出國報告（出國類別：出席國際會議）

2016 年全球網路及管轄權研討會報告
GLOBAL INTERNET AND JURISDICTION CONFERENCE 2016

服務機關：法務部

姓名職稱：資訊處高級分析師林美綉

國際及兩岸法律司科長李蒂娜

派赴地點：法國巴黎

出國期間 **:105** 年 **11** 月 **14** 日至 **105** 年 **11** 月 **16** 日

報告日期 **: 106** 年 **2** 月

目錄

壹、前言

網際網路跨國特性，對於經濟社會、政治提供前所未有之利益，但是也因為跨境網路之方便性及其應用，也造成全球網路上所適用之國家法律之緊張局勢逐漸增加。由於犯罪調查越來越需要境外之私人公司所儲存之使用者資料及數位證據，傳統之司法互助顯無法因應，為避免各國立法以資訊提供者將計算設施設於國內作為服務提供者在其領土內執行業務之條件，妨礙企業發展，或因而導致各國網路使用取得不平等，造成對於接近即使用資訊之人權造成損害情況，則在設施不在國內之情況下，究竟如何迅速取得犯罪資料或嚇阻犯罪之發生，如何在既無損業者之利益，又不造成人權危害之情況下，加強跨境合作，遂成為重要議題(from legal arms race to transnational cooperation)。

本會議係由網路及管轄(internet & Jurisdiction，I & J)組織所舉辦，該組織係一個全球多方利益關係人政策網絡(A global multi-stakeholder policy network)，成立於 2012 年，為非營利、中立之組織，經費來源為德國外交部、瑞士政府、Google、微軟、臉書、迪士尼等公私部門，宗旨在致力於促進司法互助、人權、數位經濟及網路安全間之和諧，期能透過全球性之政策過程發展出一套既可加強跨境合作又不影響網路無所不在特色之途徑。該組織目前的執行長為 Bertrand de La Chapelle，曾擔任法國外交官等職位。

本次會議為 I & J 首次召開之全球性會議，地點在法國外交部部長會議中心，為期 2 天半，全程以英文進行，我國出席人員為法務部資訊處高級分析師林美綉及國際及兩岸法律司科長李蒂娜，與來自美國、歐盟、法國、巴西、德國、印度、韓國、阿根廷、英國、比利時、聯合國、經濟合作暨發展組織(OECD)等來自 40 個國家及組織，超過 200 名政府、網路平臺、技術、社會團體、學界及國際組織之官員同聚一堂，討論跨境網路之未來管轄問題。

貳、會議介紹與議程內容摘要

一、2016年全球網路及管轄權會議

本次會議時程由 2016 年 11 月 14 日至 11 月 16 日止，首(11/14)日辦理報到、開幕及第一全體會議，次日(11/15)進行分組討論，第 3 日(11/16)進行分組討論結果報告、第二次全體會議

及閉幕式。第 2 日分組討論分為 3 組，包括資訊與管轄(Data & Jurisdiction)、內容與管轄(Content & Jurisdiction)、網址與管轄(Domain & Jurisdiction)，本部代表參加資訊與管轄小組之討論，討論重點在於跨境資訊流之管理原則以及隱私之保護與網路濫用者相關資訊合法取得間如何取得協調。

與會人員在會議期間，除討論各國、地區、組織間就此議題所做之努力及進展外，亦對此議題之發展提出許多前瞻性及建設性的意見和建議，且高度肯定 I & J 擔任此多方利益關係人合作交流平臺之貢獻，期許未來持續召開類此會議，強化彼此聯繫，增進不同利益關係人間之瞭解、擴大共識、發展友誼、加強合作，期能發展出一套所有利益關係人雖不能滿意但均可接受之準則。

二、發言重點

（一）開幕式

跨境網路之管轄及未來/所有利害關係人共同關注之議題

1. 瑞典前首相、網路治理全球委員會主席 Carl Bildt 表示，該委員會成立於 2014 年，29 個會員經過 2 年努力後完成一份報告，提供給對這些議題可能帶來之可能性及挑戰之大仍不甚瞭解之決策者做為參考。此外，該委員會也出版了包括管轄、網路安全、治理規則、國家監控及暗網（dark web）挑戰等議題之文章共 50 多篇。他認為網際網路在很短的時間內已是全世界最重要之基礎建設，成為全球社會及經濟建設之基礎。有人稱之為第四次工業革命。但事實上，我們是在工業革命的最終階段，逐步邁入對政治、經濟、社會帶來充滿挑戰及無限潛能之數位時代。對於那些錯過參與工業時代的國家也提供大量機會。透過網路之協助，我們看到一波數位創業浪潮正在席捲全世界。我們同時也看到危害網路未來的不信任感在逐漸加深，包括對於政府及私人企業處理個人資料的不信任、對於網路穩定及安全的不信任、對於網路管理者生態系統及網路管理可能性的不信任。這些逐漸加深的不信任感倘若不處理，將對網路的未來及全球的未來帶來危機，因為政府可能要求設施落地並進行資訊監控，可能影響層面不僅包括希望成為數位世界王國之私人公司也可能造成個人乾脆拒絕使用網路。因此，我們必須採取行動。但因為這些都是不容易的議題，所

以，在行動前，我們必須深思熟慮、多方討論。這些議題正在打破西發利亞條約所建立之全球秩序基礎，如何處理這些議題將型塑我們的全球數位未來。Carl Bildt 強調必須先找出爭議所在，然後一步一步設法解決。未經深思熟慮之行動可能導致解決方式之誤用，對未來造成嚴重後果。基本上，這些解決方式必須尊重聯合國宣言中之基本人權保障，網路上亦然。國家的功能之一就是保障這些權利，也因此，國家應該維護法治。這在有邊境、絕對管轄的年代，並不難達成，但在目前社會及經濟加速互相依賴，合作關係逐漸加深的數位時代裡，儼然已是個挑戰。未來我們或許能夠對於網路治理之全球性生態系統達成共識，但目前離此目標還十分遙遠。由於不同國家、不同社會有不同價值體系，因此，藉由一步一步尋找務實解決方式，能夠逐漸建立互信，發展出不損害人權之運作方式。希望藉由更多決策者參與討論能夠一步一步建立數位未來之治理方式。

2. OECD 副秘書長 Douglas Frantz 表示，網際網路全球互連之特性創造了極大社會及經濟利益，帶動了國際性之革新。網路是沒有國界的，但是法律不是。因此，國際合作之需求由此而生。 國際合作已成為 OECD 工作裡越來越重要之主題。最近的一項研究顯示，國際合作在包括基本研究、國際智慧財產權、租稅及政府治理方面更顯重要。同樣地，OECD 也注意到與網路法律相關之國際合作需求逐漸增加。每個國家均有處理與網路相關議題之法律，根據這些法律與規定，政府及私人企業根據這些法律與規定，向其他國家的網路業者提出請求，要求他們刪除網頁上之內容、扣押網域名稱、提供關於使用者之保密資訊。這些來自不同管轄領域之請求，不僅本質不同、要求取得之證據不同、要求回應之時間不同，同時也不見得提供確認要請求者身份之適當資料或者透過主管機關提出請求，有時也沒解釋不同管轄權領域的法律衝突應該如何解決。因此，處理這些請求耗費相當多資源，可能對中小型企業造成影響，小型網路企業更可能因為可處理這些請求耗費大量資源而無法繼續經營下去。大量的請求，不管合法與否，也可能影響較大公司繼續經營之能力。面對這種威脅，企業可能決定，除非是來自其管轄權領域內之法院命令，否則一概置之不理或者因為希望儘快解決這些請求，因此決定完全配合。這兩種結果對於網路的開放都有不好的影響。如果某個國家發現請求始終被外國公司擱置，

可能制訂設施落地之強制性法規。如果網路業者選擇一味退讓，則毫無根據之刪除、扣押或使用者資訊之移轉情事必然發生，這將造成對網路資訊接近及使用之減少，嚴重損害使用者之信任，從史諾登透露美國監看網路事件對美國雲端公司之影響就可以知道當網路使用者覺得無法再信任這些公司時，後果會是如何。OECD 去年 6 月就數位經濟在坎昆召開之部長級會議中得到的重要訊息之一就是網路開放帶來強大利益，我們必須確保網路開放。網路開放增加國際貿易，網路購物佔美國 2011 年出口之三分之一。2013 年，Paypal 支付平台就經手 440 億元跨境交易。如果網路流受到阻礙，上述那些經濟的瓦解還只是冰山一角。網路開放鼓勵創新及創業，提供提升社會福利之機會。因此，OECD 開始進行一項名之為抓住數位化帶來之成長利益及福祉計畫，協助各國利用數位科技繁榮發展。因此，問題不在各國能否發展出放諸四海皆準之運作程序，問題在能不發展出這樣的程序嗎？透過這個會議的討論，希望能夠在保留網路全球化之特性下，讓跨國法律程序一致性，使每個人都能更方便、有效使用網路。也許像 Google 或 Facebook 這種網路巨人已經有資源追蹤各國法律，處理各式各樣的請求，因此對這種法律程序一致性之需求可能並不迫切，但是對於一些創新性的小企業卻絕對有此必要。OECD 一向鼓勵透過多方利害關係人之對話發展出自願接受之行為準則。有了大家都可以接受之準則，投資者不需要擔憂因為各國不同程序帶來的成本增加，將會較為願意投資網路創新事業。消費者無庸擔心因為任意資訊刪除、網域名稱被扣押或使用者資訊任意提供，造成法律上之權利受到損害，將會較樂於使用網路，帶來數位經濟之成長。同時，為達成數位經濟時代，經濟及社會之發展，數位安全及隱私保障都必須要處理，透過 I ＆J 召開的此類會議之多方對話，希望能夠取得使用者及政府對於網路安全及隱私保障更多之信任。

3. Google 副總裁暨歐洲、中東及非洲區公共政策及政府關係主管 Nicklas Lundblad 表示，這幾天所要討論之議題，事實上早在 1996 年 John Perry Barlow 發表網際空間獨立宣言(A Declaration of the Independence of Cyberspace)時就已經開始討論，接著是 Johnson &Post 的法律與國境(Law and Borders)，然後到 1998 年 Jack Goldsmith 的反對網路無政府狀況(Against Cyberanarchy)，Google 就在這個時候成立了。從成立以來，Google

一直在面對及嘗試處理這些議題。Google 認為這種多方利害關係人共同參與的會議相當重要，因為透過各種利害關係人的參與與討論，能夠發展出值得推薦、眾人均能接受之處理方式。我們必須從不同的反應觀察科技帶來的改變。其中一個重要的反應是體制反應。哈佛大學社會生物學家 E. O. Wilson 有句名言，人類最大的挑戰是我們有著舊石器時代的情感、中古世紀的體制及神一般的科技。這三者間之衝突必須設法解決。Nicklas Lundblad 提出四個問題作為與會人士將來討論之重點。第一個問題是從簽署西發利亞條約前關於管轄的原則我們學到了甚麼？中古時代的作者就已經列出 18 種帝國管轄的態樣，思考在與領土觀念切割下，管轄會是甚麼樣子。因此，在討論網路空間的管轄之際，或許那些著作是值得參考的。第二個問題是解決兩個城市間的管轄問題？點越多，參與的行為者越多，合作的誘因越高，結果會是如何？聯合管轄如何運作？第三個問題是如何加強不同法制間之連結性？如果可以解決這個問題，就可協助每個人、每個公司找到所有的平衡點。第四個問題是科技能夠做甚麼？科技無法協助我們解決這些問題，但是也許有些科技的成分能夠協助我們設計新的系統、體制，這種體制能夠讓維護網路的開放，促進經濟成長，但又能保護我們珍貴的基本人權不受侵害。這些問題都是 Google 目前仍然沒有答案的問題。

4. 全球資訊網基金會(World Wide Web Foundation)非洲區召集人 Nnenna Nwakanma 表示，在該基金會工作，使其瞭解網路文化，與網際網路發明人也是該基金會創辦人 Tim Berners-Lee 對談，使其瞭解 Tim Berners-Lee 為了人類福祉，願意將發明無償提供給大眾，使大眾可以從中獲益。因此，這種為提升公眾利益的開放精神也應該是現在全世界可以使用網路的人應有之共同願景。網路創造了 Amazon、Google 以及 Facebook 等全球性企業，網路創造財富。政府也因此可以與人民更直接溝通，提供更多公共服務、更有效的公共行政，讓人民有機會接收關於權利、健康、教育等資訊。在非洲，每天有許多年輕人都想利用網路就學、創業，他們會詢問網路上的課程是否會被承認，在非洲 Paypal 如何支付、網購商品如何退貨等問題，這些人都希望透過網路尋找機會。但是他們面臨許多挑戰。如何讓網路能夠在各地存在，如何確保每個地方的每個人都能享受網

路所帶來的社會、政治及經濟機會？網路之普及化應該是聯合國 2030 年永續發展目標中 leave no one behind 承諾的基礎建設，但是如何保持網路開放？如何使用網路？如何增加大眾之選擇？隱私及網路安全間之戰爭，政府要安全，人民也要安全，所以這不是二擇一的問題，是如何兩全其美的問題，要完成這個任務必須政府間、利害關係人，產業或學界一起努力。網路超越領土，但是網路如何超越種族，文化，宗教、年齡、職業？這是個大家需要深思的問題。我們需要的是鼓勵競爭與經濟成長、提升生產力、保障言論自由、激發創新並且眾人均可參與的問路空間。

5. 聯合國教科文組織(UNESCO)溝通及資訊處助理處長 Frank La Rue 表示，聯合國非常希望看到一套放諸四海皆準的正當法律程序的產生。但也因為教科文組織的人權、文化及倫理三個任務，所有議題都必須在這三個標準下審酌。該處主要的任務是保障言論自由，這包括搜尋及接收、接近及使用資訊及分享資訊之權利。就搜尋及接收資訊部分，該處與聯合國國際電信聯盟(International Communication Unit)合作，讓全世界更多人可以透過網路相互聯繫。而根據聯合國的 2030 年永續發展議程(The 2030 Agenda for Sustainable Development)，聯合國認為透過網路接近及使用資訊及溝通為言論自由的基本構成要件，而言論自由又是民主國家民眾參與的基本權利，唯有社區參與，許多計畫才得以實現，透過行使接近及使用資訊之權利，眾人可以相互連結，不因經濟、區域、文化或種族不同而有差異。這也代表必須尊重隱私溝通權利。在處理暴力、極端主義、仇恨性言論時，也不能忘記隱私權的保障。該組織發展出判定是否為仇恨性言論的 5 項判斷標準，包括主觀犯意、內容相關、傳播範圍大到足以引起危害、危害必須特定可能、危害必須具急迫性。建立全球一致的標準相當困難，因此，有必要讓所有之國家參與討論訂定。而在個案處理上也會有問題，到底由何國何法院管轄，各國標準為何。該組織對於文化相關性方面採取比較有彈性的作法，文化是溝通的基本成分，網路可以反應文化的不同，但是不能因文化的不同來限制人權，人權是基於人性尊嚴，不能有所例外。因此，目前的最大難題就是如何讓各國訂定不同法律程序，但又確保這些法律程序不違反人權，聯合國目前正嘗試透過對話、透過不同機制進行討論，希望能夠加速目標達成。

