ICANN 工作小組
電子報
2021/11/15

重點議題

1

ICANN72 圓滿落幕。

前往閱讀

文摘

NIS2：安全、靈活性及 DNS 伺服器基礎建設

Olaf Kolkman 檢視 NIS2，分析立法意圖和技術現實之間的差距。

個人意見：網際網路的下個 50 年

以網際網路或通訊科技的角度而言，50 年並非足以帶來巨變的時間。

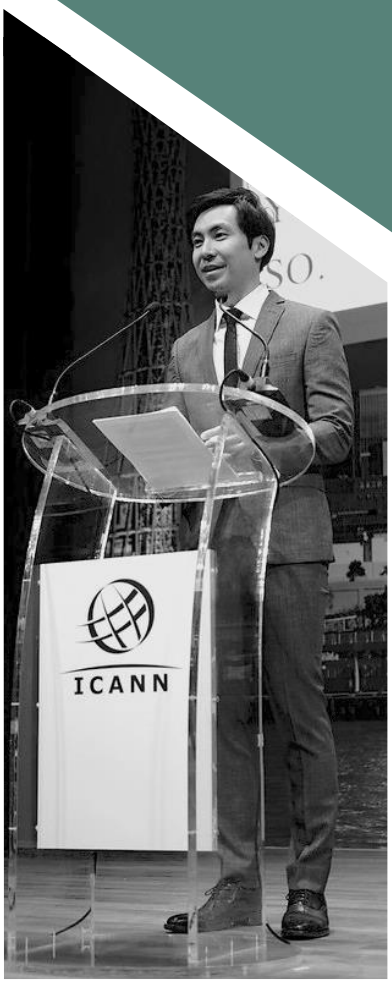
前往閱讀

最新消息

2

- ICANN73 將以線上形式舉行
- SSAD 實施評估流程：履約執行及身分認證方式
- 當責跨社群工作小組第二工作階段實施完畢：下一步
- 更全面的 DNS 安全威脅分析

前往閱讀



公眾意見徵詢

3

- 拉丁文根區標籤生成規則提案
- ICANN 文件資訊揭露政策修訂提案

前往閱讀

重點議題

ICANN72 圓滿落幕

ICANN72 已於今（2021）年 10 月 28 日結束。這是自 COVID-19 疫情以來，第 6 次全面線上舉行的 ICANN 會議，共有來自 156 個不同國家、1,305 名與會者遠端參與。根據 ICANN ORG 分享的統計資料，13.8%與會者來自非洲地區、22.1%來自亞太地區、7.63 來自拉丁美洲加勒比海地區、20.8%來自歐洲地區；來自北美地區的參與人口比例最高，共佔全體與會人口的 35.6%。

另一方面，本次會議也是 ICANN 有會議參與人數紀錄以來，史上與會人數最低的一場會議。不只比今年中 ICANN71 政策論壇的 1,330 人還少，比起 2016 年，ICANN 開始分享會議參與人數的 ICANN55 摩洛哥會議，即使當時摩洛哥仍處於恐怖攻擊的餘波，仍有 2,273 人與會，是 ICANN72 的將近兩倍。

大會議程：更包容、平等參與的混合模式 ICANN 會議

自 2020 年本應於坎昆舉行的 ICANN67 以來，ICANN 已兩年未舉辦實體會議。隨著全球疫情趨緩，疫苗接種率逐步提升，許多國際網路治理組織也開始摸索所謂的「混合」模式（hybrid）會議。雖然基本概念都是結合實體及線上參與，但由於組織組成和會議型態不同，每個國際組織會議的「混合」模式也不盡相同。

有鑑於此，ICANN72 的大會議程也以「包容、平等參與的混合模式」為名，廣邀社群探究 ICANN 專屬的混合模式會議。然而，雖然名為「混合模式」，但觀察社群討論，不難看出大家最在乎的仍是「混合」中的「實體」元素。幾個特別引起迴響的社群意見包括：

