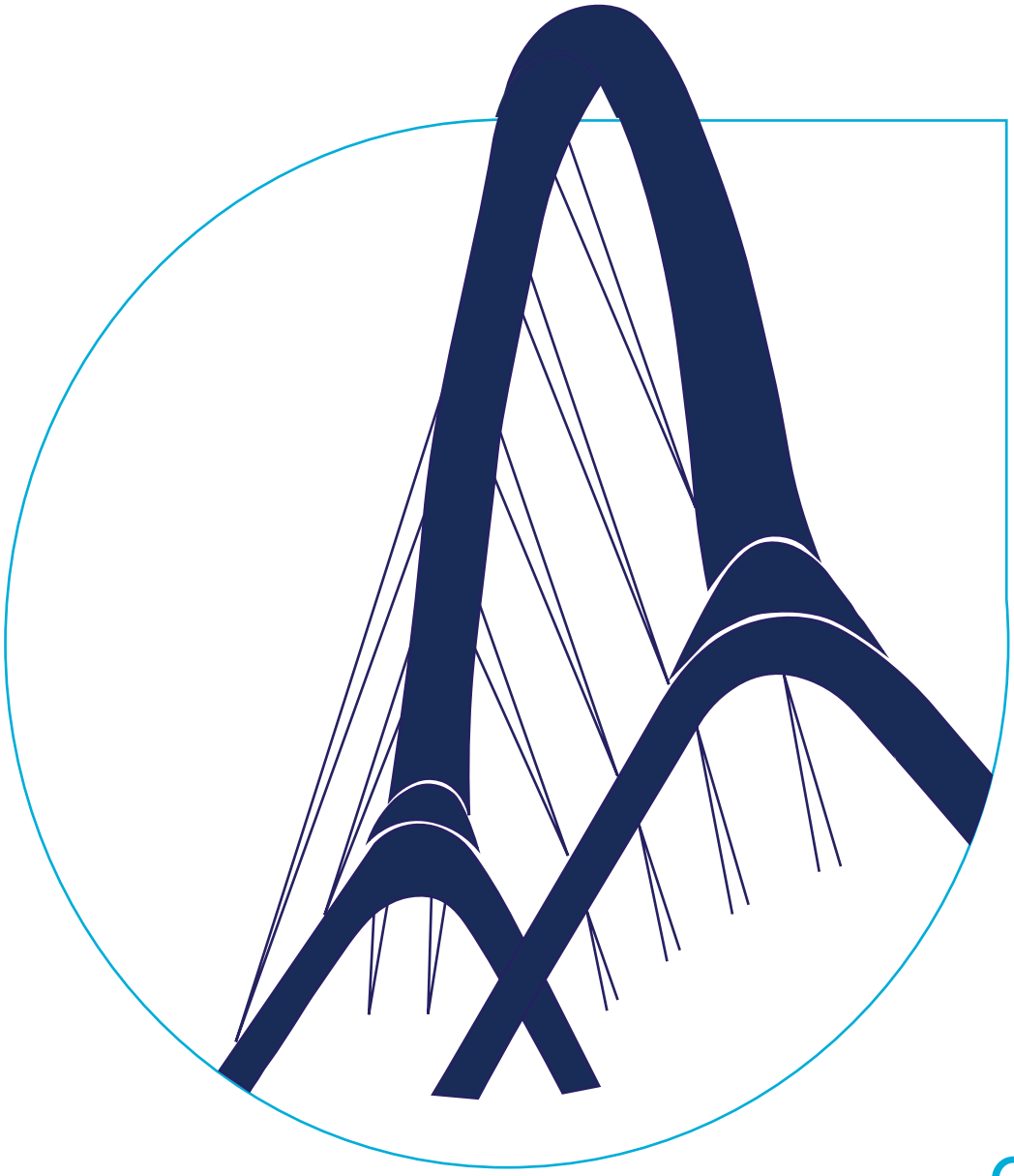
Balancing the traditional methods and procedures with the technological tools at our disposal will bring a real revolution in access to justice.

---

[265] The Art. 8 of the United Nations Convention on the Use of Electronic Communications in International Contracts states:

''1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

2. Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct''. Available at: < https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf >.



Conclusion

HOW MANY LIGHTBULBS DOES IT TAKE TO CHANGE A LAWYER? FUTURE-PROOFING THE HCCH SERVICE CONVENTION IN THE ERA OF ELECTRONIC AND INFORMATION TECHNOLOGY

BY GÉRARDINE GOH ESCOLAR [*]

"Question: How many lawyers does it take to change a lightbulb?

Answer: How many can you afford?"[266]

I. Introduction

The quality of lawyer jokes seems to be in direct proportion to the public cynicism the legal profession generates. Hidden in plain sight among the "knock, knock" and lightbulb jokes appears to be the conviction: Lawyers are Luddites, and expensive ones to boot.

But is that true? The Hague Conference on Private International Law (HCCH) convened the inaugural *HCCH a|Bridged* event on 11 December 2019 to test this hypothesis.[267] Focusing on the HCCH Service Convention[268] in the Era of Electronic and Information Technology, the event brought together legal and technology experts from every continent in open dialogue. Live-streamed online in an interactive format, the event prompted reactions both in the room and across the world. This summary of the discussions that day aims to be a synthesis of the contributors' thoughts, drawing common threads of the debate together in a tapestry of trends, ideas and solutions.

All contributors pointed to a single tipping point development in the application of the HCCH Service Convention – the digitisation of human society and the economy. The contributors noted that digital society and the digital economy have brought about three megatrends: a) democratisation, b) a blurring of formal territorial borders, and c) increased scrutiny of issues relating to privacy and security.