（二）第一天全體大會/網路上的管轄現狀

1. 美國國務院網路議題召集人 Christopher Painter 表示，從擔任聯邦檢察官開始即處理網路犯罪，迄今已有 25 年。此等議題均相當艱難且具體，並非抽象或理論性議題。隨著人類越來越依賴科技，這些爭議也變得越來越複雜，在外交方面，因此等爭議所導致之緊張情勢也逐漸增加。透過網路方式之跨境破壞行動可能對於國家安全造成威脅或帶來極大損害。美國以尋求共識、促進積極國際合作之方式，來面對不同威脅及網路資訊系統的跨境特質。美國致力於宣導國際法亦適用於網路空間之概念。另外一個美國在宣導之概念為主權並非絕對，特別是在涉及人權時。在執法方面，電子證據扮演的角色日趨重要，目前許多公司都面對衝突的法律上義務，而處理跨境取得電子資料之機制顯然已無法因應。許多美國公司及美國員工，因為遵守美國法律而被罰款或監禁，這些後來也衍生許多外交問題也導致許多國家開始立法要求設施落地。美國司法部目前正在與英國進行協商，期能加速資訊之分享。此種新型態之架構將允許英國當局得在重罪及涉嫌帳戶非美國人或美國境內人民使用之前提下，直接從美國公司取得電子資料。假如這個雙邊協定能夠簽署，將成為美國可以與其他國家合作之平臺，因為透過此種協定在確保資訊取得之同時，亦可保障隱私及其他人權。一個全球性的條約或協定是不需要的，或者說這種協定目前是不太可能達成的，因此，讓既存之協定更有效率運作，是現今最佳之解決途徑。

2. 阿根廷現代化部(Ministry of Modernization)部長 Maria Ines Baque 表示，阿根廷總統宣示該政府之 3 個目標為減少貧窮、打擊毒品走私及阿根廷之團結，為達成這 3 個目標，透過網路之數位轉型扮演重要之地位。因此，有必要發展出涵蓋所有層並降低訊息鴻溝之公共政策。為此，阿根廷內閣新增溝通及現代化兩個部會，致力於發展網路基礎建設（目前在阿根廷還有 80%沒有網路）、確保該國人民不分地區、社會地位、經濟情況或文化條件均有網路可使用、發展電子化政府、電子化健康、線上教育、促進數位經濟及電子商務來解決貧窮及失業問題。但是數位轉型有其困境，例如政府可以利用現存之公共雲端服務加速轉型？如何保護資料隱私？如何在電子商務領域扮演電子化政府之角色？在一個對於言論自由、網路犯罪及網路安全有不同規定的世界裡，如何處理恐怖主義及其他

暗黑網路走私之網路內容？如何能不影響各國網路管轄權，又不對網際網路施以不必要之限制以免影響數位經濟？阿根廷希望能從其他國家學習並與其他國合作。倘若要確保數位時代帶來的利益，就必須解決數位環境的相關議題，而要解決這些問題，必須透過對於管轄及網際網路的討論。經由非網路生態系統政府參與之全球性對話過程，才能建立創新的法律架構，今天，我們所面對的挑戰需要國際合作及積極參與才能有效解決。

3. 聯合國反恐合作處處長及德國外交部網路外交政策司司長 Thomas Fitschen 認為一個實體的管轄權一般係指該實體得以立法及執法之正當權力。從國際層面上來說，係指一個國家可以透過立法機關、行政機關或司法機關造法的正當權力。因此，管轄權就權限的分配，就是某個有權機關可以決定法律為何，哪些行為是違法，所以，清楚界定在何處及何種情況下有管轄權是非常重要的一件事。為了瞭解管轄權，必須先瞭解主權。主權與領土關係密切。政府在領土內擁有主權，得以主張管轄權，但當一個政府就跨境事件主張管轄權時，問題因此產生，因為邊境之外是另一個國家，在那個領土內有另一個主權，所以要跨境執法時，必須得到該國的同意，特別是在這個經由網際網路即可未經同意進行各種跨境搜索及獲取資訊，這個原則也必須遵守。雖然可能因為網路犯罪涉及的犯罪人所在地、資訊所在地、證據所在地分散各地，使得所有資料取得更為困難，但是一旦跨境行動，仍必須得到該國的同意。網路犯罪公約已經解決了許多複雜及技術性的問題，但因網路犯罪公約只對簽署國有拘束力，全球其他有相同問題的國家也會有同樣的問題，因此，希望經由此種多方利害關係人的討論，能夠得到一個大家都可以同意的程序。

4. 國際刑警全球創新綜合總部處長 Brad Marden 從不同角度觀察這些議題，認為大家會來參與這些討論都是希望能夠阻止犯罪行為。不採取行動的成本最高，因為不採取行動打擊犯罪，將使網路使用者喪失對網路的信賴。國際刑警組織最近處理一個跟電子郵件相關的調查涉及多個不同管轄權主體，包括電郵被害人、詐欺被害人等，最後總共有 15 個管轄權主體。其中一些工作是透過司法互助程序完成。不過在找出行為人之前，司法互助程序基本上無法展開。此外，各國對於執法人員可取的資訊有不同規定，對於確認執法人員身份有不同規定，所以，如何確認要求協助的人確實是執法人員？加上還有雙重犯

罪及因果關係等問題，雙重犯罪原則在持有所需資訊之私人公司與犯罪毫無相關之情況下更為複雜，譬如某個人以電郵帳號登入一個犯罪論壇，該電郵帳號本身與論壇上的犯罪行為無關但卻可提供警方找出犯罪行為者資訊時，警方有何正當理由向第三者取得與犯罪無關卻很重要之資訊？該私人公司是否有義務提供該等資訊？國際刑警組織有一整個部門負責確保由私人公司取得之資訊不涉及種族、宗教、政府或軍事領域，只針對犯罪，但對於於私人企業，這樣的要求顯然是太過的，然而，如果這些問題不解決，開放的網際網路將可能導致違法亂紀的情事。

5. 電子前哨基金會(Electronic Frontier Foundation)法務處處長 Corynne Mcsherry 從討論 Equustek 案件切入。Datalink vs Equustek 案一般稱之為 Google vs Equustek ，是一個營業秘密案件。Datalink 這個公司指稱員工盜取營業秘密，並開始透過網站行銷利用該營業秘密製成之商品，因此，對該新公司提出侵害營業秘密訴訟。訴訟是在加拿大提出的，後來那個新公司離開加拿大，也就是加拿大沒有管轄權，但是仍然在網路上繼續行銷該等商品。Datatlink 取得法院命令，要求該公司停止行銷該等商品。但是該公司對該禁制令置之不理，因為公司已經不設在加拿大了，法院命令無法執行。Datalink 於是找上 Google，要求 Google 不要把販售那些產品的網站列入搜尋結果。Google 一開始不願意，後來自願同意取消一些，Datalink 就要求法院命令 Google 不要將全球銷售該等產品的網站列入搜尋結果，後來大家就開始對這個小案子感到興趣，因為如果一個加拿大的法院命令，一個境外的命令可以影響到全世界的人，這將會是個很糟糕的判例，因此，包括該組織對於法院提出法庭之友的書狀。該組織最初擔心的是怕會影響到美國使用者。在美國言論自由的保障也包括網路上的言論，而那種命令有違言論自由之保障，因此，除非是違反著作權法，否則法院不可能同意發給刪除內容的命令，此外，美國對於網路提供者也有很重的損害賠償規定，所以，該組織相當擔憂該命令可能帶來的影響。況且該命令也有正當程序方面之爭議，正當程序的最基本概念是除非參與法律制訂，否則不應受影響。但是倘若一個國家法律可以對另一個國家人民生效，而該國人民沒有相同機會去影響法律制訂，就是沒有經過正當程序。該案目前仍有加拿大最高法院審理中。法院應該下這

種境外命令嗎？如果可以，審酌之標準為何？法院首先該問的是這樣的命令是否有違他國之價值觀，原告必須提出證明，接著原告必須證明證據堅強，因為在此情況下，被告都不會到場為自己辯護，因此，原告必須證明實質傷害、無其他合理方式、命令可以執行等，然後再由法院衡量公益及私益做出決定。

6. 歐盟執行委員會司法及消費者總署基本權利及公民聯盟署署長 Paul Nemitz 表示，針對每個問題所提之解決之道，都應該要先問，這樣算不算民主，因為過渡強調科技成就、網路獨立宣言或者是過度強調網路帶來的經濟發展都是不民主的。民主必須透過法律實現。歐洲人民選舉議會代表時會希望透過這些代表立法及執行能夠改變世界。歐盟所保障的基本權利除了聯合國憲章所保障者外，也包括美國人民沒有但我們承諾給歐盟人民之權利，包括對於資訊保護權給予憲法層次的保障。因此，在討論隱私議題時，必須銘記個人資料的保護跟著資料走，個人資料不是一種商品，個資受到法律保護，因此，假如這些資料被安置、出售或旅行至某處，歐洲人民會期待這些資料會依據歐盟法律得到保障。在仇恨性言論方面，歐洲人民的期待可能與美國有所不同，如果行為是發生在臉書、Google、推特在歐洲以外的伺服器，則必須適用效力原則（Effects Doctrine），假如效力發生在歐洲，就應該依據歐洲法律來判斷。之所以特別提出民主，是因為希望在思考如何規範數位未來時，不要忘記民主為主要的判斷標準之一。

7. 加納國家資訊科技委員會主委 Nii Quaynor 認為這種政策網路代表著在管轄權架構內建立可互操作性方式的好機會。雖然許多問題見解有所出入，但可以先從找出較為簡單的問題，根據共識執行。加納國家資訊科技委員會負責政府網路，也是通用頂級域（generic top-level domain, gLTD）及國家及地區頂級域 (country code top-level domain, ccLTD)管理者。非洲已透過區域性經濟會議及非洲聯盟，對於法制有逐步整合，但是仍存在著技術性及能力建構方面有待加強。大部分有關法規都是規範某政府機關負責接受域名註冊，對於跨國爭議則尚乏規範。在加納實務運作上，聯繫窗口之一必須是加納管轄內的居民。社群網站的內容不存在我管轄領域內，讓事情變得更加困難。在加納等國，律師網絡及國家及地區頂級域管理者也許能在域名及內容議題方面提供一些協助，因為該區需要外

來積極的協助，也就是技術方面的加強，這樣如果法院命令一旦做成，貼在安全的 post-it 上面，可以執行該命令的國家，就可以協助執行。由於其身兼國家網路安全諮詢委員，亦將面對內容、管轄、刪除等議題，希望有個網絡能夠更快為大家處理法律上的請求。

8. 歐洲委員會代表 Elvana Thaci 表示各國及國際決策者都面臨著本計畫所要討論之議題。I & J 能夠協助國家及非國家成員找出問題，然後設法解決是一個很大的工程。I & J 有很完善的資料庫提供大眾使用，增進大眾對議題發展的瞭解。有些法律概念，例如歐洲人權公約第 10 條的跨界言論自由、國家跨境介入網路資訊流之責任、確認及執行管轄權等，透過諸如此類的討論已在歐洲之實體法及判例法中生根。希望本次會議討論能有所成果，作為歐洲議會制訂網路政策之參考。

（三）第二天專題討論：資訊與管轄（Data and Jurisdiction）

1. 有鑑於犯罪調查取得儲存在管轄範圍外私人公司資料庫之使用者資訊及數位證據之需求日漸增加，傳統司法互助系統顯已無法因應，許多國家間開始採取一些措施，試圖解決這些困難，但究竟具規模又可行之架構必須涵蓋那些必要的安全措施及程序？資訊與管轄的分組討論重點即著眼於為了處理濫用網路的情況，跨國資訊流、隱私權保護及執法機關合法取得相關資料間應如何協調。

2. 本組是由喬治亞理工學院法學教授 Peter Swire 擔任主持人，Peter Swire 畢業於耶魯大學法學院，曾擔任歐巴馬政府情報及資訊科技五人小組成員，是隱私權與網路安全法律專家。

3. 小組成員在主持人引導下，依據工作文件(Working Document)主要討論以下議題：

(1) 目前因應措施：由於目前跨國調查的情況日漸增加，傳統的司法互助及網路服務提供者自願性合作都遭遇大極大挑戰，國家或組織間所採取之面對方式。有些國家因為使用者資料取得困難，於是立法要求網路服務提供者必須將設施設立於國境之內(即設施落地，localization)，方便取證。但是，也有國家採取簽訂協定，如美國與英國間正在就進行雙邊協定洽談，希望能讓執法機關及國家安全當局在持有合法簽署的法院拘票後，能迅速從另一國的網路服務提供者取得相關資訊，而在歐盟及歐洲議會方面，則是與服務提供者包括 Google、Facebook 跟 Twitter 等公司共同擬定取得使用者基本資料的統一請求格式。有人認為設施落地可以減少經手那些個人資訊的人，可降低對於隱私權侵害的可能性也方便執

法人員迅速取得資料，但大多數人認為設施落地實務上不可能，因為必須耗費大量資源人力，成本增加，企業難以國際化，國家更可以藉此保護國內業者，加上各國標準不一，企業實際上也無法配合，而且在一些人權保障比較不足的國家，政府會拿這些資料去做甚麼難以預料，可能造成人權侵害加劇。

(2) 管轄及請求之法律標準：由於網路資訊分為內容及非內容（包括使用者基本資料(basic subscriber information)、登入時間(traffic data)等），哪些資料一定要透過跨境請求？回答此問題前必須先決定管轄，對於非內容資料是依伺服器所在地、使用者國籍、服務提供者公司總部所在地、犯罪發生地等。但是伺服器所在地的困難在於可能一封電郵主旨、內容、附件儲存在不同國家的伺服器，而採取使用者國籍的方式，也因為重要的是目標（即那些郵件等）所在地，使用者所在地或國籍的提供可能會有對使用者的隱私保護造成影響，至於公司總部所在地，雖然方便，但是仍有待企業與政府間去協調。較多與會人員認為應該沒有單一認定管轄的方式，而是應該採取綜合適用方式（Multiple Factor Application），但有人認為這樣當然就是認定的人決定，那個人應該會傾向於採取有利自己的管轄認定方式，讓自己的國家有管轄權。至於就內容資料，美國則要求要有 probable cause，但是其他國家的標準也不太一樣，因此，到底是採請求國或被請求標準，或者是有個共同的最低法律標準，則有待各方利害關係人繼續協調討論。

(3) 通知使用者:是否該通知使用者政府機關要求取得他的資料？網路服務提供者是使用者資料的保管人，服務提供者自然必須知道自己資料被提供出去，這就是透明化的要求，特別是在要求取得的人是政府機關時，又變成人權議題了，因此，網路提供者必須在政府要求提供使用者資訊時通知使用者，如此，倘若取得不適法，將來在法庭上，使用者才能夠主張自己的權利。網路服務提供者也應該定期發佈公告，讓使用者知道有各國有多少件請求、請求標的及是否提供等相關資料。

(4) 可能合作的領域：執法機關及服務提供者認為必須改善操作程序，在目前的法制情況下，兩者應該加強對話，讓案件偵辦能夠順利進行。例如，在法國爆炸案後，一些網路提供者與法國政府就如何讓請求格式一致化進行討論，並且訓練執法人員如何使用網路提供者可

提供的資訊，再執法機關建立單一聯絡窗口等讓程序進行更有效率。歐盟已經開始與網路提供者進行這種對話。社會團體建議，網路提供者如果與政府進行此類對話，必須要注意程序要透明化，讓網路使用者清楚此項對話進展以確保使用者的信賴。另外，繼續資訊分享也是與會人員認為可以合作的領域，本組已經透過電郵及網站分享新訊息。