- ICANN 應接受一旦開始「混合」模式，有辦法實體參與的與會者，和無法實體參與的線上參與者之間，必定出現斷層。不平等是必然的結果，但缺乏實體會議，所有工作將停滯不前，也是無可迴避的現實。所以社群和 ORG 應共同思考，如何在「安全但工作無進展」和「不平等但工作有進度」之間做抉擇。
- 目前 ICANN 會議中僅提供即時口譯服務，但翻譯服務不包括文字，所有與會者只能使用英文在線上會議的聊天室中提出意見。這對非英文母語者並不公平，應思考如何建立對所有語言使用者更公平的環境。
- 對長期參與 ICANN 會議的人而言，轉換至線上形式雖不習慣，但不至於無法繼續。然而，ICANN 變成全面虛擬形式後才開始參與的初來者，在不認識任何人、對環境陌生的情況下，參與將異常困難。無法吸引新血，ICANN 社群將出現斷層；如何在全面線上的形式仍持續引入、留住新人，是必須深刻思考的課題。

2021 年 Tarek Kamel 博士培力獎得主

ICANN72 首日，ICANN 宣布來自印度的 Satish Babu 榮獲 2021 年 Tarek Kamel 博士培力獎。Satish Babu 目前是亞太地區一般使用者團體（Asian, Australasian, and Pacific Islands Regional At-Large Organization，APRALO）的主席，本獎項是對他在本土、地區及國際網路治理培力貢獻的肯定。

不只身為 APRALO 主席，Satish Babu 也是一般使用者諮詢委員會（At-Large Advisory Committee，ALAC）中推動國際化域名（Internationalized Domain Name，IDN）和全球通用（Universal Acceptance，UA）的主力，積極參與並領導 ALAC 中多個相關工作小組。全球通用是成就多語言及數位包容的網際網路的關鍵，ICANN 董事會也希望藉此獎項感謝 Babu 的付出。

TOP

最新消息

ICANN73 將以線上形式舉行

ICANN 於 11 月 4 日宣布，原訂 2022 年 3 月 5 至 10 日於波多黎各聖胡安舉行的 ICANN73，仍將以全面線上的形式舉辦。線上會議將依聖胡安時區（UTC-4）進行，但實際天數長短可能視社群諮詢結果調整。

ICANN 指出，雖然全球疫苗接種率逐漸上升，但傳染性極高的 Delta 病毒仍肆虐全球，對規劃明年 3 月於聖胡安舉行實體會議而言，風險仍太高。實體會議的前期規劃長達數月，在旅遊限制及其他變數下，ICANN ORG 及相關人員也難以前往會議場地進行技術測試或流程演練。

董事會理解實體互動的價值，以及對推動社群工作的正面效益，但首要考量仍是所有人員的健康和安全。對預計 2022 年 6 月於荷蘭海牙舉辦的 ICANN74 政策論壇，董事會重申以混合模式舉辦的意志，也已指示 ICANN 主席暨執行長與社群合作，開始設計如何以混合模式實現 ICANN74 會議。

TOP

SSAD 實施評估流程：履約執行及身分認證方式

規範具合理目的之第三方如何取得註冊資料的標準化註冊資料存取／揭露系統（System for Standardized Access/Disclosure，SSAD ）正由 ICANN ORG 進行實施評估（Operating Design Phase，ODP）。今年 10 月底的 ICANN72 中，ICANN ORG 向社群報告本工作社群進展 （錄影、簡報），表示將延長截止期限，預計於 2022 年 2 月提交實施評估分析報告。

履約執行和身分驗證方式是 SSAD 的兩大主要元素，也因此，ICANN ORG 在實施評估工作同時，希望就這兩個主題徵詢社群意見。問題內涵如下：

履約執行

SSAD 政策建議中，涉及 ICANN 履約執行的部分包括：

- 程序性投訴：若申請取得資料方或資料主體認為合約方（註冊管理機構或受理註冊機構）在處理非公開註冊資料揭露要求時，未遵守程序規定，則可提出投訴。
- 服務層級協議（Service Level Agreement，SLA）投訴：合約方未滿足 SLA 規定時（如太晚回應緊急要求），則可提出投訴。