Concerns highlighted by the contributors fall into two main categories: the logistical, and the technical. Digitisation and the implementation of new technology raise issues not only in relation to funding and operational costs, but also in regard of the (legal) authority that will supervise its operation. Contributors note that not only would the HCCH Service Convention be looked to as a focal point in the harmonisation of the law relating to service

---

[*] First Secretary, Permanent Bureau, HCCH. The author thanks Raquel Salinas Peixoto (Legal Officer, HCCH) and Natalie Ka Yau Chan (Intern, HCCH) for their invaluable input. All opinions and errors remain entirely those of the author, and do not engage the organisation(s) with which she is affiliated. Reference in the footnotes to articles, unless otherwise cited, refer to those in this publication.

[266] J. Fuqua, cited by S. Zaretsky, "How Many Lawyers Does It Take to Change a Light Bulb?", *Above the Law*, online at: < https://abovethelaw.com/2011/08/how-many-lawyers-does-it-take-to-change-a-light-bulb/ >.

[267] Recordings of the event are available at: < https://www.hcch.net/en/instruments/specialised-sections/service/hcch-a-bridged/ >.

[268] *HCCH Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters* ("HCCH Service Convention"), concluded 15 November 1965, text available at: < https://assets.hcch.net/docs/f4520725-8cbd-4c71-b402-5aae1994d14c.pdf >.

of documents abroad, but that it could also serve as a focal point in terms of harmonising the technology and practices used.

II. The Tipping Point

The hot button issue that provides the backdrop for *HCCH a|Bridged Edition 2019* is the digitisation of modern society and economy and, by extension, the legal landscape. Contributors explored whether and how modern technology can be used to improve the service of documents abroad. In most cases, the discussion centred on the use of secure email, a common or interoperable electronic platform, and distributed ledger technology ("DLT") or cryptographic technology. Contributors acknowledged that there may be a gap in technology adoption rates between Contracting Parties, as well as a lack of trust in a new system that more established and traditional means (e.g. postal delivery) may inspire. Given that contemporary society is now well past the tipping point in relation to digitisation developments, many contributors also explored the possibility of the HCCH operating digitised infrastructure for the service of documents abroad under the HCCH Service Convention.

A heartening development in this regard is the growing adoption rate of digital technologies across the world. Digitisation of the judicial process is well underway in various jurisdictions, including England and Wales, South Korea, and Brazil. Courts in England and Wales are undergoing a GBP 1 billion reform programme, with a central component of this reform a "core case data" containing all relevant case information in a database with which each jurisdiction has an interface. An online money claims service and an e-filing system are currently employed, and in the future, this system is intended to manage requests under the HCCH Service and Evidence[269] Conventions.[270] South Korea currently employs an advanced e-filing system as part of its e-litigation system. In this system, all participants have their identity verified through an authentication certificate. Registered members may use this system to file complaints online, attach documentary evidence, and pay court fees. The system is also used for posting e-documents to be served.[271] The Brazilian judiciary makes use of a digitised legal system for various purposes: as an electronic judicial process platform, a national adoption and reception system, a national prison system and socio-education measures enforcement system, and an online litigation platform, all as part of a national interoperability model (NIM).[272] The NIM is used in Brazil to set the standard for the exchange of procedural information within the judiciary, including the electronic consolidation and transfer of procedural data between various judicial actors. Its standard implementation ensures unification, inviolability, and security of legal procedures, including where procedural secrecy is necessary or mandated.

Digitisation may not only be necessary for the HCCH Service Convention to adapt to modern means of communication and work, but also to diminish the trade-off between efficiency and security of service. While acknowledging that making e-service mandatory may be overreach, some contributors noted that an interpretation of the HCCH Service Convention relying on functional equivalence may be sufficient to incorporate new

269 *HCCH Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters*, ("HCCH Evidence Convention"), concluded 18 March 1970, text available at: < https://assets.hcch.net/docs/dfed98c0-6749-42d2-a9be-3d41597734f1.pdf >.

270 D. Cook, "The Lab: All Across the World – England and Wales".

271 Y.J. Choi, "The Lab: All Across the World – South Korea".

272 Summary prepared by L. Theunissen, C. Vieira von Adamek, "The Lab: All Across the World – Brazil".

technology, so long as the main principles regarding electronic documents, identification and security can be clarified, as they have been for some other HCCH Conventions.[273]

A novel development in the digital economy/society is the evolution of DLT and cryptographic technology. In the context of service of documents abroad, three values are of vital importance: the trust between Contracting Parties (including between the respective Central Authorities), the identity of the authors and editors of the document, and the integrity of the document.[274] DLT may increase document security and traceability, improving the security of communication. However, the decentralised nature of DLT may cause undetectable breaches in the system, and would require the implementation of cryptographic security systems, which in turn require substantial amount of computational power and energy. Drawing on the experience of various States across the world, some contributors note that Contracting Parties should first reach a consensus on the software, protocols and responsibility for supervising and funding the DLT system, and the dispute settlement mechanism for issues arising out of its operation, including the establishment of a minimum international regulatory standard. Some contributors also conclude that, in conceiving of DLT as a data management model where transactions are recorded simultaneously on a great number of computers around the world, DLT embodies three features that are relevant to the HCCH Service Convention: distributed trust in the system, a decentralised consensus mechanism, and equality between participants.[275]

III. Megatrends

Three megatrends as a result of the digitisation of the legal landscape were continually identified by the contributors:

- Democratisation,
- Blurring of formal territorial borders, and
- Privacy and security concerns.

