moz://a

白　皮　書

將開放引入身分證件

開放型國民身分系統的技術性與政策性選擇

Amba Kak, Jochai Ben-Avie, Alice Munyua & Udbhav Tiwari

Chinese translated by Jasper P.W. Chen, edited by Irvin Chen

目錄

本報告原始英文版本
The original English version of this report is available at
https:// mzl.la / 3iL9vAB

摘要

線上、線下生活中，我們越來越需要證明或被證明自己的身分。像是讓人以臉書（Facebook）身分登入的社群登入服務、用來針對你精準行銷的廣告 ID（Ad ID），或是用單一身分識別連結你的簡訊、音樂偏好、購買的應用程式和支付資訊的 Apple ID。我們可以且應當關心，私人企業使用身分系統建立關於我們的龐大資料庫，於此同時，許多政府早已超前好幾步。許多國家中，民眾必須使用政府發行的單一數位（且常是生物辨識的）身分，以獲取糧食配給、醫院治療或讓手機上網，一切的一切，都登錄至集中式的政府資料庫。大多時候，這些身分系統，都是建置在缺乏資料保護法，或缺乏健全的連線基礎建設的開發中國家。

採用數位身分的推手，部分來自於主張這是擴大取得法律身分（legal ID）的必要途徑之國際開發社群。聯合國永續發展目標（SDGs）要求在 2030 年前「為所有人提供法律身分，包括出生登記。」擁有法律身分，逐漸變成使用基礎服務、取得國家與私人服務之權利的先決條件。少了這些廣泛認可的官方身分證明形式，人們便會面臨遭到排除和拒絕服務的風險。然而，特別是國際開發社群，將數位身分視同「法律身分」（或其延伸），往往造成不論是非地擁護數位身分專案之現象。

這些身分專案的數位特性，與相互串連的基礎建設，和類比式的系統相較，有著截然不同的意涵。舉例來說，常常是——包含極為敏感的資訊（生物辨識資料，甚或是 DNA 資料）、容許將身分證字號在多個資料庫間相連結、因集中的資料收集而導致更強的監控能力，以及依賴往往不甚牢靠的電力與連線做即時驗證，加劇了排外的現象。

這些身分專案的數位特性，與相互串連的基礎建設，和類比式的系統相較，有著截然不同的意涵。

數位身分的爭議帶來以下問題：生物辨識資料的合理使用、透過資料庫連結而擴大監控、在低人權環境（如：缺乏資料保護法規或無法貫徹執法的國家）的科技實驗、設計科技專案時缺乏相關諮詢。這些問題又多與網路及人工智慧（AI）等新興科技的廣泛顧慮有所重疊。

設計、執行和營運數位身分系統時，政府必須做出一系列技術性和政策性選擇。這些選擇決定了身分系統是賦能，抑或是剝削和排外。儘管有數個組織針對數位身分發佈了相關原則，這些原則對於全球各地無止境地推廣數位身分，卻往往無法有效約束。本文中，我們提倡以開放性作為引導和批判這些選擇的有效框架，同時確保身分系統是以人民為優先。我們特別針對**五大開放要素**進行檢視並提出建議：**多樣化的選擇**、**去中心化**、**課責**、**共融**及**參與**。

本文歸結出以下建議：

- ▷ 自專案的設計階段開始，政府須在身分系統的技術性和政策性選擇上，進行廣泛的諮詢。任何身分系統的生物辨識資料之蒐集與使用，皆伴隨著重大的隱私風險，應審慎地在開放、諮詢且以實證為本位的過程進行評估。必須顧及如基礎建設、連線能力、職業與數位素養，以及一國之內身分證明的制度性、社會性及政治性背景等因素。

- ▷ 在身分證明的使用及持有上，應該讓人民在分享重要的身分屬性時，有多樣的選擇；而非強推單一、僵固且強制性的萬用型身分系統。

- ▷ 數位身分自構想階段，便應規劃避免其淪為賦予和強化政府及私人監控的工具。各國應嚴加檢視驗證紀錄之必要性，並確實制定法規，限制驗證紀錄之留存、取用與分享。此驗證的過