以上項目將循既有的履約執行標準流程執行。投訴人須透過域名服務介面（Naming Services portal，NSp）提出 SSAD 相關投訴，每筆投訴將以單一事件處理。必要情況下，也可以為 SLA 投訴建立自動化流程。

社群意見徵詢問題

- 政策中指出涉及履約執行的項目，是否已包含所有 ICANN 履約部門有權執行的部分？

身分認證方式

SSAD 建議中指示，所有透過 SSAD 提出註冊資料請求的使用者都必須取得認證。建議中將使用者分成兩類：

- 非政府之自然人及法人：ICANN 將作為中央認證權威，負責管理此類使用者的身分認證。
- 政府機關或跨國政府組織：上述由 ICANN 擔任的中央認證權威，不負責此類使用者的身分認證。

為了非政府自然人及法人的身分認證，ODP 專案團隊調查了市面上的身分認證方式。以下是 ICANN 提議，用來認證自然人使用者的認證選項：

- 電子身分證（eID）系統；
- 提出附照片、當地政府發放的身分證明；
- 提出具電子認證功能、當地政府發放的身分證明。

針對法人，ICANN 則提議：

- 通過上述認證流程的自然人，提出法人的名稱、組織形式、地址、稅務或其他編號後，由中央認證權威或指定之身分認證單位負責驗證。

針對如何驗證自然人代表特定法人單位的主張屬實，ICANN 提議的驗證方式包括：

- 通過系統驗證、取得身分認證的自然人，可主張其代表法人單位提出非公開註冊資料請求。
- 此自然人必須提供代表法人單位的相關資訊，包括法人名稱、法人形式、實體地址、稅務或其他法定編號。
- 確認自然人代表及法人單位指定聯絡人之間的關係。自然人代表須與 SSAD 系統中指名此指定聯絡人，且指定聯絡人需隸屬法人單位之下。
- 此指定聯絡人將提交法人單位的存續證明書（certificate of good standing）或具同等效力之文件。

更多細節說明，請參考 ICANN72 相關議程簡報。

社群意見徵詢問題

- 上述提議的身分認證方式是否符合以下資格的驗證需求？
  - 可能成為 SSAD 使用者的自然人；
  - 將以「使用者所屬單位」存於 SSAD 紀錄中的法人；
  - 自然人與主張代表單位的關係。
- 上述提案是否確保未來可能的 SSAD 使用者（如下列）需付出一定努力以取得認證資格？
  - 希望取得認證資格的使用者；
  - 主張屬於特定法人單位的使用者；
  - 主張代表特定法人單位的使用者。

切記，雖然需要透過 SSAD 請求取得資料的使用者必須通過身分認證，但取得身分認證並不保證一定能取得資料。大多數情況下，合約方在收到資料揭露請求後，仍將依規定審核資料請求，才會決定是否提供對方要求之資料。