These will be summarily discussed in turn.

a) Democratisation

Some contributors argue that DLT is a crucial asset in improving the service of documents abroad; specifically, DLT reinforces access to justice and facilitates cross-border civil proceedings, allowing service abroad of documents to be conducted in a simple, efficient and secure way. This democratises civil procedure, providing security through time-stamping and tamper-proofing, and makes the service easily possible from anywhere in the world at any time.[276]

An issue close to the heart of access to justice is how efficient service may preserve the principles of democratisation, fair trial and procedural equality. Inadequately served documents may be used to show that proceedings were unfair, and one contributor highlighted the need for retaining guarantees currently provided by judicial officers when digitising service of documents abroad. In particular, the contributor identified six barriers

273 X. Kramer, "Are you being served? Digitising judicial cooperation and the Hague Service Convention".

274 E. Van Gelder and E. Themeli, "Reflections on the use of distributed ledger technologies for the purpose of the HCCH Service Convention".

275 F. Guillaume and S. Riva, "Launching the HCCH Service Convention in the Crypto Space".

276 *Ibid.*

to the extensive use of electronic service abroad: technical, legal, informational, linguistic, costs and limited trust. In overcoming these barriers and democratising the service process, however, it is important to balance the goals of democratisation with the necessary procedural safeguards.[277]

In line with these concerns, another contributor is of the opinion that, despite technological advancements, postal channels will remain relevant for the service of documents abroad. While the terminology used in the Convention (particularly Article 10(a)) allows the Convention to keep pace with modern technological developments, the notion of "postal channels" was so ubiquitously understood and has remained largely unchanged since the days in which the HCCH Service Convention was being negotiated. The ubiquitous understanding and use of "postal channels" contribute greatly to the democratisation of procedures for the service of documents abroad.[278]

Democratisation can hardly be discussed today without an in-depth look at social media. At least one contributor argues that social media is a strong contended in the race to facilitate electronic service abroad. Considering its global reach and accessibility, social media has great potential for simplifying and expediting the service procedure, thereby promoting greater access to justice. Despite an explicit reference in the HCCH Service Convention to social media, this contributor argues that, under the functional equivalence approach, social media could possibly one day be acceptable as a means of service abroad. The contributor acknowledges the challenges that must be overcome before that day, including issues of identity verification, informational privacy, and a general reluctance to adopt unconventional methods of service. However, the contributor remains optimistic that social media may one day prove to be a vital instrument for the application of the HCCH Service Convention.[279]

b) Blurring of formal territorial borders

Access to information on a blockchain removes temporal and territorial constraints on service and the progress of proceedings. As noted above, this not only democratises civil procedure, but also blurs formal territorial borders.[280] However, this blurring of territorial and traditional State boundaries raises the question of whether blockchain technology would comply with the HCCH Service Convention's provisions on transmission, the principles of non-discrimination, technological neutrality, and functional equivalence. Some discussion centred on whether, as the HCCH Service Convention was drafted at a time where special attention was given to territoriality and sovereignty, the development of new technology may warrant a change in how the Convention conceives of territorial delineation.[281] This contributor noted that a paperless age is also one that can be borderless, and that there may be a need to take stronger legal measures that guarantee the continued relevance and applicability of the HCCH Service Convention.

277 A. Bhikari, "The importance of service of process".

278 B. Warren, "You've (still) got mail: Postal channels in the 21st century".

279 C. Kalibbala, "Trending on social media? #You've been served!".

280 F. Guillaume and S. Riva, see *op. cit.* note 275.

281 L. E. Teitz, "Is the Service Convention ready for early retirement at age fifty-five? Or can it be 'serviceable' in a world without borders?".

c) Privacy and security concerns

Privacy and security concerns invited much discussion from the contributors. Although there is no consensus as to how privacy and security could be or, indeed, should be guaranteed, there is some agreement that an effective solution implies a trade-off with efficiency.

Privacy and security concerns within the process of digitising methods of document transmission were raised, although one contributor noted that it would be illogical to avoid the use of digital (specifically, email) transmission simply because absolute security cannot at present be guaranteed.[282] Methods of guaranteeing postal authenticity, whether postal or digital, are available, and if digital methods of transmission are secured with additional technologies such as public key encryption (PKI), DNSSEC and DKIM, the transmission can be robustly and cryptographically protected. However, in order to do so, Contracting Parties must overcome barriers to the adoption of such technologies. This contributor proposed a cost-benefit analysis in order to ascertain whether the HCCH itself could operate the PKI infrastructure to ensure secure digital transmissions for service abroad.

The issue of privacy also came up in the discussion surrounding the use of a common electronic platform to aid in the transmission of requests under the HCCH Service Convention.[283] The purpose of such a platform would be to centralise and streamline procedure, promoting communication and interoperability between Contracting States and increasing accountability in the fulfilment of Contracting Parties' international obligations under the HCCH Service Convention.[284] Given the complicated logistics of implementation, as well as the amount of sensitive and personally identifiable information required for the service process, the contributor noted that many issues that must be resolved before such a common platform can be established. These include the privacy and security regulations that would apply, the requirement in some States for a hard copy of the service request, standardisation of digital and electronic signatures, formalities relating to proof of service, and responsibility for the costs and operation of the common platform.

An apt analogy in this regard could be drawn from the modified 2007 European Union Service Regulation, under which the mandatory electronic transmission of requests is considered in the context of three mechanisms: a common IT platform, secure emails, and a decentralised IT system. In elaborating on the pros and cons of each of these three mechanisms, the contributor particularly emphasised security and data protection, as well as interoperability.[285]

IV. A Solution?

Several solutions put forward by contributors advocate a multifaceted approach, including the seamless use of traditional and modern technology (e.g. faxing and then printing hard copies of documents),[286] and the use of a combination of permissioned/permissionless blockchains.[287]

---

282 T.J. Folkman, "Email as a secure means of transmission under the Service Convention".

283 K.V. Ossenova, "Use of an electronic platform for communication and transmission between Central Authorities in the operation of the HCCH Service Convention".