程，可產生某人在何時何地使用身分的數位紀錄，這樣的驗證紀錄，也會造成隱私和安全上的重大風險，並增加了監控的可能性。

▷ 私人公司資料庫上留存國民身分證字號的使用情形，可用來剖析（profile）和區別各個公民。如此用途必須經過公開討論並加以規範。在不同資料庫中，藉由身分證件之使用，相互關聯的能耐，可大大強化私人公司的追蹤能力，應由法律禁止或規範至最低程度。根據政府發行的身分（特別是具有開放 API 的系統）所創造的私人生態系，皆須詳加檢查，特別是將個人資料用於掠奪用途的應用方式，更須如此。

▷ 推行任何國家級生物辨識身分專案前，需先具備資料保護法，且有強大、獨立的執法人員。

▷ 身分系統的技術，必須可由獨立的外部實體進行稽核，以確保信任、安全與共融。為確保身分系統在技術上，符合監管該系統及個人資料的法律框架，應進行稽核。我們也建議開放所有國民身分系統的原始碼，如此可以提升系統的透明度，並確保其產出經得起稽核的驗證。

▷ 可驗證之共融性（inclusion）應為數位身分系統設計的重心之一。沒有人該因人口學的特徵或身體特徵而受到排除。身分系統必須顧及不同族群的數位素養（digital literacy）能力，也必須在低連線能力的環境下維持運作。不可因未持有特定身分證件，或系統無法運作，而拒絕個人使用必要的服務。

▷ 所有人在使用自己的身分證件時，必須可以剔除（opt out）特定類型的資料分享，特別是揭露時，可能會造成傷害的敏感資訊。

導論

今日**數位身分**有諸多意義。數位網路的擴張，引介了電子郵件位址、電話號碼、社群訊息的化名（handle）及社群媒體服務等一連串新的識別方式，這些方式則由一些最大的網路公司（谷歌、臉書、推特、LinkedIn）。現在有越來越多這樣的公司，也化身為「身分提供者」，供使用者在網路上互動。好比說，每當有人決定要「以臉書帳號登入」（或以谷歌或 LinkedIn 帳號登入）網站或應用程式，這些公司便會進到這些交易和相關的資料足跡當中。這些使用者在線上行為的資料足跡，形成了個人辨識檔，自成一種數位身分。這些數位身分對許多人來說，無論是社群媒體公司，或是廣告網路，都是寶貴的資源，可用以鎖定使用者、客製化內容並行銷給使用者。

於此同時，政府這樣較為傳統的「身分提供者」，也在轉化自己的身分系統的本質，無論是將他們類比式身分系統，升級為數位式身分系統，或是創建新式、全數位連線的身分系統。最明顯的模式，就是要求人民輸入多模態生物辨識資料（multi-model biometrics，指紋、虹膜掃描及相片），以取得專屬的身分證字號。透過這些系統使用服務時，會要求人們分享字號與自己的生物辨識資料（如：指紋），接著以電子方式傳送至集中式資料庫，與檔案比對驗證。這樣的驗證流程，可產生某人於何時何地使用身分的數位紀錄。事實上，即使我們還在討論線上匿名的價值和合理保障隱私的方式，全球各地的政府，也正在爭先恐後地建立數位系統，來辨識和追蹤居民的線上以及線下的生活。

Mozilla 致力於尋找使科技服務公共利益、豐富人類生活的方式。數位身分的討論凸顯出這項議題。帶出生物辨識資料的合理使用、透過資料庫連結而擴大監控、在低人權環境（如：缺乏資料保護法規或無法貫徹執法的國家）的科技實驗、設計科技專案時缺乏相關諮詢等問題。這些問題，大多與網路和人工智慧（AI）等新興科技的廣泛顧慮有所重疊。

本立場文件書將專注探討政府數位身分專案的背景，大量援引印度與肯亞的經驗，並參考愛沙尼亞與加拿大卑詩省（British Columbia）等地的經驗。過去幾年來，我們見到全球多個政府，宣布並推出國家等級的數位通用型身分專案。這些專案有許多形式，有晶片為主且含有生物辨識資料的智慧卡，有專屬號碼為主的系統，也有採用手機為主的識別與認證機制。政府發行的數位身分，往往是強制居民使用的證件，供其享用福利及其他服務，也因此為所有民眾帶來顯著、真切的影響。對多數邊緣化的族群而言，身分系統往往是他們首次與數位科技互動的管道之一。