任何問題，或針對上述問題若有任何建議及反饋，都可寄信至 ODP-SSAD@icann.org。此信箱收到的所有信件都是公開庫存，可點此查看。

TOP

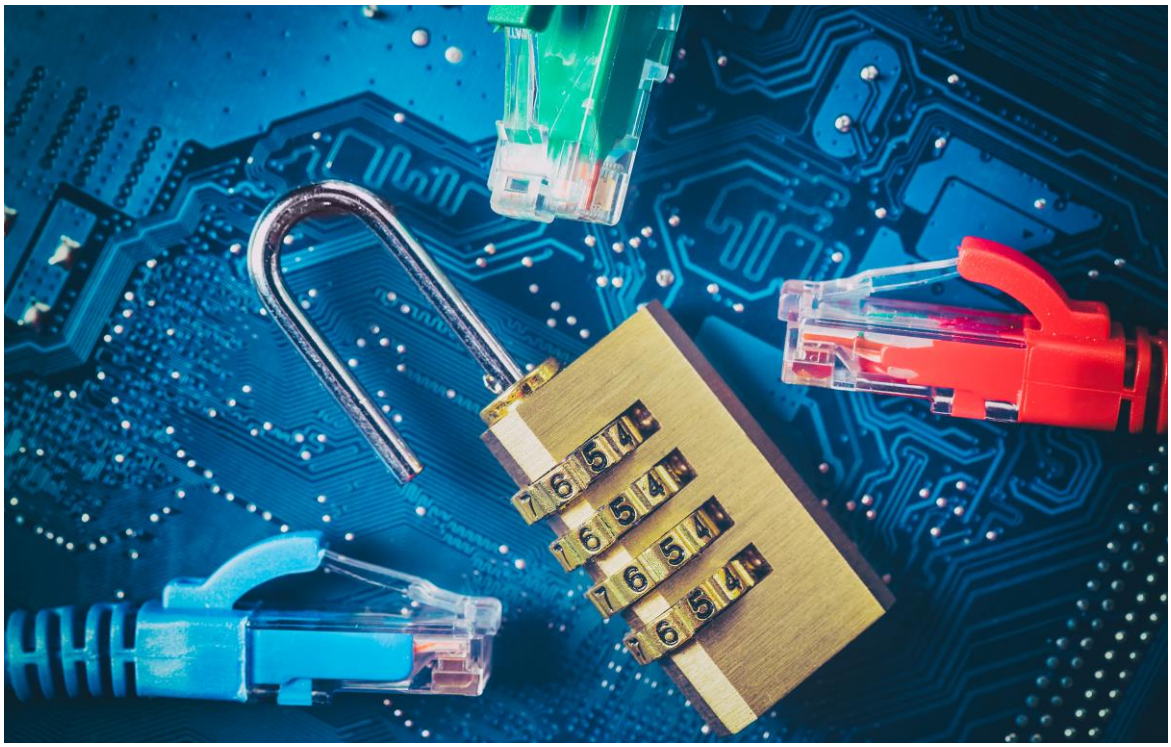
當責跨社群工作小組第二工作階段實施完畢：下一步

ICANN 今年 11 月宣布，改善 ICANN 當責跨社群工作小組（Cross-Community Working Group on Enhancing ICANN Accountability，CCWG-ACCT）第二工作階段（Work Stream 2，WS2）已實施完畢。

WS2 的結案報告中，共向社群及 ICANN ORG 提出超過 100 項當責與透明度的相關建議，目的是確保 ICANN 持續對多方利害關係社群負責。

在 2021 年 3 月的進度報告中，ICANN 曾向社群表示，組織內部召集專業人才組成跨部門專案團隊，也針對經董事會決議通過之建議，制定了強化現行工作的執行計畫。計畫中包括 ICANN ORG 應如何支援社群規劃各團體的 WS2 建議執行，隨著組織內部的相關工作告一段落，未來 ICANN ORG 也將持續協助社群審視文件、流程，討論工作排程，以及任何其他可能工作（如草撰提案）。

TOP



更全面的 DNS 安全威脅分析

ICANN ORG 於 2021 年 6 月就曾分享，希望延伸域名濫用活動報告（Domain Abuse Activity Reporting，DAAR）以涵蓋受理註冊機構資料。DAAR 是由 ICANN ORG 維護，研究並記錄頂級域名（top-level domain，TLD）註冊管理機構相關安全資料的系統。

過去，將受理註冊機構資料納入 DAAR 的最大障礙，在於 ICANN ORG 難以取得域名註冊資料中的受理註冊機構 ID。經研商，ICANN ORG 與合約方已取得原則共識，將透過修改基本通用頂級域名（Generic Top-Level Domain，gTLD）註冊管理機構協議，容許 ICANN ORG 未來取得此資料，供研究用途使用。