284 F. Heindler, "Nationally developed IT systems and the HCCH Service Convention".

285 M. Vautravers, "Knowing me, knowing EU: Security and Data Protection".

286 E.M. Gilley, "Bridging the divide: The role of a scanned and printed document".

287 F. Guillaume and S. Riva, *op. cit.* note 275.

One contributor proposes a unique solution to the choice of law issues which has thus far precluded the possibility of electronic service across borders. Unlike physical delivery, electronic service is not tethered to a specific jurisdiction, which creates an issue regarding choice of law. The contributor suggests an elegantly simple solution: documents can be scanned and then printed at the jurisdiction of the intended addressee, thereby ensuring that the applicable law is certain. In the mix between the old and new, this practical interim solution allows a geographically-independent technical framework such as cloud computing to be definitively linked with the geographically-depending legal framework within which electronic service currently functions.[288]

Another possible (future) solution is the use of DLT and blockchain. This solution does give rise to some issues related to scope, data access and delivery. In particular, since blockchain deals exclusively with transactional information, the ledger itself cannot ascertain whether a document complies with certain formal requirements. Moreover, the integration of closed-circuit governmental informational systems with the blockchain will create complex issues of granting access rights, identification, and confidentiality of information. Additionally, blockchain may be unable to record all the factors required by Article 6 of the HCCH Service Convention, such as effective proof of delivery. It was also noted that many industries, the legal one among them, are sceptical of adopting DLT and blockchain. However, DLT demonstrates great potential to improve the storage and transmission of legal records and documents, especially in forms that are, or can be, legally recognised.[289]

In considering how best to future-proof the HCCH Service Convention, the majority opinion among the contributors is that, as new technology "revamps" traditional application and approaches to the Convention, it also increases access to justice. In a reading of the HCCH Service Convention with reference to the Vienna Convention on the Law of Treaties, it has been noted that the HCCH Service Convention could be given an interpretation that would extend to include electronic and digital means of transmission and service abroad.[290] In light of the object and purpose of the HCCH Service Convention – to ensure that service documents are "brought to the notice of the addressee in sufficient time" – it may be that electronic service is an increasingly obvious way to achieve this objective.

V. Conclusion

Perhaps the question should instead be, "How many lightbulbs does it take to change a lawyer?" As each idea becomes a lightbulb moment, then the answer to that, fittingly, is "How many can the lawyers afford?" How many good ideas does it take to change the attitude of the legal profession? How many can the legal profession afford to let slip by?

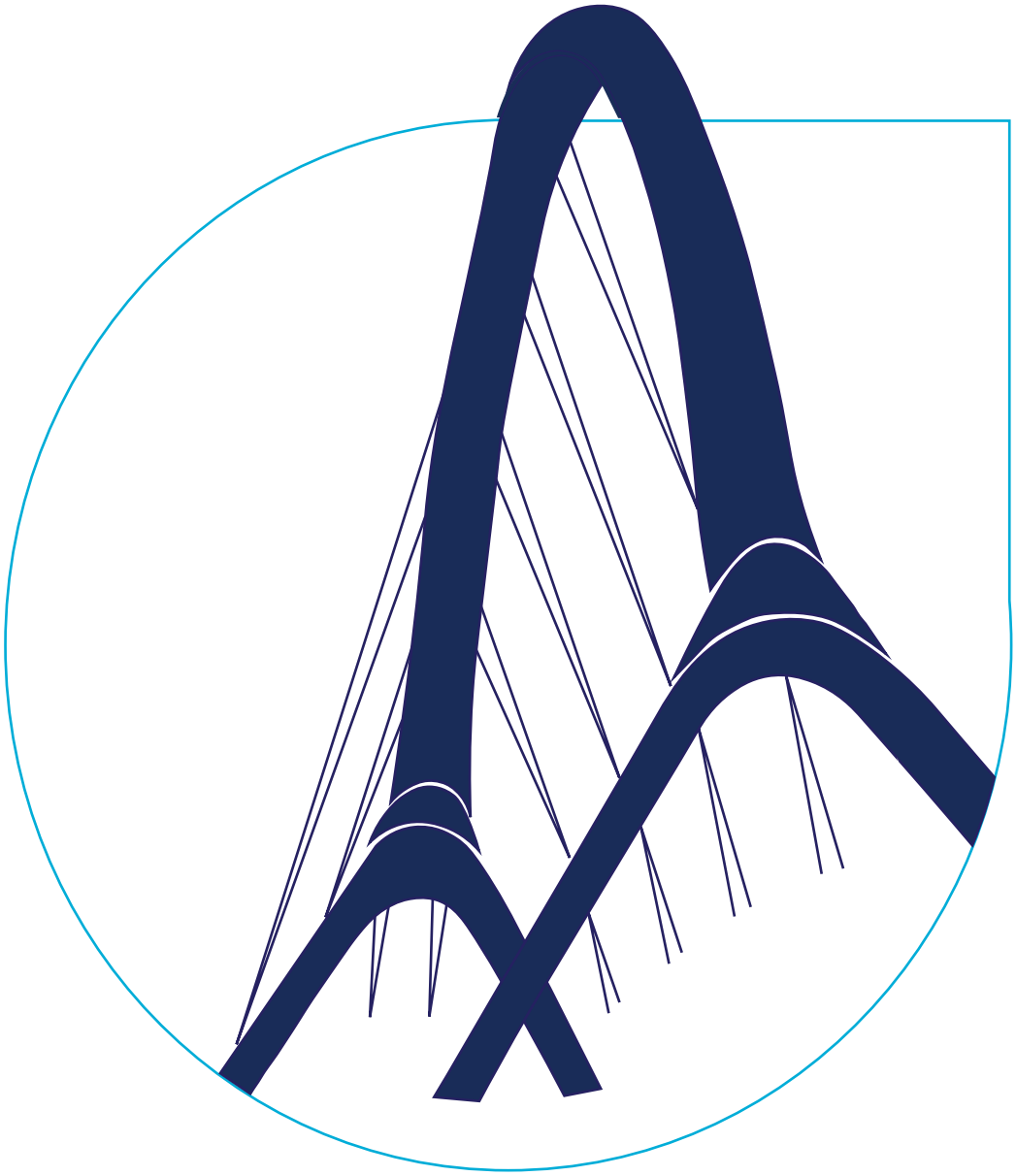
HCCH a|Bridged Edition 2019 brought hot button topics on the intersection of technology and the law related to service of documents abroad to the forefront. With an eye on the necessary proper safeguards, the technology neutrality of the HCCH Service Convention may be best guarded by an open-minded acceptance of the technologies that provide not just for the continuing relevance of the Convention, but for ever better ways in which to achieve its object and purpose.