1.
背景問題與情境設定

1.1 法律身分 vs. 數位身分

聯合國永續發展目標（SDGs）要求在 2030 年前「為所有人提供法律身分，包括出生登記。」擁有法律身分，逐漸變成使用基礎服務、取得國家和私人服務之權利的先決條件。少了這些廣泛認可的官方身分證明形式，人們便會面臨遭到排除和拒絕服務的風險。

然而，特別是國際開發社群，將數位身分視同「法律身分」（或其延伸），往往造成不論是非地擁護數位身分專案之現象。這些身分專案的數位特性，與相互串連的基礎建設，和類比式的系統相較，有著截然不同的意涵。舉例來說，往往會：

- ▷ 包含生物辨識甚或是 DNA 等資訊
- ▷ 容許將身分證字號以電子方式在各個連線資料庫間相連結
- ▷ 強化基於人口學條件的搜尋篩選能力
- ▷ 倚賴不甚可靠的電力與連線做即時驗證

這些數位特性，通常會被鼓吹為增進登記與驗證效率的方式，相較於類比式的系統也更難造假。然而，透過各國經驗的驗證，這些所謂的效率，卻完全會因其建置的情境而有所不同。更甚者，數位與生物辨識系統帶來新的問題與威脅，我們也會在後續章節作探討。一切關於效率的聲明，皆須受到嚴格檢視，而我們也必須準備好思考：數位科技在身分證系統的適用性與適切性問題。

1.2 監控與數位身分

身分系統引起政府監控的合理限度之問題。從登入到無線網路熱點到購買火車票、預約門診，當各式各樣的服務，針對同一個專屬號碼，透過國家的集中式系統進行驗證，國家便取得一個人移動、活動和關係的精細紀錄。即使在身分證字號本身無法連結敏感資訊的場域，其得以在不同資料庫裡，辨識出特定人士的能力，也可產生出敏感的關聯資訊。在印度，中央政府創建了居民的線上公開圖表，並可按宗教信仰與種姓等級[1]進行搜尋，需要的只是結合數個互不連結，但奠基在 Aadhaar 號碼（印度強制性、連結生物辨識資料的身分證號碼）的資料庫。

身分系統促進和協助政府監控的能力，常常是不宣之秘，但有時也會是這些專案明載之目標。在印度，最高法院基於貧弱的行政審核能力，及可能導致「權力濫用」緣故，剔除了允許驗證紀錄揭露給政府監控的法律條文。在墨西哥[2]和巴基斯坦，其國民身分證專案便載明其反恐、維持法紀與秩序的目標。巴基斯坦的身分資料庫「NADRA」，便連結[3]至刑事資料庫，並時常用於刑事調查之中。

除了政府，私人公司也可能利用身分系統的監控能力。印度的數位身分系統，奠基在容許公共與私人用途的開放 API 系統，便是一例。無論是電信公司[4]、銀行或作背景查核[5]，或是我們發現的追蹤遺失的亞馬遜（Amazon）包裹[6]，越來越多的服務，開始要求 Aadhaar 號碼。雖然這些公司不一定能夠看到個人的完整驗證紀錄，卻仍可以保有身分證字號的相關紀錄，並可再與其他企業和服務的類似資料庫相結合。最終這會讓資料庫更輕易相互聯結，方便大量剖析所有人。2018 年 9 月，印度的最高法院，針對私人公司於 Aadhaar 系統毫無限制的用途，加上了幾個限制[7]，部分原因，便是出於這些可預見的隱私風險。

除了政府，私人公司也可能利用身分系統的監控能力。印度的數位身分系統，奠基在容許公共與私人用途的開放 API 系統，便是一例。

1.3 聚焦開發中國家

光是**世界銀行**本身，過去十五年來在開發中國家，便已支持至少 63 個身分證件專案[8]，而數量也只會是有增無減。不同發展階段的國家，在實行數位身分時，其中亦顯見國際開發社群，刻意鼓勵[9]開發中國家，升級或「大躍進」地採用這些技術。