（四）第三天全體會議

1. 加拿大創新科學及經濟發展部國際通訊政策及聯絡司司長 Erin Dorgan 表示，想要找出一個務實的解決途徑是一個很大的挑戰。在面對領土及合作議題時，一般人總是從自己的角度出發，所以大家必須超越特定利益、特定觀點並體認這個合作契機。網路管轄權的挑戰必須所有利害關係人的共同努力與革新。因此，不管是資訊、內容或網域方面的議題，都有必要由私人企業、學界、技術界或社會團體的人員參與討論。而政府機關則需要保持靈活，處理的方式必須有創意，必須發展出實際上可以在全球網路上執行之政策及法律架構。政府機關必須考量實務上網路交易知如何進行，資料、內容及網域是如何處理，政府也應該接受外界所提出之解決方式。由於網路已發展成網路使用者的得力助手，因此，有必要確保提出之建議能夠符合當前及未來網路使用者之需求及期待。多方利害關係人可以合作的領域包括建立共同的語言，加強內部能力建構及建構對於如何提出請求及收到請求後如何處理之透明化程序。我們如何面對這些挑戰及利用這些機會，將對未來之全球網路帶來相當大的影響。因此，對話非常重要，透過對話我們才能看到機會、聽到真知灼見。
2. 冰島傳播部媒體委員會主委 Elfa Yr Gylfadottir 表示，前一天內容與管轄那組得到結論是大家價值觀不同。但能得到這個結論的討論過程是很重要。由眾人就不同議題進行討論，得以獲致部分結論，釐清相同與不同看法，進而逐漸縮小差距。冰島政府覺得挫折感很重，因為從管轄權的角度來說，很多平臺提供者不認識冰島這類小國，但是在大國，對話似乎進得也不太順利。因此，不管大國或小國都需要這樣的對話機制，共同找到解決方案。參與的對象必須儘可能包括各類型之利害關係人。
3. 義大利外交及國際合作部政治事務與安全司副司長 Gianfranco Incarnato 提到，英國與美國已經將網路使用在打擊 ISIS 方面，但是至於程序如何進行則尚未形諸於文字。世界各

國領導者最需要的是安全，這也包括網路安全。另外，法國及德國內政部都希望能有體制性的規範，如此才能夠在恐怖攻擊發生時，迅速取得涉案者之個人資料。義大利也嘗試與暗網合作，暗網是不可忽視的一環。在 2016 年 7 月，北太平洋公約組織(North Atlantic Treaty Organization, NATO)正式確認網路空間為第五軍事作戰區域(fifth domain of a warfare) ，但是關鍵問題在於如何才能構成網路作戰?攻擊股網算不算?到甚麼程度?2 年前，許多國家在避免太空、網路間衝突之共同目標下，同意聯合國第 51 條之規定在如此類的衝突亦有其適用。但是判定之基本原則何在?比例原則應有其適用。國家發展網路武力之能力應受到管制，各國就網路犯罪應建立溝通平台，目前美國與中共正在進行網路武力管制的討論。

4. 里約科技與社會研究院院長 Carlos Affonso Souza 表示，I&J 的網站提供網路與管轄方面最新發展的相關報導，大家可以妥善利用。大家來這裡討論了很多爭議的問題，昨天在內容與管轄的分組討論中就提到被遺忘的權利(right to be forgotten)，有人提到這種權利可能只有歐洲人有，巴西或中國人可能就沒有，確實是這樣，不過還是很期待看到這個歐洲法院在 2014 年 5 月 13 日做成的判決，對其他國家造成甚麼影響。在此之前，巴西只有 4 個與遺忘權及網路相關的案件，但判決做成後到現在，總共有 42 個案子，這就是各國相互啟發影響的實例。

5. 網際網路名稱與號碼指配組織(Internet Corporation for Assigned Names and Numbers, ICANN)政府參與部門主席資深顧問 Tarek Kamel 表示，此類會議應該儘量邀請各方利害關係人共同參與討論，現在問題的複雜度已經不是像 ICANN 在 5 年或 10 年前所處理的，而且對於各國也越來越重要，如果亞洲或非洲的國家不能參與，召開網際網路治理大會後各國仍自司其政的情況可能會再度產生，因此，ICANN 希望這個會議能得出結論，告訴 ICANN 該如何從旁協助，如果需要能力建構，全球應該團結合作。ICANN 願意提供既有的工作成果及經驗，協助儘快達成解決網域與管轄方面的問題。

6. 歐洲安全與合作組織(Organization for Security and Cooperation in Europe, OSCE)媒體自由代表處代表 Dunja Mijatovic 認為應該多聚焦於人權及言論自由，與會的人員為了確保網路安

全及自由開放齊聚一堂，網路上甚麼可以做甚麼不能做，大家都有共識，但是外面的世界就差很多，因此，大家必須逐步漸進。Dunja Mijatovic 表示許多政府的作為包括限制、封鎖或過濾都正在發生中。2016 年，政府對於網路的監控、過濾及封鎖的事件層出不窮。諸如此類的事情，對個人有何影響呢?又該如何讓政府停止以監控、監禁、威脅、騷擾等工具影響人們?我們同時也該設法讓全球 50%仍然無網路可使用的人有使用網路的機會。資訊、透明、開放等議題很重要，但是這些人性面議題的的討論也不能少，雖然有許多決議、指導綱領，聯合國、歐盟的許多國家口頭上也都說尊重，但是事實上，在那些國家仍有許多因為在網路上刊登文章而被監禁的人，因此如何讓那些國家願意自動去尊重網路上的人權才是最重要的。

（五）閉幕式

1. 巴西外交部科技司司長 Benedicto Fonseco Filho 提出 4 點，希望全體利害關係人可以共同努力。第 1 點，本次會議需要完成的是完成一份雖然無法得到所有利害關係團體的認同，但仍能夠執行的原則性文件，全球應該加強執法方面的國際合作，以維護網路安全及避免網路犯罪。討論的結果可以做為其他組織、團體或論壇所召開之治理會議的討論文件。這些原則包括在人權、保護網路提供者、不同利害關係人間如何合作等。第 2 點，多方利害關係人的討論應該儘可能邀集各類行為者，不僅在地域方面、議題方面、利益種類方面如此，也包括政府裡其他部門的參與。第 3 點，多方利害關係人的概念及如何適用，此次達成的共識，巴西仍然需要迎頭趕上，在每個過程都需要確保各方利害關係人參與，扮演該扮演的角色，承擔該承擔的責任，這意味著各個利害關係人都必須參與不同議題的討論，但是比重可以不同，例如在重要資源方面，政府的參與就可以減少，但在網路安全，打擊網路犯罪部分，政府就該扮演重要的角色。第 4 點，自律性規定在管轄權相關領域比較難實現，因此，可由政府間共同行動或者簽屬協定打擊網路犯罪，這就是歐洲理事會所採取的方式。
2. 印度國家法律大學資訊治理中心執行長 Chinmayi Arun 指出技術方面的討論，通常對於從

事人權方面工作的人會覺得很無聊，但是這些技術方面的討論對於未來會有極大的影響，因此，這個多方利害關係人的討論能讓政府得到單純從政府角度切入無法了解的議題，特別是在與未參加本次會議的政府機關交涉時，更可以提供為協助，I &J 創造的這個空間讓出席者可以為因為某種理由無法參加的政府發聲，譬如，歐洲發展出 資料保護法，這樣印度的人就可以要求訂定隱私保護法，因為顯然並非沒因為顯然並非沒有必要的。在這個會議中，大家可以各自表達不同利害關係人的看法，創造跨境衝擊的機會。希望未來能有更多類似會議的召開。

3. 新美國基金會(New American Foundation)數位權利評比計畫(Ranking Digital Rights)主任 Rebecca MacKinnon 表示，這次會議集結各類不同團體，希望 I & J 可以擔任這些不同團體會議間的締結組織，讓各會議間能夠一起合作。眼前的議題必須靠政府、私人企業及社會團體間的互動來解決。政府機關裡頭也有專門負責人權、國家行動方案或者是商業方面的專責機關，也應該要參加這類會議，因為國家行動方案也包括了經濟、貿易政策、網路等方面的內容，這些專責機關參與討論後所擬定的國家行動方案才能促使私人企業尊重人權。當資訊取得及內容限制之相關議題未以尊重人權之方式處理，將導致全球社會團體空間的壓縮，社會團體就無法發聲，無法參與這種國際性辯論。因此，一定要與人權連結，並且引入非政府、非公司組織的參與。

4. 微軟技術政策部資深處長 Paul Mitchell 認為人權在網路上亦有適用，立論基礎為人權宣言。大家也認知該文件沒有統一的解釋。雖然大家都認為言論自由在美國及歐洲都是基本價值，但是歐洲人權宣言第 11 條與美國第一修正案則有相當出入。因此，如何體認此等不同觀點但同時支持這些不同觀點，減少這些不同觀點濫用，讓網路能夠繼續發展就成為一個難題。微軟在全世界有超過 10 億客戶、數百個資料中心並且在 222 個國家營業，微軟希望能夠協助每個人、每個組織去成就大事業，但是倘如沒有隨處可操作的合理、一致且易懂之有效行為準則、依據正當法律程序訂定之程序準則以及適當防護措施，微軟將無法完成這項任務。這種跨境的討論能夠協助大家了解有何不足之處。但是，現在已經到了該對找出的問題採取實際行動的時候了。我們應該了解及接受不同利害關係人

的目標，嘗試在異中求同。昨天在參加內容及管轄權分組討論裡，聽到從程序及價值間擺盪的討論，結論是必須依據價值觀，而不同利害關係人的有著不同的價值觀。Paul Mitchell 建議為了大家討論方便，應該先發展出共通的語言。另一個建議是公私部門開始共同擬定內容刪除的程序，方便雲端服務提供者使用，在跨境資料取得方面也可以這樣適用。相信再加上其他的補充研究，就可以從理論性討論邁向具體可見的解決方案前進，讓管理資訊及處理資料是否揭露的主體有程序可以遵循。

5. 歐洲執行委員會資訊社會暨媒體總署首席顧問 Megan Richards 認為管轄權是個網路上很大的問題，因為上每個網路使用都是跨境，可能是跨好幾個國家，單純只在國內的反而真的是少數，因此這些問題的討論，對所有網路使用者而言，均相當重要。但首先要在術語、透明化等方面尋得解決途徑，因為應由同樣術語才能避免誤會。另外一個議題是 ICANN 應該如何找出與網域名稱相關的特定議題。ICANN 的會議提供討論如何確保網域名稱系統平穩安全議題的絕佳機會，這也是 ICANN 成立的目的之一。本次的會議則是由不同利害關係人從不同角度出發來進行討論，在歐盟有些關於基本原則的法律與命令，但是也必須透過各國法律原則及其他法律來執行。在數位單一市場，歐洲執行委員會希望在不須處理 28 個會員國間不同法律的情況下，仍能確保數位及國內市場能夠在網路上順利運作。假使大家能夠在事實、訊息及標準基礎上共同努力，清楚使用的術語所代表的意思，那就是很大的進步了。

6. 美國商業部資訊通信助理部長 Lawrence Strickling 表示問題在於如何執行的方式然後開始執行，與會人員都認為這是個很迫切的議題，但是大家是否已經準備好要開始當個行動者了?過去 2 年來，ICANN 透過多方利害關係人程序已經成功轉型。假如美國在 2014 年就告訴參與 ICANN 程序的班底這個轉型需耗時 2 年，且必須寫很多電郵，開上千個小時的會議，大家一定都會認為做不到，但是最後他們做到了。Lawrence Strickling 並提出建議 3 點，第 1 點是，各位必須要善用多方利害關係人的會議，讓更多人參與討論，程序也必須透明，才能就解決途徑取得共識。第 2 點，此類會議需要資源，也許就像剛剛說的 ICANN 可以在網域名稱方面資助，不管耗費多少金錢，都必須要完成任務。第 3 點，

合法性必須透過公開、透明、共識及多方利害關係人參與取得。發展出的解決途徑可以與有意願的政府合作，先試行, 將想法落實為可執行之的策略。

7. 法國外交部政治事務與安全總署署長 Nicolas De Riviere 表示法國一向認為網路是世界公共財，但是網路又是一個根據各國不同法制而轉換的國際網絡，因而產生安全、人權及經濟成長等層面的問題。國家的管轄權如何適用於跨境網路上，對於所有政府、業界、技術提供者及社會團體都是種挑戰。解決網路管轄問題是發展數位社會的關鍵，數位社會也應該要尊重人權、推動革新並確保值得信賴的環境。召開這種多方利害關係人的會議是在公部門與網路平臺之私部門發展出適當之跨國合作架構的方式。法國政府一向致力於網路安全維護。其他國家警察、法官如何迅速取得網路使用者資料，這是法國巴黎大爆炸後，法國最重視的問題。另外，如何確保骯髒的內容、國人被砍頭的影像在法國無法點閱，又如何確定法國可以與持有那些內容的平臺合作?司法互助制度必須重新被檢核，因為司法互助制度無法處理網路犯罪之案件偵辦，也無法使政府迅速採取行動。就這些議題，許多主要的網路平臺已經開始進行對話。Nicolas De Riviere 也表示歡迎提出新的司法互助方式。但是傳統方式也不能拋棄，希望有越來越來政府能夠受惠於網路犯罪公約，根據該公約之原則訂定程序。社會團體的擔心是必然的，但是如果所採取的行動不被質疑就必須保障人權及透明化，最重要的是會議討論的結果必須要能付諸實行。政府與私人企業間必須在國際及區域的架構下合作。

參、心得與建議

本次參加全球網路及管轄權研討會，透由分組結論，分享各國對於網路社會下司法互助、人權、網路安全等之經驗分享，謹臚列心得及建議如下：

1. 本次會議由網路及管轄權組織主辦，主要由來自美、法等國之人員及公司組織成員約 200 餘人參加，大會提供各參與成員良好溝通舞台，並透由三個分組之熱烈討論廣泛蒐集意見。其中資訊與管轄權分組之結論，認為網路社會下之司法管轄權的挑戰在於「資料自由流通」(free flow of data)與「合法取得權」(lawful access requirements)等兩議題，對於如何建立可行

(viable)流程與防衛措施(safe guard)架構，有初步之討論。

2. 會議場地設於法國外交部，進出會場需憑證件並通過安全檢查，議程安排緊湊、分組討論場地安排則於事前報名時排定座位，故未發生混亂之情形。雖非官方主辦之會議，惟於維護會場及與會人員安全及議程場地之選定，均展現主辦單位之用心。

3. 網路社會下之司法管轄權已為重要的議題，本次會議後，主辦單位則續於 105 年 12 月 6-9 日在墨西哥辦理相關會議，由此可見該議題受重視之程度，面對此一新興議題，我國有必要持續觀注網路司法合作等議題之內容。

4. 富比士雜誌(Forbes)專欄作家 Ralph Jennings 在 2016 年 12 月 28 日撰文指出臺灣人民不關心國際事務主要是由於邊緣化的結果，因為國家前景無法預料，因此選擇拒絕談論國際展望，只追求小確幸(little comforts)。參加這次會議才發現即便是在臺灣從事國際事務的我們，對於國際上正在發生甚麼仍有待加強，因為，之所以參加此次會議是因為在服務貿易協定(Trade in Services Agreement, TiSA)談判及跨太平洋伙伴協定(Trans-Pacific Partnership, TPP)條文中均處理電子商務設施不落地（Localization of the Facilities）的議題，由於法務部國際及兩岸法律司主要業務是司法互助，加上在設施不落地的情況下，網路上犯罪相關資訊如何取得一直是我們的疑慮，但是我們一直找不答案。參加這次會議才發現，原來全球已經至少在 5 年前就已經開始在討論網路犯罪資料取得、人權保障及服務提供者商業發展間如何取得平衡。

5. 這個會議與一般臺灣能參加的國際會議比較不同的是大部分採取討論方式，而非一個主題各自發表文章然後接受提問，參加的人員包括政府、組織、網路服務提供者、社會人權團體等，就如何解決這項影響全世界的問題進行開放討論，有辯論、有妥協，透過這種討論方式達到共識，對照臺灣自己舉辦經常淪為大拜拜的所謂國際會議，有著天壤之別，將來本部在舉辦國際會議時，或可採取這種模式。

6. 臺灣與美國既簽有臺美刑事司法互助協定，且每年均進行諮商，或許可就此與美國諮商，比照美國與英國的方式簽署此類雙邊協定，且由於微軟、Google、臉書、推特等大型網路服務提供者在美國均有設立公司，當這些公司與美國或歐盟其他政府協調出請求的統一格式時，

我國也可透過與美國諮商，取得該格式，加速網路犯罪資料之取得。

肆、附件

一、議程

DAY 1 MONDAY, NOVEMBER 14

12:30–14:00 Registration and Networking

14:00–14:45

OPENING SESSION
Jurisdiction and the Future of the Cross-border Internet: An Issue of Common Concern for All Stakeholders

- **CARL BILDT** Former Swedish Prime Minister and Chairman, Global Commission on Internet Governance
- **DOUGLAS FRANTZ** Deputy Secretary-General, OECD
- **FRANK LA RUE** Assistant Director-General for Communication and Information, UNESCO
- **NICKLAS LUNDBLAD** Vice President, Head of Public Policy and Government Relations for EMEA, Google
- **NNENNA NWAKANMA** Africa Regional Coordinator, World Wide Web Foundation

14:45–16:00

STAKEHOLDER PLENARY
The State of Jurisdiction on the Internet (Part I)

This plenary session, held in two parts, will assess the increasing tensions around the world between national jurisdictions and the cross-border nature of the Internet. Given the potential negative impact on human rights, the global digital economy, and cybersecurity, a particular focus will be: What are the social, political, and economic costs of inaction for the global community?