---

288 E.M. Gilley, *op. cit.* note 286.

289 Summary prepared by T.E. Coleman, M. Saken, "Legal documents and chains of blocks: Transmitting and storing legal records via DLT".

290 N. Lozada Pimiento, "From physical location to electronic address: Omnipresence in the era of the internet".



Annex 1
Summary Programme

Summary programme of HCCH a|Bridged Edition 2019: The HCCH Service Convention in the Era of Electronic and Information Technology
11 December 2019, The Hague, Netherlands

09:00 **Arrival and Registration**

09:30 **Welcome**

Christophe BERNASCONI | *Secretary General, HCCH*

10:00 **Ground Rules**

Elizabeth ZORRILLA | *Legal Officer, HCCH*

Introspective and Three Questions

Gérardine GOH ESCOLAR | *First Secretary, HCCH*

10:20 **The Prism: The Tech Battle for e-Service**

Theodore FOLKMAN | *Partner*
Pierce Bainbridge Beck Price & Hecht LLP / Founder, Letters Blogatory

Katerina OSSENOVA | *Trial Attorney*
Office of International Judicial Assistance, Office of Foreign Litigation, U.S. Department of Justice

Emma VAN GELDER | *PhD Candidate*
Erasmus University Rotterdam / Research Member, Deep Tech Dispute Resolution Lab, Oxford University

Florian HEINDLER | *Assistant Professor*
Sigmund Freud University

11:15 *Break*

11:45 **HCCH Unplugged: The Convention Rebooted**

Knowing me, knowing EU: Lessons on Privacy & Security from the Service Regulation Revision
Marie VAUTRAVERS | *Deputy Head*
Private International Law Unit, Civil Affairs & Seals Directorate, Ministry of Justice, France

Can I help you, officer? Technology to the Aid of Judicial Officers
Aashna BHIKHARI | *Judicial Officer & Innovation Team Member*
International Union of Judicial Officers (UIHJ)

You've (Still) Got Mail: The Future of Postal Channels
Brody WARREN | *Legal Officer, HCCH*

12:30 *Break for Lunch*

14:00 **The Lab: All Across the World**

David COOK | *Queen's Bench Master*
Judiciary of England and Wales, United Kingdom

Yoon Jung CHOI | *Judge*
Seoul Central District Court, Republic of Korea

Carlos VIEIRA VON ADAMEK | *Judge & Secretary-General*
National Council of Justice, Federative Republic of Brazil

14:45 **HCCH Unplugged: NewTech**

Trending on social media? #YouveBeenServed!

Christine KALIBBALA | *Lecturer*
Wittenborg University / Catholic University of Lille

Legal Docs and Chains of Blocks: Transmitting and storing legal records via DLT

Madi SAKEN | *Senior Legislative Coordinator*
Blockchain & Data Center Industry Association of Kazakhstan

Scanned, Sealed, Delivered: The Legality of Scanned and Printed Documents

Ellen GILLEY | *Associate*
Ropes & Gray LLP

Let's Get Digital: Access to Justice in a digitized world

Nicolás LOZADA-PIMIENTO | *Partner*
Rincón-Cuellar & Asociados / Professor, Externado University of Colombia

15:30 **The Open Lab: The Text of Tomorrow**

Xandra KRAMER | *Professor of European Civil Procedure*
Erasmus University Rotterdam

Florence GUILLAUME | *Professor of Private International Law*
University of Neuchâtel