大衛・里昂（David Lyon，2009）指出[10]，幾乎所有的已開發國家，如美國[12]、英國[13]、加拿大[14]、法國[15]與澳大利亞[16]，便曾見證過，除了相片[11]以外，加入其他資料之國家生物辨識身分證件專案，遭到反對並最終消亡，反對的原因便包含隱私考量等因素。在開發中國家，儘管當地和國際公民社會團體積極阻止、提出疑慮，卻往往來不及在這些專案的設計階段，影響其結構性的改革。印度身分專案的法律框架，是在大部分的人民登記後才引入；而肯亞通過了一項法案，授權蒐集生物辨識資料（包含 DNA），作為新式數位身分系統的一部份，在此之前卻未曾公告周知或做公眾討論。公眾諮詢對受影響的利害關係人與公民社會團體參與來說，至關重要。印度與突尼西亞[17]，儘管有經過貧乏的諮詢過程，針對身分證件專案，仍舊出現各式各樣的抗議與行動，而牙買加最高法院，則裁定其身分證件專案完全違憲；然而，許多國家卻難以從如此強健的公民社會受益，或是從如此強健的司法反應受益。

儘管在資料保護上，僅有微弱的法律規範（及有限的執法紀錄），亞洲、拉丁美洲與非洲中許多開發中國家，卻在努力推行數位身分，讓人憂心。包含印度、肯亞、奈及利亞與馬來西亞，幾個國家，在沒有任何既有法規，約束政府使用個人資料的情形下，便已實行數位身分系統。各個政府與捐助組織，在評估國家身分系統的潛在衝擊時，必須將這些法律及制度性的具體事實納入考量。

1.4 當前以原則為基準之方法

近期的研究（New America，2018 [18]）將各種以原則為基準（principle-based）的身分證件框架作比較，包含國際組織（世界銀行[19]、世界經濟論壇[20]）、公民社會組織（Access Now [21]）及個別專家（Kim Cameron [22]、Christopher Allen [23]）。這些框架或多或少，樂於強調隱私和安全性，作為核心價值，也注重身分證件在不同社會經濟差異上的普遍性及可近性。

我們希望主要在兩大方向上，補足這些成果：

- 其一，儘管這些框架[24]中有些是將開放性視為價值，卻幾乎縮限在互通性上——更具體來說，指採用開放 API 或身分證件的開放標準，以防掉入供應商陷阱[25]（vendor lock-in）。然而，身分證件的開放性，應該較這個侷限的定義來的更為廣泛。不僅是要包含更廣泛的技術指引，更重要的是，也必須包含多種社會、法律及政策選擇，以賦予個別使用者最大的能力。後續的章節中，我們將說明開放性的各個價值，可在哪些面向，更全面地引導數位身分的討論。

- 其二，這些原則大致都承認，隱私應作為數位身分討論的核心，我們亦點出一些，特別是在開發中國家的情境下，達成此目標的必要規準。

2.
開放型國民身分系統

所有數位身分系統，皆是一連串技術與政策設計選擇的結果。開放性的幾個關鍵面向之考量，提供一個有用的框架，於其中做出將人民納入（並保持）在這些系統之核心的設計選擇。具體來說，我們整理出有關國民身分證討論之開放性的五大面向：多樣化的選擇、去中心化、課責、共融及參與。

2.1 選擇多樣化之開放

人都應該有多樣化的選擇，得以選擇揭示個人身分組成之關鍵屬性的方式，而非強推單一僵固的系統。然而，選擇使用哪種身分之選項，無論是在現實或是法規，常常淪為幻夢一場。特別是在集中式的國民身分系統，更是如此，畢竟政府通常有權在多種必要的公共（有時也是私人）服務上，要求出示國民身分證。