註冊管理機構利害關係團體（Registries Stakeholder Group，RySG）主席 Samantha Demetriou 表示：「RySG 支持 ICANN ORG 在 DAAR 中納入受理註冊機構資料的計畫，進一步提升 ICANN 社群對 DNS 濫用的整體知識，展開資料導向、事實為本的相關討論。」受理註冊機構利害關係團體（Registrars Stakeholder Group，RrSG）主席 Ashley Heineman 也補充：「我們對此更新倍感期待。」

接下來，ICANN ORG 會根據此原則共識調整協議文字，在取得雙方同意後，依正式流程修改基本 gTLD 註冊管理機構協議。

DAAR 的整體目標，是打造健全、值得信賴且可再現的安全威脅活動趨勢分析方法，如此一來，ICANN 社群將得以基於事實證據展開政策討論。新增受理註冊機構層級的量測指標後，DAAR 會變得更全面，對更多人而言，包括受理註冊機構自己，DAAR 也將成為更有用的工具。

TOP

「公眾意見徵詢」

拉丁文根區標籤生成規則提案

開始日期	2021 年 9 月 23 日	結束日期	2021 年 11 月 23 日
提請人	ICANN ORG		
類別／標籤	技術		
簡介	根區標籤生成規則（Root Zone Label Generation Rules，RZ-LGR）是為了判斷國際化域名（IDN）頂級域名（TLD）及異體字標籤是否有效的保留機制。而 RZ-LGR 的成功，仰賴不同語言社群組成的標籤生成委員會（Generation Panel，GP），為自己的語言研究、規劃並提出標籤生成規則。 拉丁文本的標籤生成委員會已完成拉丁文的標籤生成規則。在提交予 RZ-LGR 整合委員會之前，ICANN ORG 公告本提案，針對提案中的碼點指令表（code point repertoire）、異體字定義及管理規則，徵求公眾意見。		
網頁連結	https://www.icann.org/en/public-comment/proceeding/proposal-for-latin-script-root-zone-label-generation-rules-23-09-2021		

ICANN 文件資訊揭露政策修訂提案

開始日期	2021 年 10 月 21 日	結束日期	2021 年 12 月 6 日
提請人	ICANN ORG		
類別／標籤	其他		
簡介	為符合 WS2 結案報告建議，ICANN ORG 修訂了組織的文件資訊揭露流程（Documentary Information Disclosure Process，DIDP）。本意見徵詢主要希望徵求社群對修訂文件中，關於監察員（Ombuds）及投訴主管的 DIDP 關聯責任，尋求社群建議及反饋。		
網頁連結	https://www.icann.org/en/public-comment/proceeding/proposed-revisions-to-the-icann-documentary-information-disclosure-policy-21-10-2021		

TOP

文摘

NIS2：安全、靈活性及 DNS 伺服器基礎建設

資料來源：Internet Society（原文連結 ）
內容摘要：

歐盟的網路及資訊安全指令第二版（second Network and Information Security directive，NIS 2）雖然尚在制定過程，但去年底歐盟執委會提出修訂草案時，就已引起相關網路技術社群的注目。許多意見認為，草案中試圖嚴加規範 DNS 的內容，將不利於 DNS 的安全和靈活性。

歐盟作為歐洲國家的政經集合體，有其特殊的立法體系。目前，NIS2 的草案就有 3 個版本，分別來自歐盟國會（European Parliament），歐盟議會（European Council，由歐盟成員國組成），以及歐盟執委會（European Commission，歐盟的布魯塞爾行政部門）；未來三方將就各自提出的草案進行協商，產出單一最終版本。

自 NIS2 草案首次公開，網際網路協會（Internet Society，ISOC）便一直密切注意相關進展。ISOC 網際網路技術、政策及倡議總監 Olaf Kolkman 所撰此文聚焦於歐盟議會提出的 NIS2 草案，透過檢視草案中關於 DNS 的文字，分析立法意圖和技術現實之間的差距。