Louise Ellen TEITZ | *Professor of Law*
Roger Williams University

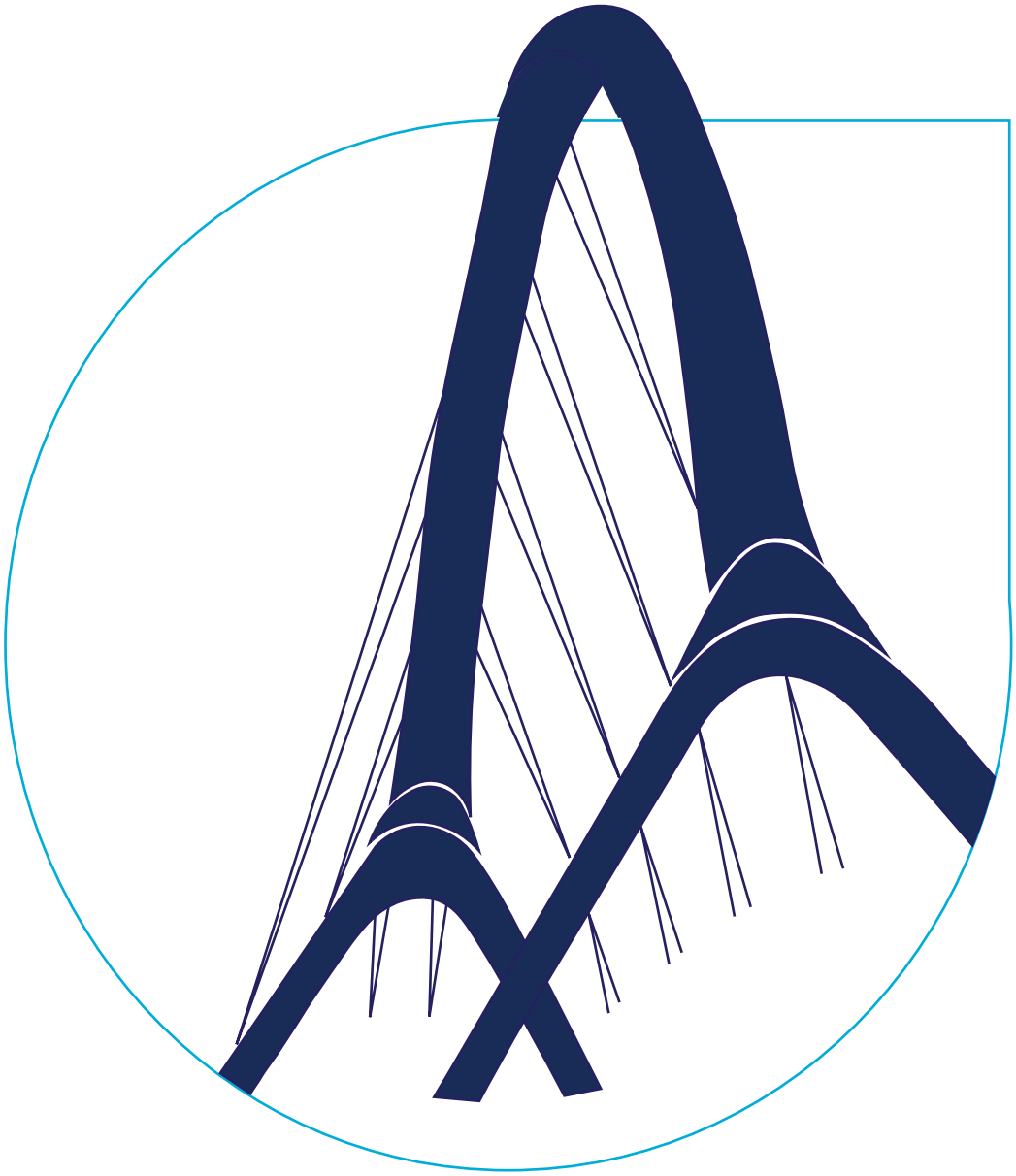
16:15 *Break*

16:45 **The Wrap-Up**

Gérardine GOH ESCOLAR | *First Secretary, HCCH*

18:00 **Networking Event**

Recordings of the event are available online on the HCCH YouTube channel at this link.



Annex 2
Contributors

Contributors to HCCH a|Bridged Edition 2019

Aashna BHIKHARI

Aashna Bhikhari is an Enforcement Officer based in the Netherlands. After graduating from the University of Leiden (majoring in International Law), she received an appointment in 2010 as a Judicial Officer. Since then, Aashna has witnessed the transformation of the profession from a traditional to a modern one, a profession where technology meets law. Her interest in international law took this to another level; therefore she has been appointed by the UIHJ as an expert and member of the Innovation Team. She is also a lecturer on both domestic and international litigation enforcement law.

Yoon Jung CHOI

Yoon Jung Choi graduated from Seoul National University in 2006. She was appointed as judge in 2008, and has worked at the Seoul central district court, Seoul western district court, Wonju branch and Goyang branch court. She received a master's degree in commercial law from Seoul National University School of Law in 2017, and visited the University of Southern California School of Law as a researcher in 2017-2018 supported by the Korean Supreme Court. She has published several papers about e-discovery, seizure and search of e-stored information. Yoon Jung was on secondment at the HCCH at the time of HCCH a|Bridged Edition 2019.

David COOK

David Cook was appointed as a Master of the Queen's Bench Division of the High Court in 2011. He is responsible for providing judicial leadership for the digital aspects of the reform programme in the civil jurisdictions of England and Wales. David is currently working on the establishment of the "On-line Court" and the roll out of an electronic case management system for the higher courts. He is a member of the sub-group of experts on the use of Video-link in the Taking of Evidence Abroad under the HCCH Convention and was a member of the European Commission's expert group on Modernisation of Judicial Cooperation in Civil and Commercial Matters.

Theodore FOLKMAN

Theodore J. Folkman is Founder of Folkman LLC. He was a partner with Pierce Bainbridge Beck Price & Hecht LLP in Boston, Massachusetts. He handles complex civil and commercial cases with a special emphasis on cross-border disputes. He is widely recognised for his expertise in international judicial assistance, including the taking of evidence for use abroad and the HCCH Service and Evidence Conventions, and is the author of several relevant chapters and articles as well as Letters Blogatory, a leading blog on private international law topics. A graduate of Harvard Law School, Ted was elected to the American Law Institute in 2018.

Ellen GILLEY

Ellen Gilley is a senior associate at Ropes & Gray LLP and is based in Boston. Ellen's practice focuses on counseling clients on international and domestic disputes, including international arbitration, issues in international civil procedure, and disputes with governmental agencies. In addition to her practice, Ellen develops and teaches courses for practitioners and law students on international and comparative legal analysis, international arbitration, and communication and leadership. Prior to joining Ropes & Gray, Ellen served as legal advisor to Judge Rosemary Barketton the Iran-United States Claims Tribunal.