每個人通常應該能依情境之合理要求，僅須揭示自己身分之特定、相關的屬性。反對論點便是主張一套「基本」身分系統，應擁有廣泛的（而非特定的）功能，以在方便性、可近性與易用性上享有大大的好處。儘管這些都是值得考慮的重要價值，卻不該作為藉口，強迫不願在不同情境下使用同一種身分證件的人接受。在許多國家之中，單一身分系統之推行，常常意味著，可能一夜之間，先前的身分證便遭淘汰，留給使用者的僅是有限的選擇。

在不同情境下強推萬用型、單一、集中式系統的另一副產品，便是單一驗證紀錄（包含身分證件的所有使用情形之紀錄），揭露出每個人的詳細資訊與行動，侵害隱私並形成嚴重的安全風險。應該將系統設計成，完善個人在不同情境中的能動性與彈性的系統。

堅持採用由集中式主管機關發行之單一身分證件，而非憑據需求導向之方式，就如同秘魯與印度的經驗所示，可能會有嚴峻的後果。在祕魯[26]，2012 年政府衛生福利專案的登記數量，在要求孩童必須使用國家身分證後，大幅滑落，最終導致在部分的重點區域，出現大量的孩童營養不良。至於印度的 Aadhaar 系統，雖然明訂完全是自願採用，卻看到該身分證件成為許多必要的公共與私人服務之先決條件，造成實質上的單一標準，再也無法使用舊版的身分證件。在印度的幾個不幸案例[27]中，人們因無法取得糧食配給而餓死，原因不是沒有 Aadhaar，就是系統本身缺乏功能、電力或連線能力維持運作。值

堅持採用由集中式主管機關發行之單一身分證件，而非憑據需求導向之方式，就如同秘魯與印度的經驗所示，可能會有嚴峻的後果。

得注意的是，在祕魯與印度兩國的法律中，確實允許替代方案，以避免拒絕服務（如：使用另一種政府發行的身分證件），但這些指示卻未貫徹至前線的行政人員。

更宏觀地說，我們執迷於尋求，達到「單一」正確的身分模式之專案。舉世界銀行的身分證件原則為例，其提出許多關於隱私、安全與互通性的進步價值。然而，以上這些都形塑出要有「一個」健全的身分證件及「一個」單一平台之暗示，而非像真實世界般，有個足以自多種權威性來源，取得各種屬性與身分之系統。當我們探討數位身分的優劣形式時，應當將選擇及免於迫害作為討論的核心。

2.2 去中心化之開放

國民身分證專案通常本身就是集中導向，其驗證包含：公民出示一組號碼，接著在政府的集中式資料庫進行搜尋，如出示的驗證要素，與檔案上的相吻合，該使用者便視同通過驗證。若將指紋生物辨識資料登記進去，便是看該指紋是否吻合。這些系統的目的，往往是創造出幾乎適用於所有身分證明用途的身分。在Aadhaar的情境中，Mozilla早已表明[28]，儲存包括生物辨識資料等個人敏感資訊之集中式（或集中連結式的）基礎建設的諸多危險。近來數個大型資料洩漏案例證明，集中式系統意謂著，可供惡意攻擊的單一弱點。另一個相關的問題，則是驗證紀錄的集中化，可強化得以檢視紀錄之實體的監控能力。就政府身分證件而言，如此可強化「功能潛變」（function-creep）的恐懼，恐怕驗證紀錄可被用於監控用途，而這也是登記在系統上的人，所意想不到的功能。例如：基於取得好處的前提，所提供的個人敏感資料，可能會用來傷害人並妨害隱私，無法剔除，甚或收到通知。

試圖解決這些問題的替代技術模型紛紛出現，其概念是設計出，人們有權控制身分屬性之用途及分享對象的系統，著重在確保使用者，在使用服務驗證身分時，不會留下一個集中式的資料足跡。

近期加拿大卑詩省的「服務卡」（BC Services Card [29]），就是身分系統在技術設計上，內建隱私保護的一個例子。其系統的設計，讓居民所出示的同一張「卡片」，在不同系統上有不同的樣貌。舉例來說，在醫療情境下，呈現為衛生系統識別證；在路上被攔檢時，出現的是駕照號碼；同時針對驗證紀錄，也有著嚴格的資料最少蒐集原則（data minimization）及儲存限制政策。