NIS2 希望保障歐洲經濟體仰賴的基礎建設安全且值得信任。這個目標很合理，事實上，我們應該希望全球各地經濟民生仰賴的網路基礎建設，都保持安全可信。

然而，為了達成「安全」的目標，NIS2 希望將規範之手伸進 DNS。歐盟議會版本的 NIS2 附件寫到，「DNS 服務供應業者，包括在歐洲具一定規模（超過 10 個據點）的根域名伺服器營運方」，都將是 NIS2 規管對象。

Kolkman 主張，如果以網路安全三大支柱——完整性（Integrity）、真實性（Authenticity）、可用性（Availability）來檢視 NIS2 針對 DNS 的規範文字，NIS2 並無法真正加強 DNS 的安全或信任。

在 DNS 中，所謂的「完整性」是指「使用者收到的域名資訊，與域名營運方提供的資訊相符且正確」。DNS 安全擴充（DNS Security Extensions，DNSSEC）利用數位簽章，確保使用者收到的回應未遭竄改（完整性）的同時，也驗證此回應的確來自使用者試圖查詢的域名本人（真實性）。

換句話說，DNS 服務供應業者是否啟用 DNSSEC，才是確保 DNS 查詢回應完整性和真實性的關鍵，跟業者在歐洲的據點數量無關。而根據 ISOC 量測資料，歐洲整體的 DNSEEC 部署率其實相當不錯。

對使用者而言，「可用性」代表送出 DNS 查詢後能即時得到回應，成功前往目的地域名。

在 DNS 中，這個過程涵蓋：使用者的 DNS 查詢傳到本地 DNS 遞迴解析器，再由解析器詢問權威域名伺服器取得答案後，回傳給使用者。在此過程中，解析器會建立並保留一份哪些伺服器有什麼域名的資訊清單；日後收到針對特定域名的查詢，解析器會隨機向清單上有此域名資訊的伺服器送出查詢，無論對方位於何處。

也就是說，解析器中轉域名查詢時，並不像法規想像的會限於某洲或某地區內，而是隨機向地球任一角落的伺服器送出查詢。

為了強化 DNS 的靈活性、可用性和效能，DNS 伺服器廣泛使用一項名為「anycast」的技術。簡單來說，就是完整備份特定 DNS 伺服器的資訊後，把這個備份大量散置於網路各處。這些與「本尊」伺服器擁有一模一樣資訊的「分身」叫做「instance」，每個 instance 都會成為網際網路上接收、回應解析器查詢的訊務磁鐵。

建立大量 instance 有兩大好處。第一是加強效率，第二則是 instance 身為訊務磁鐵的特質，一旦受到服務阻斷攻擊（denial-of-service，DOS），網管人員得以即時發現、迅速處理。換句話說，一個區域內的 instance 越多，當地網路使用者就越不容易受到 DOS 攻擊的影響。

這也代表，歐洲境內的域名伺服器 instance 越多，歐洲的網路使用者就可以享有更穩定、效能更好的網路。

然而，NIS2 反而把「據點」較多的網路營運業者列為規管對象。這很可能導致營運業者寧願減少歐洲境內的伺服器數量以迴避規範，進而傷害歐洲網際網路基礎建設的靈活性和可用性。

Kolkman 解釋，基於 DNS 的架構設計，整個系統的當責其實是由下而上成就。若政府試圖透過法規從上向下規範，反而可能導致網路分裂，也不利網路安全。他認為，現行的多方利害關係治理模式是最適合、也最有利於根伺服器系統管理的最佳實踐，NIS2 應該直接將根伺服器系統排除於規管對象。

TOP

個人意見：網際網路的下個 50 年

資料來源：APNIC Blog（原文連結）

內容摘要：

APNIC 首席科學家 Geoff Huston 試圖想像網際網路的下個 50 年。原文從 50 年前談起，解釋電話網路和網際網路的差異，並觀察市場的連帶演變。除了預測未來 50 年的網際網路發展，Huston 也列出如此發展下，網際網路基礎架構可能如何改變。礙於篇幅，本文摘僅節錄原文中關於未來 50 年網際網路發展預測的部分。