Discussants include

- **MARIA INES BAQUE** Secretary of Public Management and Innovation, Ministry of Modernization, Argentina
- **THOMAS FITSCHEN** Director of International Cyber Policy, Federal Foreign Office, Germany
- **BRAD MARDEN** Assistant Director, Digital Crime Investigative Support, INTERPOL
- **CORYNNE MCSHERRY** Legal Director, Electronic Frontier Foundation
- **PAUL NEMITZ** Director, Fundamental Rights and Citizenship, DG JUSTICE, European Commission
- **CHRISTOPHER PAINTER** Coordinator for Cyber Issues, US Department of State
- **NII QUAYNOR** Chairman, Ghana National Information Technology Agency
- **ELVANA THACI** Head of Internet Standard-setting Unit, Council of Europe

16:00–16:30 Break

16:30–18:30

STAKEHOLDER PLENARY
The State of Jurisdiction on the Internet (Part II)

18:30–21:30 Dinner Reception

DAY 2 TUESDAY, NOVEMBER 15

The parallel Workstreams will follow an identical structure, as described below:

8:30–9:00	Morning Coffee
9:00–10:00	**Key Issues and Current Approaches** (in Workstreams) Introductory interventions will present the main aspects of the problem under discussion and major initiatives currently underway to address it.
10:00–11:00	**Operational Challenges – Part I** (in Workstreams) An open, moderated discussion in each Workstream will allow stakeholders to pinpoint specific operational challenges and explore efforts necessary to overcome them.
11:00–11:30	Break
11:30–12:30	**Operational Challenges – Part II** (in Workstreams)
12:30–14:00	Lunch (Plenary Room)
14:00–15:00	**STAKEHOLDER PLENARY** **The Future of Territoriality** (Plenary Room) Stakeholders will discuss together how the issue of territoriality is reflected in each workstream. What do traditional concepts of territoriality mean for the future of the cross-border Internet?
15:00–16:30	**Cooperation Areas** (in Workstreams) On the basis of the input papers and earlier discussions, stakeholders will identify a short list of specific areas that require more cooperation.
16:30–17:00	Break
17:00–18:30	**Priorities and Timelines** (in Workstreams) Surveys wil be conducted in each Workstream to identify common priorities for joint action. Possible modalities and timelines will be discussed, including the role that the multistakeholder policy network Internet & Jurisdiction could play moving forward.
18:30–21:00	Dinner Reception

DAY 3 WEDNESDAY, NOVEMBER 16

8:30–9:00 Morning Coffee

9:00–9:45

STAKEHOLDER PLENARY
Three Workstreams Report Back

Rapporteurs will present the outcomes of discussions in the three Workstreams and potential areas for cooperation and joint action.

9:45–11:00

STAKEHOLDER PLENARY
Taking Stock and the Way Forward (Part I)

Following the presentations by rapporteurs, participants will provide their feedback on priorities and modalities for joint action. The focus will be on ensuring coherence across policy sectors, promoting legal interoperability, and establishing due process across borders.

Discussants include

- **CARLOS AFFONSO SOUZA** Director, Institute for Technology and Society (ITS Rio)
- **ERIN DORGAN** Director, International Telecommunications Policy and Coordination, Department of Innovation, Science and Economic Development, Canada
- **ELFA YR GYLFADOTTIR** Director, Media Commission, Ministry of Communications, Iceland
- **GIANFRANCO INCARNATO** Deputy Director General for Political Affairs and Security, Ministry of Foreign Affairs and International Cooperation, Italy
- **TAREK KAMEL** Senior Advisor to the President for Government Engagement, ICANN
- **DUNJA MIJATOVIC** Representative on Freedom of the Media, OSCE

11:00–11:30 Break

11:30–12:15

STAKEHOLDER PLENARY
Taking Stock and the Way Forward (Part II)

12:15–13:00

CLOSING SESSION

Shared cooperation frameworks and policy standards as transnational as the Internet itself are necessary. How can ongoing multistakeholder dialogue be fostered to build trust and catalyze their development?

- **CHINMAYI ARUN** Executive Director, Centre for Communication Governance, National Law University Delhi
- **BENEDICTO FONSECA FILHO** Director, Department of Scientific and Technological Affairs, Ministry of Foreign Affairs, Brazil
- **REBECCA MACKINNON** Director, Ranking Digital Rights, New America Foundation
- **PAUL MITCHELL** Senior Director, Tech Policy, Microsoft
- **MEGAN RICHARDS** Principal Adviser, DG CONNECT, European Commission
- **NICOLAS DE RIVIERE** Director General for Political Affairs and Security, French Ministry of Foreign Affairs
- **LAWRENCE STRICKLING** Assistant Secretary for Communications and Information, US Department of Commerce

二、與會人員名單

Registered Participants of the Global Internet and Jurisdiction Conference

- .au Domain Administration Ltd (auDA)
  Lujia Chen
  Registrar Liaison Officer
  Australia
- Access Now
  Wafa Ben Hassine
  MENA Policy Analyst
  Tunisia
- African Union Commission
  Moctar Yedaly
  Head, Information Society Division
  Ethiopia
- Albright Stonebridge Group
  Nicole Wong
  Senior Advisor
  USA
- Alexander von Humboldt Institute for Internet and Society (HIIG)
  Wolfgang Schulz
  Professor
  Germany
- Amazon Web Services
  Stéphane Ducable
  Head of Public Policy EMEA
  USA
- American Registry for Internet Numbers (ARIN)
  John Curran
  President and CEO
  USA
- American University Washington College of Law
  Jennifer Daskal
  Associate Professor
  USA

- Amnesty International
  Rafendi Djamin
  Director, South East Asia and Pacific
  Thailand
- AndCo Law
  Pierre Landy
  Co-founder
  France
- Apple
  Jane Horvath
  Senior Director, Global Privacy
  USA
- Apple
  Lisa Pearlman
  Senior Manager of International Policy and Government Affairs
  USA
- Argentina, Ministry of Modernization
  Maria Ines Baqué
  Secretary of Public Management and Innovation
  Argentina
- Argentine Chamber of Internet (CABASE)
  Alejandro Amendolara
  Legal Advisor
  Argentina
- Argentine Chamber of Internet (CABASE)
  Esteban Lescano
  Head of Legal and Public Policy Affairs
  Argentina
- Article 19
  Avani Singh
  Senior Legal Officer
  South Africa
- Association of the Internet Industry (ECO)
  Michael Rotert

Chairman
Germany

- AT&T
  Claudia Selli
  European Government Affairs Director
  Belgium
- AXA
  Caroline Baylon
  Information Security Research Lead
  United Kingdom
- AXA
  Mathieu Cousin
  Security Research Analyst
  United Kingdom
- Blacknight Internet Solutions
  Michele Neylon
  CEO
  Ireland
- Bond University
  Dan Svantesson
  Professor
  Australia
- Brasilia Institute for Public Law (CEDIS/IDP)
  Sergio Alves
  Research Coordinator, Centre for Law, Internet & Society
  Brazil
- Brazil, Federal Prosecutor's Office of the State of São Paulo
  Melissa Blagitz
  Federal Prosecutor
  Brazil
- Brazil, Federal Prosecutor's Office of the State of São Paulo
  Fernanda Teixeira Souza Domingos
  Federal Prosecutor
  Brazil

- Brazil, Ministry of Foreign Affairs
  Benedicto Fonseca Filho
  Director, Department of Scientific and Technological Affairs
  Brazil
- Brazilian Internet Steering Committee (CGI.br)
  Luiz Fernando Martins Castro
  Councillor
  Brazil
- Brazilian Internet Steering Committee (CGI.br)
  Flávia Lefèvre Guimarãaes
  Board Member
  Brazil
- Brazilian Internet Steering Committee (CGI.br)
  Diego Rafael Canabarro
  Advisor to the Executive Secretariat
  Brazil
- BT Group
  Jane Frances Hill
  Chief Counsel Security, Privacy and Internet
  United Kingdom
- Canada, Department of Innovation, Science and Economic Development
  Erin Dorgan
  Director, International Telecommunications Policy and Coordination
  Canada
- Canada, Permanent Mission to the United Nations
  Chrystiane Roy
  First Secretary, Cybersecurity and Internet Governance
  Canada
- Castex Chair of Cyber Strategy
  Alix Desforges
  Researcher
  France
- Castex Chair of Cyber Strategy
  Frédérick Douzet

Chairwoman
France

- Center for Democracy & Technology (CDT)
  Greg Nojeim
  Senior Counsel and Director, Freedom, Security and Technology Project
  USA
- Centre for International Governance Innovation (CIGI)
  Bassem Awad
  Deputy Director, International Intellectual Property Law and Innovation
  Canada
- Centre for International Governance Innovation (CIGI)
  Eileen Donahoe
  Distinguished Fellow
  USA
- Centre for International Governance Innovation (CIGI)
  Sam Anissimov
  Junior In-House Counsel
  Canada
- Centre for International Governance Innovation (CIGI)
  Oonagh Fitzgerald
  Director, International Law Research Program
  Canada
- Centre for Internet and Society
  Elonnai Hickok
  Director, Internet Governance
  India
- CloudFlare
  Michael Nelson
  Public Policy
  USA
- Columbia University, Global Freedom of Expression Project
  Agnes Callamard
  Director
  USA

- Council of Europe
  Elvana Thaci
  Administrator, Information Society Division
  France
- Council of European National Top-Level Domain Registries (CENTR)
  Peter Van Roste
  General Manager
  Belgium
- Council of European National Top-Level Domain Registries (CENTR)
  Nina Elzer
  Policy Adviser
  Belgium
- Council of the European Union
  Monika Kopcheva
  Policy Officer
  Belgium
- Dailymotion
  Clément Reix
  Project Manager, Public Affairs
  France
- Derechos Digitales
  Juan Carlos Lara
  Research and Policy Director
  Chile
- Digital Age Defense
  Cathy Gellis
  Attorney
  USA
- Diplo Foundation
  Marilia Maciel
  Digital Policy Senior Researcher
  France
- Dropbox
  Gazala Haq

Head of Public Policy and Government Affairs, EMEA
United Kingdom

- Dutch National Police Agency
  Hessel Schut
  Strategic Digital Expert, National High Tech Crime Unit
  The Netherlands
- eBay
  Hanne Melin Olbe
  Director, Global Public Policy
  Switzerland
- The Economist
  Ludwig Siegele
  Technology Editor
  United Kingdom
- Electronic Frontier Foundation (EFF)
  Corynne McSherry
  Legal Director
  USA
- Electronic Privacy Information Center
  Marc Rotenberg
  President and Executive Director
  USA
- Estonia, Ministry of Foreign Affairs
  Piret Urb
  First Secretary, International Organisations Division
  Estonia
- European Commission, Directorate General for Communications Networks, Content & Technology (DG CONNECT)
  Megan Richards
  Principal Advisor
  Belgium
- European Commission, Directorate General for Justice and Consumers (DG JUST)
  David Friggieri
  Coordinator on combating anti-Muslim hatred

Belgium

- European Commission, Directorate General for Justice and Consumers (DG JUST)
  Paul Nemitz
  Director, Fundamental Rights and Citizenship
  Belgium
- European Commission, Directorate General for Justice and Consumers (DG JUST)
  Titus Poenaru
  Policy Officer
  Belgium
- European Commission, Directorate General for Migration and Home Affairs (DG HOME)
  Cathrin Bauer-Bulst
  Deputy Head of Unit, Fight Against Cybercrime
  Belgium
- European Parliament
  Marietje Schaake
  Member of the European Parliament
  The Netherlands
- European Registry of Internet Domain Names (EURid)
  Geo Van Langenhove
  Legal Manager
  Belgium
- European Telecommunications Network Operators' Association (ETNO)
  Lise Fuhr
  Director General
  Belgium
- European Telecommunications Network Operators' Association (ETNO)
  Natalia Vicente
  Public and Regulatory Affairs Officer
  Belgium
- European Union, European Data Protection Supervisor (EDPS)
  Jacob Kornbeck
  Legal Officer
  Belgium

- European Union, European Data Protection Supervisor (EDPS)
  Romain Robert
  Legal Counsel
  Belgium
- European Union, European Data Protection Supervisor (EDPS)
  Wojciech Wiewiórowski
  Assistant European Data Protection Supervisor
  Belgium
- Europol
  Philipp Amann
  Head of Strategy, European Cybercrime Centre (EC3)
  The Netherlands
- Facebook
  Anton'Maria Battesti
  Public Policy Manager
  France
- Facebook
  Matt Perault
  Head, Global Policy Development
  USA
- Fenwick & West LLP
  Andrew Bridges
  Partner
  USA
- Financial Times
  Greg Callu
  Ombudsman
  United Kingdom
- Finland, Ministry of Foreign Affairs
  Pia Rantala-Engberg
  Ambassador, Cyber Affairs
  Finland
- Finland, Ministry of Foreign Affairs
  Juuso Moisander