還有其他許多新興的模型，採用去中心化、加密模型確保身分的驗證，是由身分證件的分享對象進行，並確保沒有一個集中式的紀錄。在私部門部分的相關例子有：

加拿大卑詩省的「服務卡」，就是身分系統技術設計上，內建隱私保護的一個例子。其系統的設計，讓居民所出示的同一張「卡片」，在不同系統上有不同的樣貌。

Evernym、uPort [30]和 VeresOne。像加拿大[31]等政府，也是積極資助並實驗去中心化的系統。名為「去中心化身分識別碼」（Decentralized Identifier，DID）的開源標準[32]，便是由個人（居民）掌控權力。如政府機關等所有發行主管機關，皆可使用此識別碼，配發可驗證的證件給居民，包含旅行證件、駕照及教育證書。儘管這些模型都有其潛力，應用的高度複雜性，以及可用性與可行性之問題，仍是一大挑戰，特別是在有基建障礙和素養障礙的開發中國家，更是如此。要設計出去中心化且安全的系統，仍有努力的空間，才能使人無須仰賴高度的數位素養，也能信賴這樣的系統。

2.3 課責之開放

封閉式系統，是個對於其影響的民眾與生活不為所動的系統。國民身分系統的集中化設計，自然會賦予政府與其他實體，對於登記在系統並經此識別的人，有著極大的權力。這也是這些系統之設計，必須確保能一直回應所影響的人並向其負責。在系統的幾個關鍵重點上的開放，對於制衡國家力量，並讓使用者在知情且同意的情況下，管理自己向政府與私人系統表明身分的方式，十分重要。對於身分的主動維護，可理解為被動系統的反面，而被動系統，就像是可以在群眾中，利用臉部辨識演算法辨別出個人，並刻意迴避取得有效同意之必要性的系統。

法律課責

課責架構之一便是透過法律，規範由身分系統所蒐集之身分資訊的資訊流。這些法律必須有可信賴的執法機制支持，一體適用於政府及透

過該系統取得資料的私人實體。完整的資料保護法及監控的規範，得以確保任何身分系統蒐集最少的資料（蒐集限制原則，collection limitation principle），而所產生的資料庫，不會用於其主要功能之外的目的（目的限制原則，purpose limitation principle）。

針對身分系統的常見顧慮，便是「功能潛變」，即身分資料庫用於資料庫原始目的以外、完全不一樣的目的（根據的也常常是已然獲得的同意授權）。在西方民主國家中，關於國民身分系統的功能潛變與資料分享的問題，是在許多政府服務引入大型伺服器資料庫時，開始受到關注[33]。1960 後期至 1970 年代初期，各式各樣的公眾討論，包含主流出版品的文章[34]、政府公聽會、報告[35]，最後藉由法律行動[36]，大大縮限社會安全碼（social security number）——美國實質上的國民身分證——的用途[37]。

理論上，可以想像蒐集指紋的生物辨識身分證件，可在福利支出上，遏止詐騙行為。萬一這樣的指紋資

完整的資料保護法及監控的規範，得以確保任何身分系統蒐集最少的資料（蒐集限制原則），而所產生的資料庫，不會用於其主要功能之外的目的（目的限制原則）。

料庫，後來用在掃描比對犯罪現場證據呢？這樣的用途，等同將所有公民視為犯罪嫌犯，也是民眾起初同意提供自身指紋時，從未設想到的用途。適用於國家機關的完善資料保護法與確實執法，可以防止此類的濫用情形。

資料保護框架亦可確保，一旦不需要這樣的資料時，像是有人選擇退出或身亡，他的資料便會自系統中刪除；若有相關的驗證資料，也僅會在必要的最短期間內留存。重要的是，資料保護法如同歐盟的《一般資料保護規則》（General Data Protection Regulation），提供個人存取自己資料的權利。愛沙尼亞[38]的國民身分系統中，每個人都可以要求得知，各個政府機關持有哪些關於本人的資訊及其原因。愛沙尼亞人通常可檢查，有誰在何時存取了他們的資料，而未獲授權的政府請求是有其罰則的。