Huston 認為，依視野不同，50 年其實可長可短，但以網際網路或通訊科技的角度而言，50 年並非足以帶來巨變的時間長度。他指出，今日的科技其實早在 50 年前就可看出端倪，而且帶動過去 50 年科技發展的驅動力，跟推進未來 50 年的並無不同。

根據這些驅動力，Huston 認為未來 50 年的網路發展有四大重點：更大、更快、更好，也更便宜。

更大代表會有更多海底電纜、全球網際網路的訊務流量會更龐大；不只是基礎建設，連網裝置的數量也將一路攀升，裝置數量和訊務流量的成長也將帶動更多網路內容和服務。

硬體建設規模和訊務流量既然都將一路上漲，那使用者對速度的要求也只會越來越高。對現代使用者而言，100 mbps 只是基本要求，而 5G 網路能達到的最高速率（20 gbps），大概不久後也會被認為「太慢了」。所謂的「更快」，追求的不只是傳輸系統本身的速度，也是系統回應使用者的速度。換言之，未來的網路會持續往低延遲、高容量邁進，對使用者而言，網路的「反應」會越來越快。

「好」是個相對抽象的概念，但 Huston 認為，若「更好」代表「更值得信任」和「更保護隱私」，那目前的網路可能已小有進展。然而，由於網際網路基礎建設問世的時代背景已與現在大不相同，過去預設無條件信任的網路協定，在今日反而廣遭濫用，使用者的隱私也因此不保。有鑑於此，為了確保網際網路更值得信任，服務、應用程式、內容和網路基礎建設之間的信任，反而必須消失。

以網路的發展而言，更快、更好並不代表更貴，反而是更便宜。有時候甚至看起來是免費的，例如，任何人使用 google 搜尋引擎都不用付錢。但實際上，google 之所以無需仰賴使用者付費支應維運搜尋引擎的開銷，是因為它們搜集大量使用者資料，再把資料賣給廣告商營利。當然，這意味使用者個資是足以換錢的資產，但有趣的是，若任一使用者想販賣自己一個人的個資給廣告商，對方恐怕也不屑一顧。個資唯有累積到數千萬筆的規模，對廣告商才有價值；也可以說，這些「免費服務」是因為萬千使用者集結而成的集體資產才成為可能，而這種經濟模式，其實也反向確保網路不會成為精英獨享的服務。

很多人認為不可能同時達到更大、更快、更好又更便宜，然而數位平臺做到了。數位服務平臺之所以能提升流量並降低價格，並非單靠擴大硬體網路的規模；改變使用者取得服務的方式，是另一個主要關鍵。

現在的網路運作模式，幾乎已經不再透過網路把內容從當地一路傳到另一端，而是在邊緣進行大部分工作。邊緣運作可以縮減封包傳輸路徑、降低網路開銷、提高回應效率，而這也意味著體感速度的提升。Huston 認為，持續把大部分工作推向網路邊緣，會是未來幾十年的趨勢。

然而，對 Huston 而言，這並不代表網路將變得更華麗、更有用，或更「聰明」。恰恰相反。他主張，把網路的功能推向邊緣，表示網路基礎架構和邊緣裝置不再共同負擔開銷、承擔責任，這將進一步削弱互聯互通、全球共享的單一網際網路的重要性。

一直以來，我們都認為網際網路意謂網路通用、協定通用，位址資源也通用。任何連網裝置都可以將 IP 封包透過網路，傳給另一個連網裝置。只要用的是通用位址資源中的位址，所有人都還是這網際網路的一部分。

隨著上述演變，這個簡單事實似乎也不再是現實。未來的網際網路會代表什麼？或許，未來的網際網路只是一種通用概念，指稱使用同一參照機制（DNS），沒有實體形狀、分散的服務聚合。

結論看似悲觀，但 Huston 其實還是樂觀的。他指出，人類過去無數次成功推翻自己對科技的既有想像，造就許多驚人美好的技術成就。他也期待，未來 50 年間，類似情形仍將持續發生，而且只會更多，不會更少！

TOP