Commercial Secretary
Finland

- Foundation for Internet Domain Registration Netherlands (SIDN)
  Maarten Simon
  Senior Legal and Policy Advisor
  The Netherlands
- France, Ministry of Culture and Communication
  Joanna Chansel
  Deputy Head, EU & International Affairs
  France
- France, Ministry of Economy and Finance
  Ghislain de Salins
  Senior Advisor, Global Internet Policy
  France
- France, Ministry of Foreign Affairs
  Najma Bichara
  Digital, Regulatory Affairs
  France
- France, Ministry of Foreign Affairs
  Nicolas de Rivière
  Director General for Political Affairs and Security
  France
- France, Ministry of Foreign Affairs
  David Martinon
  Ambassador for Cyberdiplomacy and the Digital Economy
  France
- France, Ministry of Interior
  Eric Freyssinet
  Advisor to the Prefect in Charge of the Fight Against Cyberthreats
  France
- France, National Cyber Crime Investigation Unit (OCLCTIC)
  Catherine Chambon
  Joint Director
  France

- Frankfurt University
  Matthias Kettemann
  Post-Doctoral Fellow
  Germany
- French Institute for Research in Computer Science and Automation (INRIA)
  Jean-François Abramatic
  Joint Director, Transfers and Industrial Partnerships
  France
- French Network Information Centre (AFNIC)
  Mathieu Weill
  General Director
  France
- Fundação Getulio Vargas Law School
  Luca BelliSenior
  Researcher
  Brazil
- Galway Strategy Group
  Jim Prendergast
  President
  USA
- Georgia Institute of Technology, Scheller College of Business
  Peter Swire
  Professor
  USA
- Germany, Federal Government Commissioner for Culture and Media
  Oliver Schenk
  Legal Advisor, International Media
  Germany
- Germany, Federal Foreign Office
  Thomas Fitschen
  Ambassador and Director of International Cyber Policy
  Germany
- Germany, Federal Ministry for Economic Affairs and Energy
  Frank Goebbels

Head of Unit, European Digital Policy
Germany

- Ghana, National Information Technology Agency
  Nii Quaynor
  Chairman
  Ghana
- Global Commission on Internet Governance
  Carl Bildt
  Chairman
  Sweden
- Global Compass
  Jean-Christophe Bas
  CEO
  France
- Global Network Initiative (GNI)
  Judith Lichtenberg
  Executive Director
  USA
- Global Partners Digital
  Charles Bradley
  Executive Director
  United Kingdom
- Global Partners Digital
  Lea Kaspar
  Executive Director
  United Kingdom
- Google
  Benjamin du Chaffaut
  Senior Legal Counsel, Head of Litigation
  France
- Google
  Thibault Guiroy
  Public Policy Manager
  France

- Google
  Nicole Jones
  Senior Counsel, Law Enforcement and Security
  USA
- Google
  Nicklas Lundblad
  Vice President, Public Policy and Government Relations EMEA
  Sweden
- Harvard University, Berkman Center for Internet & Society
  Urs Gasser
  Executive Director
  USA
- Holland & Knight LLP
  Charles D. Tobin
  Partner
  USA
- Iceland, Ministry of Communications
  Elfa Yr Gylfadottir
  Director, Media Commission
  Iceland
- ict Development Associates
  David Souter
  Managing Director
  United Kingdom
- India, Data Security Council (DSCI)
  Rama Vedashree
  CEO
  India
- India, Ministry of Electronics and Information Technology
  Aruna Sundararajan
  Secretary
  India
- Infoblox
  Rod Rasmussen

Vice President of CyberSecurity
USA

- Institute for Technology and Society (ITS Rio)
  Carlos Affonso Souza
  Director
  Brazil
- Inter-American Association of Telecommunications Companies (ASIET)
  Juan Jung
  Director, Public Policy
  Uruguay
- Inter-American Association of Telecommunications Companies (ASIET)
  Pablo Bello
  Executive Director
  Uruguay
- International Bar Association
  Alexandra Neri
  Vice-chair, Intellectual Property and Entertainment Law Committee
  France
- International Chamber of Commerce
  Elizabeth Thomas-Raynaud
  Senior Policy Executive, Digital Economy Commission
  France
- International Chamber of Commerce
  Sophie Tomlinson
  Assistant Policy Manager
  France
- International Organisation of La Francophonie
  Emmanuel Adjovi
  Program Manager, Information Society
  France
- INTERNETLAB
  Jacqueline de Souza Abreu
  Project Lead
  Brazil

- Internet Corporation for Assigned Names and Numbers (ICANN)
  Rinalia Abdul Rahim
  Board Member
  Malaysia
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Fabien Betremieux
  GAC Relations Advisor
  France
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Maarten Botterman
  Board Member
  The Netherlands
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Cherine Chalaby
  Board Member
  USA
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Olivier Crepin-Leblond
  Chair, EURALO
  United Kingdom
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Chris Disspain
  Board Member
  Australia
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Anne-Rachel InnéVice President, Global Engagement
  Switzerland
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Tarek Kamel
  Senior Advisor to the President for Government Engagement
  Egypt
- Internet Corporation for Assigned Names and Numbers (ICANN)
  Markus Kummer
  Board Member

Switzerland

- Internet Corporation for Assigned Names and Numbers (ICANN)
  Theresa Swineheart
  Senior Vice President, Multistakeholder Strategy and Strategic Initiatives
  USA
- Internet Democracy Project
  Anja Kovacs
  Director
  India
- Internet Infrastructure Coalition
  David Snead
  Board and Policy Chair
  USA
- The Internet Infrastructure Foundation (IIS)
  Elisabeth Ekstrand
  General Counsel and Chief Administrative Officer
  Sweden
- Internet Society (ISOC)
  Constance Bommelaer
  Senior Director, Global Internet Policy
  USA
- InternetNZ
  Jordan Carter
  Chief Executive
  New Zealand
- Interpol
  Brad Marden
  Assistant Director, Digital Crime Investigative Support
  Singapore
- Iptegrity
  Monica Horten
  Policy Analyst
  United Kingdom
- Ireland, Department of Justice and Equality

Davina Bracken
Deputy Head, Central Authority for Mutual Legal Assistance
Ireland

- iRights.info
  Matthias Spielkamp
  Managing Partner
  Germany
- Italy, Ministry of Foreign Affairs and International Cooperation
  Gianfranco Incarnato
  Deputy Director General for Political Affairs and Security
  Italy
- Jones Day
  Olivier Haas
  Counsel
  France
- Jones Day
  Evgenia Nosareva
  Associate
  France
- Latvia, Ministry of Foreign Affairs
  Janis Karklins
  Permanent Representative of Latvia to the United Nations Office
  Latvia
- LinkedIn
  Sara Harrington
  VP Legal for IP, Product and Privacy
  USA
- Mackenzie Presbyterian University
  Ana Cristina Carvalho
  Professor
  Brazil
- Mexico, Federal Telecommunications Institute
  Mario Fromow Rangel
  Commissioner

Mexico

- Mexico, Federal Telecommunications Institute
  José Guadalupe Rojas Ramírez
  Advisor and Coordinator to the Commissioner
  Mexico
- Microsoft
  Lani Cossette
  Director, EU Government Affairs
  Belgium
- Microsoft
  John Frank
  Vice President, EU Government Affairs
  Belgium
- Microsoft
  Mark Lange
  Director, EU Institutional Relations
  Belgium
- Microsoft
  Paul Mitchell
  Senior Director, Tech Policy
  USA
- Milathan
  Stéphane Van Gelder
  Managing Director
  United Kingdom
- Motion Picture Association
  Sarah Van Reempts
  Legal Counsel
  Belgium
- Mozilla
  Chris Riley
  Head, Public Policy
  USA
- National Law University, Delhi, Centre for Communication Governance

Chinmayi Arun
Executive Director
India

- NBC Universal
  Braxton Perkins
  Vice President, Creative Content Protection
  USA
- The Netherlands, Ministry of Economic Affairs
  Arnold van Rhijn
  Senior Policy Coordinator, Global Internet Governance
  The Netherlands
- The Netherlands, Ministry of Foreign Affairs
  Joost BunkPolicy
  Officer, Task Force International Cyber Policies
  The Netherlands
- The Netherlands, Ministry of Security and Justice
  Joost Raeven
  Senior policy advisor
  The Netherlands
- The Netherlands, Public Prosecution Service
  Martijn Egberts
  Prosecutor, Cyber Crimes
  The Netherlands
- New America Foundation
  Rebecca MacKinnon
  Director, Ranking Digital Rights
  USA
- New Partnership for Africa's Development (NEPAD)
  Towela Jere
  Principal Programme Officer
  South Africa
- Nominet
  Richard Plater
  Policy Executive

United Kingdom

- Olswang
  Jean-Frederic Gaultier
  Partner
  France
- The Open Net Association
  Igor Milashevskiy
  Director
  Russia
- Open Net Korea
  Kyung-Sin Park
  Co-founder
  Republic of Korea
- Oracle
  Joseph Alhadeff
  Vice President, Global Public Policy and Chief Privacy Strategist
  USA
- Organization for Economic Co-operation and Development (OECD)
  Janos Ferencz
  Trade Policy Analyst
  France
- Organization for Economic Co-operation and Development (OECD)
  Douglas Frantz
  Deputy Secretary-General
  France
- Organization for Economic Co-operation and Development (OECD)
  Jeremy West
  Senior Policy Analyst
  France
- Organization for Security and Cooperation in Europe (OSCE)
  Matthijs Berman
  Principal Advisor
  Austria
- Organization for Security and Cooperation in Europe (OSCE)

Dunja Mijatović
Representative on Freedom of the Media
Austria

- Organization for Security and Cooperation in Europe (OSCE)
  Frane Maroevic
  Director, Office of the OSCE Representative on Freedom of the Media
  Austria
- Packet Clearing House
  Bill Woodcock
  Executive Director
  USA
- PayPal
  Mathilde Bonneau
  Manager, Government Relations EMEA
  USA
- Poland, National Prosecutor's Office
  Janusz Grzyb
  Prosecutor
  Poland
- Poland, National Prosecutor's Office
  Tomasz Iwanowski
  Prosecutor
  Poland
- Portugal, Ministry of Science, Technology and Higher Education
  Ana Neves
  Director, Department of Information Society
  Portugal
- Portugal, Ministry of Science, Technology and Higher Education
  Charlotte Simões
  Policy Officer, Department of Information Society
  Portugal
- Privacy International
  Caroline Wilson Palow
  General Counsel

United Kingdom

- Public Interest Registry
  Elizabeth Finberg
  Vice President and General Counsel
  USA
- Quadrature du Net
  Agnès de Cornulier
  Legal and Policy Analysis Coordinator
  France
- Queen Mary University of London
  Ian Walden
  Professor
  United Kingdom
- Real Time Register
  Theo Geurts
  Compliance Officer
  The Netherlands
- Reliance Industries
  Raghu Raman
  President, Risk, Security and New Ventures
  India
- Reliance Industries
  Rajneesh Akhoury
  Senior Security Advisor
  India
- Reporting and Analysis Centre for Information Assurance (MELANI)
  Adrian Koster
  Analyst & Legal Advisor
  Switzerland
- Republic of Moldova, Ministry of Information Technology and Communications
  Andrei Cușca
  Deputy Head, Directorate for Information Technology Policies
  Republic of Moldova
- Rocket Internet

Gianluca Varisco
Vice President, Security
Germany

- Rouen University
  Aude Géry
  Researcher
  France
- SaferNet
  Thiago Tavares
  President
  Brazil
- Serbia, Ministry of Foreign Affairs
  Maja Rakovic
  First Counsellor
  Serbia
- Slovakia, Ministry of Justice
  Zuzana Stofova
  Head of Department, International Legal Cooperation
  Slovakia
- Society-University de San Andrés, Center of Technology
  Paula Vargas
  Professor
  Argentina
- Software Freedom Law Centre
  Mishi Choudhary
  Legal Director
  USA
- Spain, Ministry of Industry, Energy and Tourism
  Gema Campillos González
  Deputy Director, Information Society Services
  Spain
- Stanford University, Center for Internet and Society
  Daphne Keller
  Director, Intermediary Liability

USA

- Stanford University, Center for Internet and Society
  Giancarlo Frosio
  Intermediary Liability Fellow
  USA
- Supreme Court of India
  Malvika Kalra
  Lawyer
  India
- Sweden, Ministry of Enterprise, Energy and Communications
  Helena Strömbäck
  Deputy Director
  Sweden
- Sweden, Ministry of Enterprise, Energy and Communications
  Helene Ramqvist Engellau
  Deputy Director and Legal Advisor
  Sweden
- Switzerland, Federal Office of Communications (OFCOM)
  Frederic Riehl
  Ambassador, International Director
  Switzerland
- Switzerland, Federal Office of Communications (OFCOM)
  Thomas Schneider
  Deputy Director of International Affairs
  Switzerland
- Taiwan, Ministry of Justice
  Ti-na Li
  Section Chief
  Taiwan
- Taiwan, Ministry of Justice
  Mei-Shiou Lin
  Senior System Analyst
  Taiwan
- Telefonica

Andrea Fabra
Public Policy & Internet Manager
Spain

- Telefonica
  Christoph Steck
  Director, Public Policy and Internet
  Spain
- Telefonica
  Paloma Villa Mateos
  Manager, Public Policy and Internet
  Spain
- The Washington Post
  David Post
  Columnist
  USA
- Twitter
  Nick Pickles
  Head, UK Public Policy
  United Kingdom
- Twitter
  Elizabeth Banker
  Associate General Counsel
  USA
- UNINETT Norid
  Annebeth Lange
  Special Advisor, International Policy
  Norway
- United Kingdom, Department for Culture, Media and Sport
  Mark Carvell
  Senior Policy Adviser, Global Internet Governance
  United Kingdom
- United Kingdom, Foreign and Commonwealth Office
  Paul Gaskell
  Deputy Head, Intelligence Policy Department

United Kingdom

- United Kingdom, National Crime Agency
  Sarah Pritchard
  Deputy Legal Director
  United Kingdom
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  Sylvie Coudray
  Chief of Section, Communication and Information Sector
  France
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  Xianhong Hu
  Assistant Programme Specialist, Communications and Information
  France
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  Frank La Rue
  Assistant Director-General for Communication and Information
  France
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  Julie Miville-Dechene
  Representative of the Government of Quebec, Permanent Delegation of Canada
  Canada
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  Rachel Pollack Ichou
  Associate Programme Specialist, Communication and Information Sector
  France
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
  Dan Shefet
  Consultant
  France
- United Nations Interregional Crime and Justice Research Institute (UNICRI)
  Francesca Bosco
  Project Officer, Emerging Crimes Unit
  Italy
- University of California, Irvine School of Law

Adam Lhedmat
Researcher, Advisor to UN Special Rapporteur on Freedom of Expression
USA
Amos Toh
Legal Advisor to UN Special Rapporteur on Freedom of Expression
USA

- University of Geneva
  Jacques de Werra
  Professor and Vice Rector
  Switzerland
- University of Liège/KU Leuven
  Vanessa Franssen
  Assistant Professor
  Belgium
- University Paris II Pantheon Assas
  Suzanne Vergnolle
  PhD candidate
  France
- USA, Department of Commerce
  Lawrence Strickling
  Assistant Secretary for Communications and Information
  USA
- USA, Department of Commerce
  Fiona Alexander
  Associate Administrator, National Telecommunications and Information Administration (NTIA)
  USA
- USA, Department of Justice
  David Bitkower
  Principal Deputy Assistant Attorney General, Criminal Division
  USA
- USA, Department of Justice
  Aaron Cooper
  Counsel to Assistant Attorney General

USA

- USA, State Department
  Christopher Painter
  Coordinator for Cyber Issues
  USA
- US Embassy in Paris
  Dan Wald
  First Secretary, Economic Affairs
  USA
- VeriSign
  Keith Drazek
  Vice President, Public Policy and Government Relations
  USA
- VeriSign
  Patrick Kane
  Senior Vice President of Naming Services
  USA
- The Walt Disney Company
  Thomas Spiller
  Vice President, Global Public Policy
  Belgium
- WAN-IFRA
  Ilaria Fevola
  Project Assistant
  France
- WAN-IFRA
  Elena Perotti
  Executive Director, Public Affairs and Media Policy
  France
- Wikimedia Foundation
  Michelle Paulson
  Interim General Counsel and Legal Director
  USA
- Women’s Economic Empowerment Program

Valerie D’Costa
Senior Private Sector Development Specialist
USA

- World Wide Web Foundation
  Nnenna Nwakanma
  Africa Regional Coordinator
  Nigeria
- Yelp
  Kostas Rossoglou
  Head, EU Public Policy
  Belgium
- ZwillGen
  Aaron Altschuler
  Counsel
  USA

四、討論文件

WORKING DOCUMENT

MORE COOPERATION OR A LESS GLOBAL INTERNET

The cross-border nature of the Internet has generated unprecedented economic social and political benefits for humanity but tensions concerning the application of national laws on the global network are increasing. As connectivity and Internet penetration increase, so do conflicts between jurisdictions.