這些法律框架，若只是個亡羊補牢的措施是不夠的。建置生物辨識身分系統的國家，必須在應用這些系統前，便具備資料保護法及獨立、強力的執法人員。少了法律保障，登記與驗證（和任何已取得的同意授權）之資料蒐集流程，便無法課責，使已登記的人幾無選擇或有效之保障。

技術課責

課責的技術機制也是關鍵，從整體系統的底層設計，到各個元件，皆是如此。這些系統之設計階段的開放性，對取得公民社會意見相當重要，以便確保在身分系統運作方式上，能減少傷害的風險。系統設計並建置完成後，重要的是，要可以由外部監督實體，進行系統的技術稽核。必須能在系統持續運作之情形下，讓外部的獨立稽核人員，檢查系統的安全設計與措施。尤其是如果程式碼本身並未開源的情況下，更須如此。

另一個達成開放性的方式，是允許檢視身分系統真正的程式碼。開源的程式碼，也可以讓公民、公民社會團體、公司及其他利害關係人，對系統和政府的目的有更大的信心。公開程式碼及相關的 API，可讓所有人查核並驗證系統的安全與隱私，也可揭發出許多潛在的惡意活動。開放身分系統的原始碼，也可創造一群致力於捍衛系統安全，並發展更多新功能的社群，為居民提供更大的隱私及掌控權。在與廣大社會介接的大型政府系統上，更是如此；其中程式碼及相關元件的透明度，有助於改善掌握如此規模的敏感資料庫時，無可避免的信心低落之問題。模組化開源身分平台（Modular Open Source Identity Platform，MOSIP [39]）等計畫，也強力佐證單靠開放的程式碼是不夠的。端賴採用這樣基礎的政府，是否能維持這開放性的承諾——不僅在程式碼上，亦包含將規範這樣系統的社會及法律系統。

在印度的 Aadhaar 案例中，Mozilla 一再[40]警告，不透明的安全措施，連同不斷發生的人口資料外

單靠開放的程式碼是不夠的。端賴採用這樣基礎的政府，是否能維持這開放性的承諾——不僅在程式碼上，亦包含將規範這樣系統的社會及法律系統。

洩，讓人難以信任該系統的可靠性。綜觀其安全漏洞，如報告所提[41]，有可能以低廉的價格取得 Aadhaar 資料庫編輯的權利，這樣的漏洞，在如此規模的系統，是個不可接受的風險。像這樣的潛在安全漏洞，會影響到超過十億的印度人，並將數個重要的公共與私人服務置於危險之中。持續拒絕接受讓 Aadhaar 做獨立的安全稽核，是個相當嚴重的問題。

這也凸顯出具有開放 API 的身分系統，與有效開放的身分系統之間的落差。儘管 Aadhaar 具有開放的 API，並允許開發大量的私部門與公部門的用途；單靠如此，並不能確保 Aadhaar 亟需的課責。事實上，奠基在國家發行的證件上所創造的私人生態系，必須受到嚴格檢驗，特別是使用個人資料於掠奪式用途的應用方式（例如：信用貸款）。這些用途，可輕易將讓賦予人民權力的身分系統，轉變成剝削人民的身分系統。

2.4 共融性之開放

開放往往是確保共融性的關鍵。共融式系統，允許每個人有能力以自己的方式參與技術系統。某種程度而言，這是確保沒有人會因為身體上、社會上或經濟上的不足，而遭身分系統排除在外。鑒於這些系統建置在開發中國家，而這些國家所具備的低度連線基礎設施及數位素養，著實是個大問題。舉例來說，完全無卡式系統用於即時驗證，在斷斷續續的連線能力，或時常斷電的情況下，就會變得十分不可靠。這些都再再提醒著我們：急於「大躍進」至數位科技的同時，千萬別忘記，實體離線系統在特定情境下，所能提供的諸多效率。

幾個現有的身分證件原則，皆提及這樣不得因為人口學的特徵，或身體特徵（如：因勞動而磨損指紋的人）而放棄任何人的目標。然而，共融性要求的是，必須兼顧兩個方面：確保所有人不會因缺乏特定身