Gérardine GOH ESCOLAR

Gérardine Goh Escolar is First Secretary at the Permanent Bureau of the HCCH. Her portfolios span family law and child protection, and international commercial and financial law. Previously, she practised in international arbitration and litigation. She was Legal Advisor to the President of the Iran-United States Claims Tribunal, and principal legal officer in the chambers of a Judge at the International Court of Justice. Geri has served as legal officer in the service of the government of Germany, in-house counsel at a satellite geoinformation company, and VP (External Relations) at a start-up. She holds a doctoral degree from the University of Leiden, an LL.M. from University College London, and an LL.B. (Hons.) from the National University of Singapore.

Florence GUILLAUME

Florence Guillaume is a Full Professor of civil and private international law at the Faculty of Law of the University of Neuchâtel, Switzerland since 2006. She teaches courses in private international law, inheritance law, international family law, and international business litigation. Florence has been the Dean of the Faculty of Law and is currently member of the Council of the University. She has also been a professor on secondment at the HCCH. Before entering academics, she practiced as a lawyer at the Geneva Bar and the Zurich Bar. She also worked as Deputy to the Head of Private International Law at the Federal Office of Justice in Berne.

Florian HEINDLER

Florian Heindler is Assistant Professor at the Faculty of Law at Sigmund Freud University (Vienna) where he teaches private law and conflict of laws. Florian obtained his diploma in law from Vienna University in 2009, a diploma in philology in 2011, and a PhD in law in 2016. Since June 2017, he has been the Chairperson of the Interdisciplinary Association of Comparative and Private International Law (IACPIL). In 2019, Florian became an associate member of the International Academy of Comparative Law (IACL).

Christine KALIBBALA

Christine Kalibbala is an innovative and passionate international lawyer and academic based in the Netherlands. Qualified in Pretoria, South Africa (B: Com Law, LLB, Honours B: Com), Switzerland (Cert in Transnational Law, University of Geneva) and the Netherlands (LL.M. International Law and Globalization, Maastricht University) Christine advises on cross-border contentious and non-contentious legal matters. She has worked in private practice and in-house, lectures at Universities in the Netherlands and France and participated in the 28th session of the United Nations Human Rights Council in Geneva.

Xandra KRAMER

Xandra Kramer is a Professor of civil justice and private international law at the Erasmus University Rotterdam and Utrecht University in the Netherlands. Her research focuses on access to justice and justice innovation, the functioning of civil justice systems, international contracts, and transnational complex litigation. She has been involved in multiple studies for the European Parliament, the European Commission, and the Dutch Ministry of Justice, and is co-reporter of the overarching working group of the ELI-UNIDROIT project on European Rules of Civil Procedure. She is Principal Investigator of the ERC consolidator project 'Building EU Civil Justice'.

Nicolás LOZADA PIMIENTO

Nicolás Lozada Pimiento is a Colombian lawyer and techno-enthusiast. He is a Professor at Externado University, a partner at Bogota-based firm Rincón-Cuellar & Asociados, and an arbitrator at several Colombian and Spanish arbitration centers. His main fields of interest and practice are LegalTech, Alternative Dispute Resolution and International Law. In 2012, Nicolás was appointed Colombia's delegate to UNCITRAL Group III on Online Dispute Resolution (ODR). This led him to conduct research, promote legal reform, and become a speaker on the topic, including giving a Ted Talk.

Katerina OSSENOVA

Katerina Ossenova manages the Office of International Judicial Assistance, the U.S. Central Authority for the HCCH Service and Evidence Conventions, the Inter-American Convention on Letters Rogatory, and letters rogatory received through diplomatic channels. Previously, Katerina was an Attorney-Advisor International with the Commercial Law Development Program in the Office of the General Counsel of the U.S. Department of Commerce. She received her J.D. degree from the University of Pittsburgh School of Law and graduated with an International and Comparative Law Certificate.

Madi SAKEN

Madi Saken is a senior coordinator for government relations and legislation at the Blockchain & Data Center Industry Association of Kazakhstan. He is a member of the working group on the draft law "On Amendments and Additions to the Legislative Acts of the Republic of Kazakhstan on the Regulation of Digital Technologies" and one of the major drafting contributors with respect to regulation of blockchain, smart contracts, digital assets and personal data. Madi is a frequent speaker at governmental, legal, and IT events; a visiting lecturer at local universities; and works with the telecom sector in the field of big data analytics.

Louise Ellen TEITZ

Louise Ellen Teitz is a renowned scholar of private international law and international procedural law. Her areas of expertise include private international law, international litigation and dispute resolution. She has taught and been a visiting scholar at several U.S. and European law schools, the Max Planck Institute Luxembourg, UNCITRAL, and UNIDROIT. She was a member of the U.S. Delegation for the HCCH Judgments Convention and Choice of Court Agreements Convention, and the U.S. Secretary of State's Advisory Committee on Private International Law. She also served as First Secretary at the Permanent Bureau of the HCCH.

Emma VAN GELDER

Emma van Gelder is a PhD candidate at the Erasmus University Rotterdam in the Netherlands, working on the PhD project 'consumer online dispute resolution in the EU against the background of access to justice', within the wider ERC consolidator project 'Building EU Civil Justice'. Emma graduated from Utrecht University in 2017 obtaining her master's degree in Legal Research (cum laude). She is also a research member of the Deep Tech Dispute Resolution Lab at the University of Oxford.