Twenty-first century digital realities challenge the Westphalian international system and traditional modes of legal cooperation. An extensive application of the territoriality criteria and uncoordinated actions by the various actors put the global community on a dangerous path. If nothing is done, the resulting legal arms race could lead to severe unintended and negative consequences for the future of the global digital economy, human rights, cybersecurity, and the technical infrastructure.

Preserving the global character of the Internet while ensuring the respect of the rule of law(s) demand innovative cooperation mechanisms as transnational as the network itself. Their development is the urgent joint responsibility of all actors: none of them can address this challenge on its own. There is however an institutional gap regarding governance "on" the Internet. It can only be solved by drawing lessons from the collaborative approach among all stakeholders adopted for the technical governance "of" the Internet.

LEGAL INTEROPERABILITY

International human rights provide overarching principles. It is now widely recognized that they apply online as

well as offline. Yet, substantive legal harmonization at a global level regarding the use of the Internet is unrealistic (and often not desirable) given the diversity of legislations and their strong connection to national identities. A procedural approach is therefore a more promising route to develop operational solutions to jurisdictional challenges and enable the coexistence of diverse norms in shared online spaces.

Common procedures establishing transnational due process could in particular structure the increasingly direct interactions between states, businesses and users across borders. Interfacing these heterogeneous actors like the TCP/IP protocol did for heterogeneous networks, multistakeholder "policy standards" would create the conditions for legal interoperability and have the capacity to progressively scale.

These innovative transnational cooperation frameworks, establishing mutual commitments between the different stakeholders, can enshrine existing best practices or set new, jointly developed principles, norms, rules, and decision-making procedures.

THREE WORKSTREAMS

Since 2012, the Internet & Jurisdiction Secretariat has facilitated dialogue on jurisdictional challenges among governments, major Internet platforms, technical operators, civil society, international organizations and academia. They collectively identified cross-border requests for access to user data, content takedowns, and domain suspensions as priority areas for the development of such transnational due process mechanisms. Building on this preparatory work, this first Global Internet and Jurisdiction Conference brings together about 200 senior participants to help move discussions towards operational solutions. In order to facilitate interactions, the Conference eschews formal panels in favor of direct interactions among participants. In particular, the second day will be organized in three parallel Workstreams, held under Chatham House Rule.

WORKSTREAM I: DATA & JURISDICTION

How can transnational data flows and the protection of privacy be reconciled with lawful access requirements to address abuses? Criminal investigations increasingly require access to information about users and digital evidence stored by private companies in jurisdictions outside the requesting country. The traditional Mutual Legal Assistance (MLA) system is under stress and competing approaches are proposed to solve this issue. What are the necessary safeguards and procedures to establish viable and scalable frameworks?

WORKSTREAM II: CONTENT & JURISDICTION

How can the global availability of content be handled given the diversity of local laws and norms? Content legal in one country can be illegal in another one. Protecting human rights and freedom of expression when dealing with hate speech, harassment, security threats, incitation to violence, and discrimination on the Internet is a major challenge when several jurisdictions are involved. How can current practices be improved in terms of transparency and due process

across borders?

WORKSTREAM III: DOMAINS & JURISDICTION

How can the neutrality of the Internet's technical layer be preserved when national jurisdictions are applied on the Domain Name System? Suspension of a domain name has a global impact and thus requires a high threshold of abuse in the content of the underlying site to justify it. There are however divergent views regarding the definition of the corresponding criteria and even where they should be discussed. What role can "trusted notifiers" play, and what kind of framework could define their responsibilities?

INPUT PAPERS

To help structure discussions, the following input papers were prepared by the Internet & Jurisdiction Secretariat. They present for each Workstream[1]: 1) the common problem stakeholders are facing; 2) the major approaches currently proposed; 3) operational challenges; and 4) possible areas for cooperation. This should help participants define priorities and timelines for joint action. Rapporteurs will record key elements of convergence. In the absence thereof, they will strive to register as accurately as possible the different perspectives on each issue.

This document is intended merely as input for participants and does not claim to be exhaustive. It presents an overview of key issues of common concern that emerged from the global dialogue process facilitated by Internet & Jurisdiction.

Comments or suggestions can be sent to gijc@internetjurisdiction.net

ABOUT THE INTERNET & JURISDICTION POLICY NETWORK

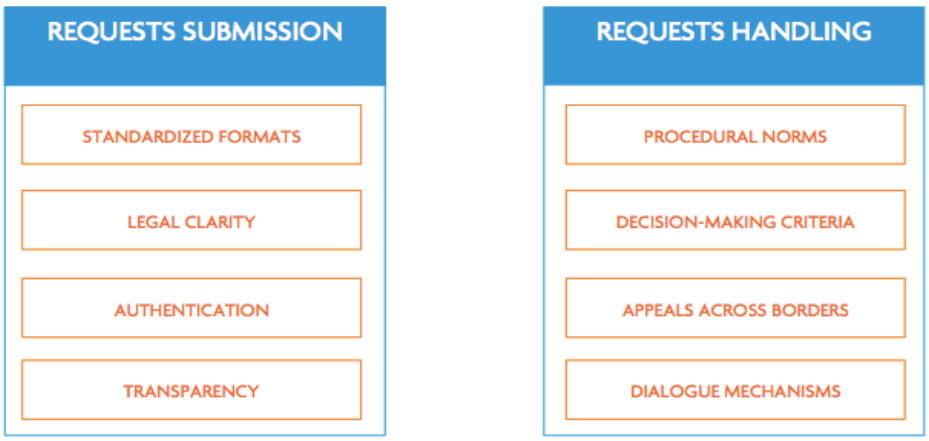
The 2016 Global Internet and Jurisdiction Conference builds on progress achieved within the global multistakeholder policy network Internet & Jurisdiction since 2012. The Internet & Jurisdiction policy network uniquely bridges relevant stakeholder groups and policy silos in order to enable transnational cooperation. Internet & Jurisdiction strives to fill the institutional gap in Internet governance at the intersection of four policy silos: legal cooperation, digital economy, human rights, and cybersecurity. Through global, regional, and thematic meetings, Internet & Jurisdiction facilitates a neutral dialogue process to build trust among the different actors and help them develop the operational solutions necessary for the coexistence of diverse laws on the cross-border Internet.

ADDITIONAL RESOURCES

The I&J Retrospect Database: To enable evidence-based policy innovation, Internet & Jurisdiction documents cases that show the increasing tension between the cross-border nature of the Internet and national jurisdictions around the world. With the help of the 30 leading academic experts of the I&J Observatory, more than 1.000 such cases have been collected since 2012. They now can be consulted in the open-access I&J Retrospect Database at: http://www.internetjurisdiction.net/publications/retrospect

The I& J Paper "Jurisdiction on the Internet – From legal arms race to transnational cooperation" (April 2016) is available at http://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the- Internet.pdf.

Transnational due process. Four years of international multistakeholder discussions within the Internet & Jurisdiction policy network helped identify key elements of transnational due process. The resulting "Transnational Due Process Architecture" for cross-border requests addresses two aspects: how requests are submitted and how requests are handled.



The eight components above provide a structure for defining best practices and improving existing mechanisms, as well as a potential architecture for novel cooperation frameworks. This serves as a general framework for discussions, and specific questions are detailed in the respective chapters of each Workstream.

GLOBAL INTERNET AND JURISDICTION CONFERENCE 2016
NOVEMBER 14-16, 2016 · PARIS, FRANCE

WORKSTREAM I:

CROSS-BORDER ACCESS TO USER DATA

1.1 THE COMMON PROBLEM

Within each country, law enforcement investigations are conducted according to strict national procedures for access to and use of evidence. To avoid abusive access, different national safeguards exist to reconcile the protection of citizens' rights and privacy, with the necessary restrictions thereof to address illegal activities. The digitization of societies and the cross-border nature of the Internet directly impact this traditional legal landscape, introducing a strong transborder dimension.

- Instead of physical documents or objects, evidence is increasingly in the form of digital data regarding the identity of Internet users and their activity online.
- Potential evidence is collected and stored by a broad diversity of private companies (many based in the US) rather than located in the physical property of the investigated person.
- The amount and diversity of the collected data is growing exponentially, especially since the development of mobile apps, and even in the absence of data retention obligations.
- Access to digital evidence is important not only for online crime but also most if not all investigations regarding illegal activities in the physical space.
- Private companies are frequently incorporated or storing their information outside of the country conducting the investigation.
- The nexus of connection of the investigated crime with a foreign country can be limited to the use of such services.
- The development of cloud services makes the actual location of data more uncertain, while the lack of working solutions can increase calls for data localization.

In light of this increasingly transnational dimension of investigations, the two main mechanisms presently employed for cross-border access to user data present significant limitations.

MLATs. International legal cooperation is traditionally handled through Mutual Legal Assistance Treaties (MLATs). However, these were initially designed to handle relatively rare cases and the MLAT system therefore struggles to adapt to the massive evolutions described above. Generally regarded as slow and complex, it needs reform and some efforts are under way in that regard. Yet, even an improved MLAT system is hardly scalable to all countries, and moreover imposes the law of the recipient country even when the case at hand has no connection to it. Frustration with this system encourages states to use national production orders based on the

mere provision of services to users in their country, or impose compulsory data localization requirements, both of which present challenges of their own if generalized around the world.

Voluntary cooperation. Requests for access to user data are increasingly sent directly by law enforcement in one country to Internet intermediaries in another to solicit voluntary cooperation. The number of such requests increased by 40% between 2014 and 2015.[2] In the US, the Electronic Communications Privacy Act (ECPA) allows voluntary communication of basic subscriber identification (BSI) and traffic data by private companies to law enforcement. Most companies mention their right to do so in their Terms of Service. However, content data still needs to be obtained through MLAT in application of the Stored Communications Act (SCA). In this context, determining the validity of a request increasingly becomes the responsibility of private entities, tasked with evaluating the applicability of a patchwork of national laws and procedures without a clear and transparent reference framework. Moreover, conflicting legislations regarding conditions for voluntary transborder cooperation can place companies in a dilemma when complying with the law of one country implies breaking the law in another.

Workstream I is dedicated to exploring in more detail the voluntary cooperation approach and its possible improvements. All stakeholders face the common challenge of reconciling several competing objectives. Their joint responsibility could be described as: *Developing policy standards respecting privacy and due process in order to define the conditions under which authorized law enforcement authorities can request from foreign companies access to stored user data necessary for lawful investigations*.

1.2 CURRENT APPROACHES

Discussions are under way in the US and in Europe to improve cross-border access to user data, with significantly different yet potentially complementary approaches regarding access to content and non- content user data (see links in Section 1.5 for more details):

- US Working Group (see Daskal-Woods references in Section 1.5). Since the end of 2015, a possible regime for cross-border access to user content data has been explored by an informal group of US-based actors from academia, civil society, and key Internet platforms, with the US government (including the Department of Justice) as observer. It would apply when the only nexus of connection with the US is the use of a US-based service provider, i.e. if the "*requesting government has jurisdiction over both the target and the relevant criminal activity*." The target should not be a US citizen or located in the United States. In such cases, an exception to ECPA and SCA would allow companies to voluntarily disclose user content data (not only basic subscriber information or traffic data) to foreign law enforcement, under specific conditions and with pre-defined procedures and safeguards.

- UK-US draft bilateral agreement. Discussions are currently underway between the UK and the US concerning a bilateral agreement for reciprocal cross-border access to data. The agreement would allow law enforcement and security authorities with lawful local warrants to request data directly from communication services providers in the other country more quickly and simply than through MLATs. Similar agreements could be progressively established with other countries. A proposed bill (see link in Section 1.5) has been presented in the US Congress to enable this mechanism. Meanwhile, a recent decision by the US Second Circuit Court of Appeals in the case regarding US access to data stored in Microsoft's Irish servers directly impacts these discussions, as it can significantly reduce the capacity of US authorities to access data stored overseas by US companies.
- European Union. On March 7-8, 2016, the Dutch Presidency of the European Union convened the conference "Crossing borders: Jurisdiction in Cyberspace" in Amsterdam. Participants explored these issues in detail and highlighted the importance of access to basic subscriber information. The conference conclusions fed into the meeting of the European Council of Ministers for Justice and Home Affairs on June 9-10, 2016. The resulting Conclusions of the Council tasked the European Commission to "*develop a common framework for cooperation with service providers for the purpose of obtaining specific categories of data, in particular subscriber data*" which would set "*commonly agreed requirements.*" The Commission was also tasked with engaging service providers "*to explore… the possibility of using aligned forms and tools*" such as "*a secure online portal for electronic requests and responses.*"
- Council of Europe. Home of the 2001 Convention on Cybercrime, the Council of Europe has devoted significant efforts to this issue within its T-CY Committee, in particular its Cloud Evidence Group, which issued its report in September 2016. Various approaches were suggested in the report, including: "*practical measures to facilitate transborder cooperation between service providers and criminal justice authorities*"; the production of a Guidance note on Article 18 of the Budapest Convention to clarify, inter alia, when a provider is *"offering services in the territory"* of the requester; and even the possible development of an additional protocol to this treaty.

Workstream I should allow stakeholders to identify additional perspectives from other regions and get feedback on these approaches from participants.

1.3 OPERATIONAL CHALLENGES

The Global Internet and Jurisdiction Conference is intended to ensure a common appreciation of practical challenges and provide an opportunity for a broad appraisal of these proposed approaches. Discussions in Workstream I can be structured by the following non-exhaustive list of key questions and participants are

encouraged to identify and discuss other relevant challenges.

General questions:

Data types: Is the distinction between 1) basic subscriber information, 2) traffic data, and 3) content data clear enough, given the diversity of online services and platforms? Would a distinction between content and non-content data be enough?

Issuing authority: Should cross-border requests always be authorized by a judge or independent authority, or are there situations where they could be issued by an executive authority?

Admissibility: Is data obtained through voluntary cross-border cooperation always admissible in courts?

Regarding cross-border access to content data:

- Jurisdiction criteria: Are user nationality/residence and the locus of the investigated crime more appropriate criteria for asserting jurisdiction than the location of the stored data or the company's place of incorporation? How difficult is it to assess the nationality/residence of an Internet user?

  Geographic reach: Should country A be able to request information from an operator in country B regarding a user located in country C?

  Baseline standards: As an alternative to the US "probable cause" requirement, could a sufficient standard for voluntary disclosure by companies be: *"specific and articulable facts showing that there are reasonable grounds to believe that the records or information sought are relevant and material to an ongoing criminal investigation"*?

  Reuse and dissemination of obtained data: What limitations should apply here?

  Scalability: Are the proposed approaches potentially scalable beyond a small number of bilateral agreements and the transatlantic realm? What should be the criteria for participation in such a regime, and who would decide who can participate in them? Under what conditions?

  Real-time interception: Should the same mechanisms as for stored communications apply?

  Encryption: What impact does the increasing implementation of encryption for reasons of privacy and security have on mechanisms for cross-border access to user data?

Regarding access to non-content:

Baseline standards: How can procedural guarantees be improved? Should standards for access to subscriber information or traffic data be identical to the ones envisaged for access to content data?

Provision of services: Is this concept sufficiently clear? In particular, would the definition in the T-CY draft guidance to Article 18 of the Budapest Convention be a globally acceptable approach?

Production orders: Would strengthening the regime for access to subscriber information and traffic data in the US increase the risk of conflicts of laws regarding national production orders?

1.4 POSSIBLE COOPERATION AREAS

Some generic areas have emerged from previous discussions as having the capacity to build confidence among actors through active cooperation. In terms of timelines, these cooperation areas range from short to long-term horizons. Participants are invited to explore aspects of these approaches that are specific to cross-border requests for user data as well as identify potential additional topics.

Shared vernacular: Common definitions and terminology can be elaborated collaboratively to facilitate mutual understanding and legal interoperability.

Serious crime: Threshold criteria regarding types of incrimination or level of penalties could help determine the scope of such cross-border regimes.

Requester identification: It is often difficult for companies to assess if the sender of a request for user data is a legitimate authority, such as a formal law enforcement agency with the appropriate competence level. Accreditation and points of contact could facilitate this verification.

Transparency: A growing number of private actors now release regular transparency reports regarding data requests they receive and how they handle them. Yet, each company has its own format and similar information is not made available from public authorities. Standardizing data structures and common terminology could facilitate a wider adoption of transparency reporting and comparative analyses. This might also encourage broader disclosure of statistics by public authorities.

Request formats: Cross-border requests are transmitted in all shapes and forms, with highly variable levels of information. Such imprecision often leads to numerous back-and-forths before a request is processed. Building on the current practices of major intermediaries and countries, including existing submission portals, procedural and substantive best practices could be developed to set minimum standards regarding the information proper requests should contain.

Portals: Some companies and public authorities have instated or plan to develop electronic portals for the emission or reception of requests. Common protocols could promote interoperability.

User notification: Cooperation is needed to determine how the targeted user should be notified (ex ante or ex post) and the criteria and duration for possible exceptions.

Appeal: Intermediaries must increasingly assess the legitimacy of cross-border requests without the user having the capacity to weigh in or object early on when notification is prohibited. Even when users are notified, their current options for recourse are either sending a reconsideration request to the company itself or engaging in cumbersome, costly, and lengthy court procedures. Additional redress avenues, including alternative dispute resolution, could help fill this gap and provide a more

progressive escalation path.

Redress and Remediation: Unlike procedures for improper content removal or domain suspensions, remediation for improper access to user data is difficult. Various measures, including inadmissibility in courts might be examined.

The Workstream will aim to identify priorities for cooperation areas, timelines, and potential distribution of responsibilities among the different actors for the work ahead. In that regard, what role can Internet & Jurisdiction play as neutral convener to foster policy coherence between ongoing initiatives, and facilitate the multistakeholder development of policy standards? Outcomes of the discussions will be reported back to the Stakeholder Plenary on Day 3 of the Conference.

1.5 SELECTED READING MATERIAL AND REFERENCES

KEY BACKGROUND DOCUMENTS

UK-US BILATERAL AGREEMENT

Draft legislation proposed to US Congress on July 15, 2016

http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf Testimony of DOJ at a Congressional Hearing in February 2016 (see Section 3, "Possible Legislation")

https://judiciary.house.gov/wp-content/uploads/2016/02/doj-bitkower-testimony.pdf

White Paper for Congress in March 2016

http://www.netcaucus.org/wp-content/uploads/20160310-US-UK-Hill-Leave-Behind-Final1.pdf

DASKAL-WOODS PROPOSAL

Article by Jennifer Daskal (forthcoming)

http://jnslp.com/wp-content/uploads/2016/09/Law_Enforcement_Access_to_Data_Across_Borders.pdf

Initial post (November 24, 2015)

https://lawfareblog.com/cross-border-data-requests-proposed-framework

EUROPEAN UNION

Conclusions of the Council of Ministers of Justice and Home Affairs (June 9-10, 2016)

http://www.consilium.europa.eu/en/meetings/jha/2016/06/Cyberspace--EN_pdf/

Discussion paper on tackling cybercrime, Meeting of Ministers of Justice (January 26, 2016)

https://english.eu2016.nl/documents/publications/2016/03/7/general-discussion-paper-justice-ministers-meeting- cybercrime

Conference – "Crossing Borders: Jurisdiction in Cyberspace"

https://english.eu2016.nl/events/2016/03/07/crossing-borders-jurisdiction-in-cyberspace

COUNCIL OF EUROPE

T-CY Committee https://www.coe.int/en/web/cybercrime/tcy

Cloud Evidence Group

https://www.coe.int/en/web/cybercrime/ceg

Final report of the Cloud Evidence Group to the T-CY (September 2016)

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e Criminal Justice access to electronic evidence in the cloud – Informal summary and options

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8

MICROSOFT IRELAND CASE

Decision by the United States court of Appeals for the Second Circuit

http://www.ca2.uscourts.gov/decisions/isysquery/72076e07-ab83-4848-a69b-26fa4355dc96/1/doc/14-2985_complete_opn.pdf

POSTS RELATED TO ACCESS TO CONTENT DATA

Albert Gidari (Director of Privacy at Stanford Law School's Center for Internet and Society)

https://cyberlaw.stanford.edu/blog/2016/02/mlat-reform-and-80-solution-whats-good-users

Mark Jaycox and Lee Tien (Electronic Frontier Foundation)

https://www.eff.org/deeplinks/2015/12/reforms-abound-cross-border-data-requests

Greg Nojeim (Director of the Freedom, Security and Technology Project, CDT)

https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf

https://www.lawfareblog.com/mlat-reform-proposal-eliminating-us-probable-cause-and-judicial-review

https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata

https://www.lawfareblog.com/mlat-reform-who-decides

Comments about the US-UK negotiations:

Jennifer Daskal: https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/

Andrew Woods: https://lawfareblog.com/us-uk-data-deal

Kevin Bankston (Director, OTI): https://www.newamerica.org/oti/press-releases/oti-condemns-plan-let-uk-government-use-american-companies-internet-wiretapping/

EXAMPLES OF COMPANIES' TRANSPARENCY REPORTS, POLICIES, AND PORTALS

APPLE

- Transparency report

https://www.apple.com/privacy/transparency-reports/

- Guidelines for information requests (with special sections for EMEIA and Japan/APAC)

https://www.apple.com/privacy/government-information-requests/

- Privacy Policy

https://www.apple.com/legal/privacy/en-ww/

FACEBOOK

- Transparency report

https://govtrequests.facebook.com/

- Guidelines for Law Enforcement

https://www.facebook.com/safety/groups/law/guidelines

- Law Enforcement Online Request System

http://www.facebook.com/records

- Data Policy (see "How do we respond to legal requests or prevent harm?" sub)

https://www.facebook.com/about/privacy/other#

GOOGLE (various services including Gmail, YouTube, Blogger)

- Transparency report, section on user data requests

https://www.google.com/transparencyreport/userdatarequests/?hl=en

- Legal process regarding requests for user information from outside the U.S.

https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond

- Privacy Policy (see "Compliance and cooperation with regulatory authorities" sub)

https://www.google.com/policies/privacy/#enforcement

MICROSOFT

- Transparency Report (Law enforcement Requests)

https://www.microsoft.com/about/csr/transparencyhub/lerr/

- Principles, Policies and Practices FAQ

https://www.microsoft.com/about/csr/transparencyhub/pppfaq/

- Privacy Statement (see "Reasons We Share Personal Data" sub)

https://privacy.microsoft.com/en-us/privacystatement

TWITTER

- Transparency report, section on information requests

https://transparency.twitter.com/information-requests/2015/jul-dec

- Guidelines for Law Enforcement

https://support.twitter.com/articles/41949

- Law Enforcement Request Online Form

https://support.twitter.com/forms/lawenforcement

- Privacy Policy (see “Law and Harm” sub)

https://twitter.com/privacy?lang=en

WORKSTREAM II:

CROSS-BORDER CONTENT REMOVAL REQUESTS

2.1 THE COMMON PROBLEM

Content hosted by intermediaries is, by virtue of the Internet, publicly available worldwide by default. The amount of granular content posted by billions of users around the world is unprecedented: each day, more than 500 million tweets, 350 million pictures on Facebook, and 500,000 hours' worth of video on YouTube videos are uploaded. However, content legal in one country can be illegal or even criminal in another. Countries around the world increasingly try to enforce their national laws regarding content in cyberspace, creating new types of tensions and difficulties for Internet companies, charged with identifying and interpreting applicable laws while upholding the human rights of users.

Several trends have developed in this context:

Issues related to terrorism, incitation to violence, and various forms of harassment are high on political agendas.

- States or regions with strong ethnic, religious, or political tensions express growing public order concerns about the rapid and viral propagation of information.
- New approaches to privacy protection have emerged, raising new questions regarding the territorial application of de-listing search results.
- Rapidly increasing quantities of content removal requests are sent directly by public authorities in one country to private actors in another, putting on these companies the responsibility of determining the validity of these requests.
- Some degree of convergence has emerged in the wording of major platforms' Terms of Service, as well as in the increasing practice of Geo-IP filtering of content.

The current situation presents significant challenges.

- Although there might be consensus on the global unacceptability of some content such as child sexual abuse imagery, national laws greatly vary regarding applicable criteria on hate speech, incitation to violence, defamation and many other issues.
- Criminal offenses existing in some countries can be strongly opposed by others, for instance blasphemy, insulting heads of state, or the criminalization of certain sexual behaviors.
- Public order concerns can be abused and invoked to justify excessive removal requests, prompt blocking by ISPS, or even full Internet shutdowns.
- Difficulties in enforcing across borders national court decisions regarding specific pieces of content trigger disproportionate blocking or filtering of entire services.
- Massive numbers of micro-decisions with potentially important human rights dimensions must be taken by private actors, raising questions regarding the procedures and criteria employed.
- Private actors are increasingly pressured to move beyond the current limited liability/notice and takedown regime and voluntarily assume additional responsibilities to more systematically enforce their community guidelines or actively monitor and remove content according to codes of conduct.

Workstream II is dedicated to exploring the modalities of transnational voluntary interactions between public and private actors on cross-border content removal requests and identifying possible improvements.
All stakeholders are facing the need to reconcile the competing objectives of handling the global availability of content in the context of very diverse local laws and norms. Their common challenge can tentatively be described as: *Developing procedures and tools framing how authorized public authorities can request from foreign companies the removal of illegal content, within a framework respecting due process*.

2.2 CURRENT APPROACHES

Multiple approaches are being conducted in parallel (see links in Section 2.5) to frame interactions between public and private actors regarding content removal. These initiatives include:

- Internal procedures of Internet intermediaries. Terms of service establish de facto the applicable norms regarding expression in the cross-border online spaces managed by platforms. In addition to the detailed criteria contained in their community guidelines, they have developed internal procedures for handling requests and internal escalation.
- Bilateral interactions. Some governments have established special relations or guidelines with major online services, with specific procedures and rules for handling content removal requests.

- European Union. In December 2015, the European Commission established the EU Internet Forum to *"bring together governments, Europol, and technology companies to counter terrorist content and hate speech online."* In May 2016, the Commission and major Internet companies further agreed on a *"code of conduct regarding hate speech,"* and in July 2015, Europol established the Internet Referral Unit to *"combat terrorist and violent extremist propaganda."*
- Council of Europe. In addition to previous recommendations, the Council of Europe established the Committee of Experts on Internet Intermediaries (MSI-NET) in 2016 *to "prepare standard-setting proposals on the roles and responsibilities of Internet intermediaries."*
- Manila Principles. A civil society coalition launched the Manila Principles on Intermediary Liability in March 2015. It recently proposed a form to notify users of impending removal requests.
- Ranking Digital Rights. The initiative has identified 31 criteria to structure discussions on how to improve current practices by IT companies and procedural guarantees.
- Global Network Initiative. The GNI has developed Principles and Implementation Guidelines regarding content takedowns.

In addition, it is important to take into account the considerable impact of landmark court decisions in defining the responsibilities of intermediaries. Such cases include the Costeja decision by the European Court of Justice, as well as the *Delfi AS v. Estonia* and *MTE v. Hungary* cases by the European Court of Human Rights.

2.3 OPERATIONAL CHALLENGES

The Global Internet and Jurisdiction Conference is intended to ensure a common appreciation of practical challenges and provide an opportunity for a broad appraisal of the various approaches. Discussions in this Workstream can be facilitated around the following non-exhaustive list of key questions.

Scale

- Volume: Are courts able to handle the enormous amount of very granular content removal requests, or is private determination of the validity of requests the only viable solution?
- Legal clarity: How can private actors appreciate the legality of content with respect to 190+ different national laws and procedures? Are they sufficiently clear, predictable, and known? Do users understand the laws that apply to the content they post online?

Protection and responsibility of intermediaries

- Protections: Are existing provisions in different jurisdictions sufficient to limit the liability of intermediaries for content by third parties? How can intermediary protections be reaffirmed?
- Responsibility: Is there a trend towards imposing a greater responsibility on intermediaries for the

third-party content they host because they already enforce detailed community guidelines?

- SMEs: How can smaller intermediaries with users around the world but limited legal resources handle requests from potentially 190+ different countries?
- Terms of Service: Do community guidelines defined by major intermediaries become transnational norms and set global standards for freedom of expression? Should they?
- Monitoring: Does the use of automatic detection tools and algorithms to avoid the re-posting of illegal material amount to de facto general monitoring?

Proportionality

- Blocking: Is a global jurisprudence emerging prohibiting the blocking of entire websites or services on the basis of the illegality of only some content?
- Partial removals: Can geo-IP filtering be considered an appropriate tool to reconcile different national jurisdictions and ensure proportionality? Could there be unintended consequences?
- Global removals: Are there types of content that justify a global removal?
- Flexibility: Is there a risk that policy standards eventually developed for large corporations would be ill-adapted for SMEs and start-ups?

Due process

- Notifications: How and when should users be notified? Are there legitimate exceptions?
- Objections: How can users object/respond to a removal request?
- Appeals: How and to whom can users appeal a removal decision?
- Criteria: Is a new type of "dual incrimination" emerging, combining both the law of the requesting country and the Terms of Service of platforms? Is it appropriate?
- Super-flaggers: How useful is this concept? What are accountability mechanisms in that regard?

2.4 POSSIBLE COOPERATION AREAS

Some generic areas have emerged from previous discussions where confidence among actors can be built through active cooperation. Participants are invited to explore aspects of these approaches that are specific to cross-border requests for content removals and identify potential additional ones.

- Shared vernacular: Common definitions and terminology can be elaborated collaboratively to facilitate mutual understanding and legal interoperability.
- Requester identification: It is often difficult for companies to assess whether the sender of a request for content takedown is a legitimate authority, such as a formal law enforcement agency with the appropriate competence level. Accreditation and points of contact could facilitate

verification.