Marie VAUTRAVERS

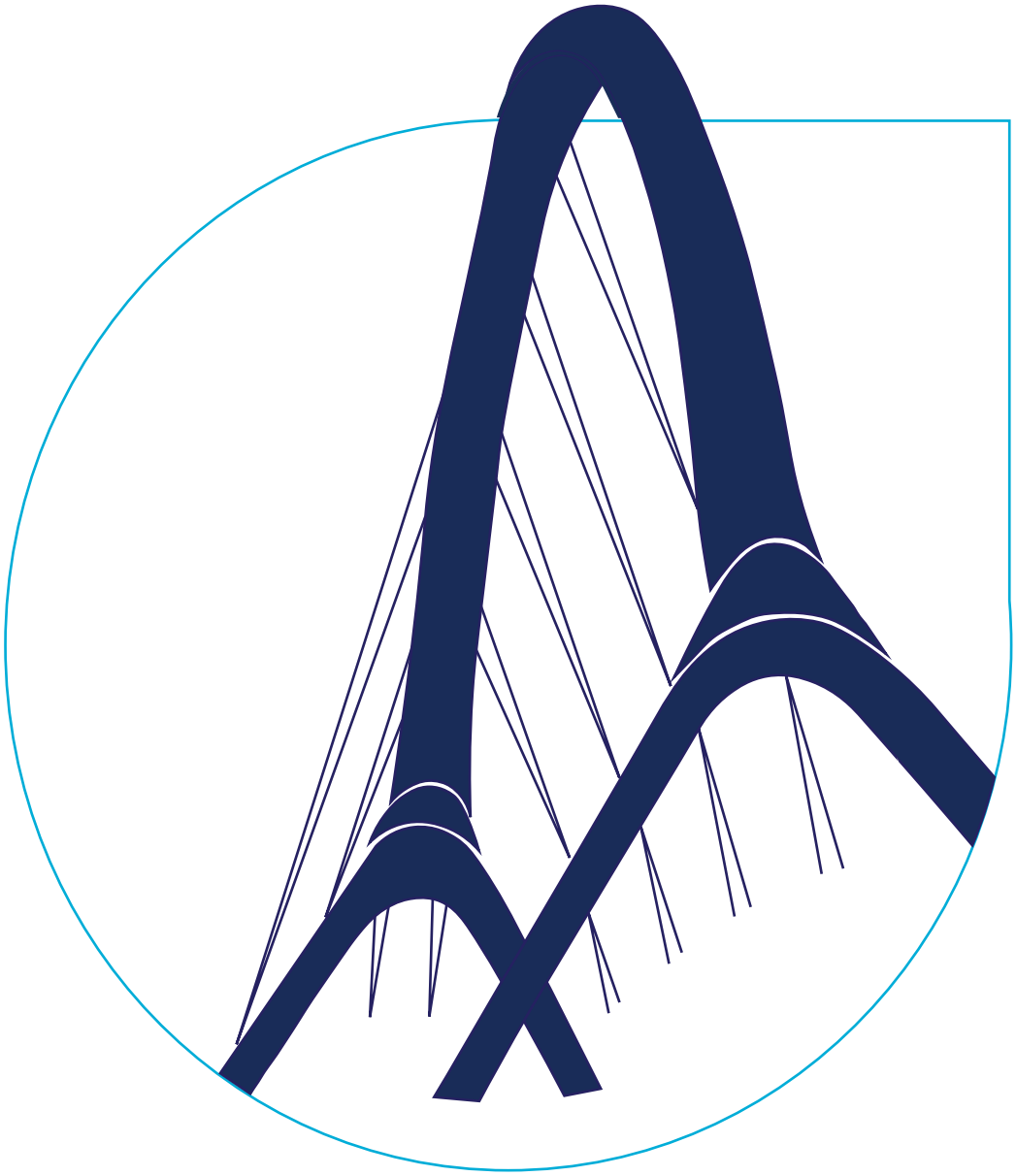
Marie Vautravers is a Legislative Officer at the Directorate General for Justice and Consumers of the European Commission. As former Deputy Head of the Private International Law and Judicial Cooperation Unit, she was previously in charge of the French Central Authority under the EU regulation and the HCCH Service and Evidence Conventions. She has previously worked as the iSupport Legal/Project Coordinator at the HCCH and was involved in the development of the iSupport case management and secure communication system. Prior to that, Marie was a Family Judge in France (Court of Evreux and Nanterre). She also holds a humanities degree (LL.L.) and is a graduate of Sciences-Po Paris and the École Nationale de la Magistrature.

Carlos VIEIRA VON ADAMEK

Carlos Vieira von Adamek has been the Secretary-General of the National Council of Justice (NCJ) since 2018. He has served as Judge of Civil Law and Electoral Judge in São Paulo, Assistant Judge and Instructor of the Superior Court, and Instructor Judge of the Supreme Court. Carlos has also served as Secretary-General of the Presidency of the Superior Electoral Court and Assistant Judge of the NCJ. He holds a bachelor's degree in law and a specialisation in Private Rights and Civil Procedural Law, both from the University of São Paulo. He has a postgraduate degree in Civil Procedural Law from the São Paulo School of Magistracy.

Brody WARREN

Brody Warren is Senior Legal Officer and Attaché to the Secretary General of the Permanent Bureau, HCCH. He joined the HCCH Permanent Bureau in 2014. He is part of the international legal cooperation and civil procedure team, responsible for the day-to-day work in relation to the HCCH Apostille, Service, Evidence, and Access to Justice Conventions. Prior to joining the HCCH, Brody worked for legal publisher LexisNexis in the Press Gallery of the Australian Federal Parliament. He holds a Bachelor of Laws (Honours) and Bachelor of Arts (Political Science/Spanish) from the Australian National University (Canberra, Australia) and is admitted to practice in the Supreme Court of New South Wales (Australia).



Annex 3
Sponsors

HCCH a|Bridged
Edition 2019

brought to you in partnership with

Federal Ministry
of Justice and
Consumer Protection

ROPES & GRAY

Hague Conference on Private International Law
Permanent Bureau

Churchillplein 6b
2517 JW The Hague
The Netherlands

Tel.: +31 70 363 3303
Fax: +31 70 360 4867
secretariat@hcch.net
www.hcch.net

HCCH

Connecter Protéger Coopérer Depuis 1893
Connecting Protecting Cooperating Since 1893