- Legal clarity: Accurate knowledge of applicable laws and their implementation in the different countries is lacking, particularly among small actors. Collaborative databases documenting the legal situation around the world could be envisaged.
- Transparency: A growing number of private actors now release regular transparency reports regarding the requests for content takedowns they receive and how they handle them. Yet, each company has its own format and similar information is not made available from public authorities. Standardizing data structures and common terminology could facilitate a wider adoption of transparency reporting and allow comparative analyses. This might also encourage broader disclosure of statistics by public authorities.
- Request formats: Cross-border requests are transmitted in all shapes and forms, with highly variable levels of information. Such imprecision often leads to numerous back-and-forths before a request is processed. Building on current practices of major intermediaries and countries, including existing submission portals, procedural and substantive best practices could be developed to set standards regarding the information proper requests should contain.
- Redress and remediation: Current recourse options for users are either sending reconsideration requests to the company itself or engaging in cumbersome, costly, and lengthy court procedures. Additional redress avenues, including alternative dispute resolution, could help fill this gap and provide a more progressive escalation path.

Participants will have the opportunity to validate and prioritize cooperation areas, timelines, and some potential distributions of responsibilities among the different actors for the work ahead. In that regard, what role could Internet & Jurisdiction play as neutral convener to foster policy coherence between ongoing initiatives and facilitate the multistakeholder development of policy standards? Outcomes of each workstream discussions will be reported back to the Stakeholder Plenary on Day 3 of the Conference.

2.5 SELECTED READING MATERIAL AND REFERENCES

APPROACHES

EUROPEAN COMMISSION

EU Internet Forum Announcement (December 3, 2015)

http://europa.eu/rapid/press-release_IP-15-6243_en.htm

Code of conduct on countering illegal hate speech online

http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

EUROPOL INTERNET REFERRAL UNIT

Announcement (July 1, 2015)

https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

First annual report (July 22, 2016)

https://www.europol.europa.eu/content/eu-internet-referral-unit-year-one-report-highlights

COUNCIL OF EUROPE

Committee of Experts on Internet Intermediaries (MSI-NET)

https://www.coe.int/en/web/freedom-expression/committee-of-experts-on-internet-intermediaries-msi-net-

SOME NATIONAL COOPERATION INITIATIVES

Germany (Agreement on rapid removal of hate speech)

http://www.theverge.com/2015/12/16/10287498/facebook-twitter-google-hate-speech-germany France (Common cooperation platform)

http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Le-ministere-de-l-interieur-mobilise-face-aux-cybermenaces

MANILA PRINCIPLES

https://www.manilaprinciples.org/

GLOBAL NETWORK INITIATIVE (PRINCIPLES AND IMPLEMENTATION GUIDELINES)

https://globalnetworkinitiative.org/principles/index.php https://globalnetworkinitiative.org/implementationguidelines/index.php

RANKING DIGITAL RIGHTS

https://rankingdigitalrights.org/

STUDIES AND REPORTS

COUNCIL OF EUROPE

Comparative Study on blocking, filtering, and takedown of illegal content (December 2015)

https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content- on-the-internet

EUROPEAN COMMISSION

Public consultation on the Regulatory Environment for Platforms, Online Intermediaries, and the Collaborative Economy

https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-

environment-platforms-online-intermediaries

INSTITUTE FOR INFORMATION LAW – UNIVERSITY OF AMSTERDAM

Study of Fundamental Rights Limitations for Online Enforcement through Self-regulation

http://www.ivir.nl/publicaties/download/1796

KEY COURT DECISIONS AND LEGAL REFERENCES

On proportionality

Turkish Constitutional Court on Twitter ban (proportionality criteria)

https://globalfreedomofexpression.columbia.edu/cases/akdeniz-v-the-presidency-of-telecommunication-and- communication/

Blocking of Facebook in Pakistan (proportionality and partial filtering)

https://globalfreedomofexpression.columbia.edu/cases/ali-v-pakistan-the-case-of-the-facebook-ban/

https://www.theguardian.com/world/2010/may/31/pakistan-lifts-facebook-ban

On the question of general obligation to monitor

European Union E-Commerce Directive (Article 15)

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031

European Court of Justice Scarlet / SABAM

http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-70/10&td=ALL

Tobias Mc Fadden v. Sony Music (opinion of the Advocate General)

http://curia.europa.eu/juris/document/document.jsf?text=st%C3%B6rerhaftung&docid=175130&pageIndex

=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=567718#ctx1

European Court of Human Rights

Delfi AS v. Estonia http://hudoc.echr.coe.int/eng?i=001-155105 *MTE v.*

Hungary
http://www.bailii.org/eu/cases/ECHR/2016/135.html

One (among many) comparative analysis of both judgments

http://kluwercopyrightblog.com/2016/03/05/mte-v-hungary-new-ecthr-judgment-on-intermediary-

liability-and-freedom-of-expression/

On the right to be de-indexed

European Court of Justice Costeja case

http://curia.europa.eu/juris/liste.jsf?num=C-131/12

CNIL (French Data Protection Authority) Decision from March 10, 2016

https://www.cnil.fr/sites/default/files/atoms/files/d2016-054_penalty_google.pdf

EXAMPLES OF COMPANIES' TRANSPARENCY REPORTS AND POLICIES

FACEBOOK

- Transparency Report

https://govtrequests.facebook.com/

- Community Standards

https://www.facebook.com/communitystandards#

GOOGLE (various services, including Gmail, YouTube, Blogger)

- Transparency Report, section on content removals

https://www.google.com/transparencyreport/removals/government/?hl=en

- Community Guidelines

https://www.youtube.com/yt/policyandsafety/communityguidelines.html

ICROSOFT

- Transparency Report, section on content removal requests

https://www.microsoft.com/about/csr/transparencyhub/crrr/

- Code of Conduct

https://www.microsoft.com/en/servicesagreement

TWITTER

- Transparency report, section on content removal requests

https://transparency.twitter.com/removal-requests/2015/jul-dec

- The Twitter Rules

https://support.twitter.com/articles/18311

WORKSTREAM III:

SITE-BASED DOMAIN SUSPENSION REQUESTS

3.1 THE COMMON PROBLEM

Trust in the Domain Name System (DNS) is critical to the functioning of the global Internet. The neutrality of the DNS vis-à-vis political or commercial pressure is a key factor in that regard. Yet, given the difficulty of dealing with illegal sites across borders, pressure is mounting to suspend domain names because of the alleged illegality of the underlying content or activity. Registries and registrars are receiving more and more of these requests, coming from inside or outside their country of incorporation.

This raises several issues:

- Domain suspension has a global impact and can easily be a disproportionate measure if only a portion of the content is objected to, or if the content is deemed illegal only in some countries.
- In any case, the objectionable website remains accessible via its IP address even after its domain has been suspended.
- National authorities' actions on operators based within their borders can have extra-territorial impacts on registrants in other countries, even when they conduct activities that are fully legal in their respective jurisdictions.
- DNS operators may have a global reach, but many are small actors with limited human and financial resources that struggle to evaluate the legitimacy of these demands.
- These operators usually only accept to comply with a decision by a court in their country of incorporation, but this is not a sustainable long-term approach, as it imposes the law of that country upon content in other jurisdictions.
- The lack of agreed-upon global mechanisms encourages blocking measures at the national level and emerging requirements for operators to register in a particular country in order to serve users there.
- This would threaten the capacity to register domain names from anywhere in the world, potentially

skewing the playing field for competition and harming developing countries.

Given the global impact of a domain name suspension, it can be justified in relation to the underlying site only if a very high threshold of illegal or objectionable activity is met, such as in the following situations:

- Abuses to the DNS itself, such as phishing, diffusion of malware, or support for botnets (with special provisions when an otherwise legal site has been compromised); or
- When the primary purpose of the site is manifestly dedicated to an activity globally recognized as harmful, such as child abuse images or blatant risk to health.

A third category of situations is much more delicate: when the site and its activity are legitimate in some countries but deemed illegal in others, or when only a minor portion of the content is considered illegal. In such cases, domain suspension is not the appropriate solution, except as last resort in certain cases.

Transnational procedures and criteria need to be developed to maintain the neutrality of the Internet's technical layer while dealing with abuses.

3.2 CURRENT APPROACHES

Two divergent approaches have been proposed:

- An ICANN-based policy approach. Some actors consider that dealing with illegal content on sites under a domain name is covered by the obligations contained in the accreditation contracts that registries and registrars sign with ICANN. Accordingly, its compliance department should enforce these provisions more systematically. In their view, the presence of all relevant actors in the multi-stakeholder ICANN community make it the natural place to develop any additional policy deemed necessary. On the other hand, ICANN itself and its Board consider that this would far exceed ICANN's limited mandate, particularly in the context of the revised Bylaws after the IANA Transition: ICANN, as technical coordinator of the system of identifiers should not be involved in policing underlying content. In any case, a full Policy Development Process (PDP) would be lengthy at best and even potentially deadlocked given the diversity of positions within the community.
- An industry-led voluntary regime. Under the impetus of some of its members, the recently formed Domain Name Association (DNA) has proposed the development of a voluntary approach under the label Healthy Domains Initiative (HDI). Among other things, it is intended to help develop *"more effective methods of addressing abuse complaints in the Internet community."* However, a clear disparity of positions inside the industry may produce important delays. Actors within the ICANN and law enforcement communities furthermore consider that the public order dimension of these issues demand that they be handled by a broader range of actors than just operators.

Irrespective of where and how such discussions should take place, a recent trend has been the growing role of third parties positioning themselves as "*trusted notifiers.*" In domains as diverse as child sexual abuse images, phishing, online pharmacies, counterfeiting, or copyright, national or international networks of associations have taken it upon themselves to proactively or reactively identify alleged abuses and report them. Even if they can potentially alleviate the operators' burden to make their own decisions, their evaluations are established without clear procedures or mechanisms for redress and may be based on the laws of only one particular country.

3.3 OPERATIONAL CHALLENGES

Discussions in this Workstream can be facilitated around the following (non exhaustive) key questions:

Territoriality

- Extraterritoriality: Should the laws of the country of location of the registry or registrar apply to the content on the site under a domain, even if it is owned and hosted outside of that country?

General criteria

- Abuse of the DNS: Is there global acceptance that domain suspension is justified for sites hosting phishing, malware, or botnets? Are there additional criteria or situations to take into account?
- Harmful content: Beyond child sexual abuse imagery, are there types of content that are broadly considered as globally unacceptable?
- Partially illegal content: Should domain suspension be envisaged as a last-resort option if a site legal in one country is manifestly targeting another where the activity is judged illegal and no compliance has been seen after repeated injunctions to not serve this jurisdiction? Should there be a distinction between commercial activities and speech-related ones?

Notifiers

- Accreditation: Who should have the responsibility to certify such operators? Or is it just a matter of voluntary adoption by the registries and registrars themselves?
- Legal foundation: What criteria do notifiers use in their determinations? Are they sufficiently global or rather anchored in one specific country or trade association?
- Procedures: How can sufficient transparency be ensured?
- Accuracy: How can false positives that lead to excessive restrictions be prevented? Rating mechanisms?
- Governance: Are notifiers independent bodies or trade associations?
- Accountability: What mechanisms could ensure accountability of these notifiers? To whom?

- Responsibility: Is there a potential risk of liability for DNS operators if they do not follow the notification of such third-party validators?

3.4 POSSIBLE COOPERATION AREAS

Some generic areas have emerged from previous discussions as having the capacity to build confidence among actors through active cooperation. Participants are invited to explore aspects of these approaches that are specific to requests for domain suspensions and potentially identify additional ones.

- Shared vernacular: Collaboratively establishing common definitions of inacceptable behavior or content could facilitate mutual understanding and legal interoperability.
- Best practices for notifiers: Clarification of the conditions and procedures under which such actors make their determinations could strengthen confidence in their accuracy.
- Validation: The creation of trusted third parties to review and validate reports by notifiers has been suggested in order to enhance due process and neutrality. The conditions of their formation, their specific mandate and the basis for their decisions would need to be examined.
- Transparency: A growing number of platforms now release regular transparency reports regarding the requests they receive and how they handle them. Yet, this practice is not yet adopted by DNS operators, often for a lack of resources. Reporting formats remain different and no similar information is available from public authorities. A standardization of data structures could facilitate a wider adoption of this practice, allow comparative analyses, and encourage broader disclosure.
- Request formats: Cross-border requests are still transmitted in all shapes and forms, with highly variable levels of information. Such imprecision often leads to numerous back-and-forths before a request can be properly processed. Building on the current anti-abuse policies of major operators and notifiers, including existing submission portals, best practices could be developed to set due process standards regarding information proper requests must contain.
- Redress and remediation: DNS operators will increasingly be asked to assess the legitimacy of cross-border requests for domain suspensions on a voluntary basis, without the registrant having the capacity to object or weigh in early on in most cases. Yet, registrants' current choice of recourse is either to send a reconsideration request to the DNS operator itself or to engage in cumbersome, costly, and lengthy procedures in (foreign) courts. Additional redress avenues, including alternative dispute resolution, could help fill this gap and provide a more progressive escalation path.

Participants in Workstream III will have the opportunity to validate and prioritize cooperation areas and timelines, as well as potential distribution of responsibilities among the different actors for the work ahead. In that regard, what role could Internet & Jurisdiction play as neutral convener to facilitate interactions and move

the dialogue forward? Outcomes of the discussions will be reported back to the Stakeholder Plenary on Day 3 of the Conference.

3.5 SELECTED READING MATERIAL AND REFERENCES

APPROACHES

ICANN

Position regarding ICANN's limited mandate (letter by Board Chair Steve Crocker)

"This does not mean, however, that ICANN is required or qualified to make factual and legal determinations as to whether a Registered Name Holder or a website operator is violating applicable laws and governmental regulations, and to assess what would constitute an appropriate remedy for such activities in any particular situation."

https://www.icann.org/en/system/files/correspondence/crocker-to-shatan-30jun16-en.pdf

Registry agreement

> 4. Abuse Mitigation
>
> 4.1. Abuse Contact. *Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.*

https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

Registrar accreditation agreement

> 3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.
>
> 3.18.1 *Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.*
>
> 3.18.2 *Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.*
>
> 3.18.3 *Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.*

https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

THE DOMAIN NAME ASSOCIATION

About the DNA http://www.thedna.org/

Healthy Domains Initiative

http://www.thedna.org/the-dna-launches-hdi-press-release-2-16-2016/

EXAMPLES OF SPECIALIZED NOTIFIERS

Anti-Phishing Working Group (APWG)

http://www.antiphishing.org/

Internet Watch Foundation (UK)

https://www.iwf.org.uk/

Inhope http://www.inhope.org/gns/home.aspx

LegitScript https://www.legitscript.com/

Center for Safe Internet Pharmacies (CSIP) https://safemedsonline.org/

Characteristics of a trusted notifier program (by Donuts, in the context of its MoU with MPAA)

http://www.donuts.domains/images/pdfs/Trusted-Notifier-Summary.pdf

五、會議相關照片

照片 1:會場入口

照片 2:會議地點

照片 3:第 1 天大會

照片 4:第 1 天大會

照片 5:分組討論會場

照片 6:分組討論會議

照片 7:會議閉幕及感謝工作人員

六、網路犯罪公約

European Treaty Series - No. 185

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well- functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;
Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R(88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;
Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;
Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;
Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion,

deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance

with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub- paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the

jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty

shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co- operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify

the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an

offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or

similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day- a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a

period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the

expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9
paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4,
Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22,
paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.