分證件，或系統無法正常運作，而無法使用必要服務；確保所有人有能力剔除自己身分證件的特定用途。

剔除專屬國民識別號碼的部分用途之能力，至關重要，特別是對於社會上最邊緣、可能因剖析而承受最大風險的族群來說，更是如此。在不同情境中限制資訊分享之能力，便對這些族群來說十分重要。舉肯亞為例，近期肯亞宣布要將 DNA 資料納入身分系統，便引起了嚴重的顧慮，擔心會將 DNA 連結到種族身分上。有鑑於肯亞的種族身分政治化前科[42]，創建有這樣資訊的資料庫，恐怕會再現並加重歧視的行為模式。在印度也是如此，需要 Aadhaar 資訊才能接受愛滋療法的做法[43]，也引發了顧慮。對於這些族群來說，紀錄被保留下來，並可能在未授權的情況下，分享出去的風險，可說是大得可怕。

2.5 透明及參與之開放

身分系統涉及一連串技術性和政策性的選擇，其中許多對於個人權利、安全及公眾信任，有重大的影響。特別是在關鍵的設計階段，需要廣泛的諮詢，包含諮詢科技專家及受影響之族群。然而現實是，許多這樣的專案缺乏公眾諮詢，往往迴避或略過公眾及國會諮詢的要求。在肯亞，允許政府，蒐集包含 DNA 等數個生物辨識資料的國家綜合身分管理系統（National Integrated Identity Management System，NIIMS），是夾藏在一個更大型的法案中，以修正案形式通過；顯然違反肯亞憲法中，針對重大立法必須作公眾參與及諮詢之要求。當印度最終建立規範 Aadhaar 的法律框架，並以行政命令運行五年之久，卻仍有爭議之處。其爭議在於是以「財稅法案」形式，即採用簡短流程，跳過討論與辯論等正常議會程序，通過[44]這項法律框架。

此舉讓人感到憂心，因為其展現出，政府想要將身分系統，視為以行政命令即可通過的技術系統。值得注意的是，在英國、法國及澳大利亞等已開發國家中，生物辨識身分系統，在諮詢階段遭遇到強烈的反對後，便在實行以前止步。如此彰顯出，這些專案的設計階段之透明度與關注的重要性，方便公眾參與探討，如何實行這些系統的方式之外，還有要不要實行的問題。

許多參與在這些技術系統之中的私人廠商，往往是外國公司，因所涉及的個人資料之敏感性，也同樣引起嚴重的國家安全與隱私的顧慮。選擇廠商時的透明度，因此也是所有健全的諮詢過程中，另一個重要的面向。舉例來說，法國廠商 IDEMIA，前身為肯亞的摩爾富（OT-Morpho），在具爭議的 2017 年肯亞總統選舉中，提供生物辨識選民驗證系統，其中涉及販售選民資料之嚴重疑慮[45]。針對[46] Aadhaar 外國廠商的相關指控（要求資訊時才得以揭發），因其達成的多個合約並不公開透明，進而導致民眾的不信任感。

以數位元件建置身分系統，有個開放且參與式流程的正面例證，也就是加拿大的卑詩省。在推行其「公民服務卡」（Citizen Services Card）前，政府透過專家論壇[47]、使用者小組[48]及所有居民皆可參與、分享自己想法的線上問卷，積極與民眾互動。收到這些回饋之後，政府也回應了相關聲音與資訊[49]。

3.

開放型國民身分系統之
建議與政策規準

國民身分系統在設計、實施與運作上，需要政府做出一系列技術性及政策性選擇。期盼下方的建議，得以引導政府及其他組織往更開放、更課責且更共融的國民身分系統邁進。

▷ 任何身分系統的生物辨識資料之蒐集與使用，皆伴隨重大的隱私風險，應審慎地在開放、諮詢且以實證為本位的過程中進行評估。不同國家的經驗顯示，所謂使用生物辨識資料的效率，完全會因其建置的情境與因素，如基礎建設、連線能力、職業及數位素養，而有所不同。更甚者，在決定建置未來可能武器化的科技時，必須考量一國之內，身分證件的機構性、社會性及政治性歷史因素。

▷ 分享重要的身分屬性上，人民應享有多樣化的選擇，而非強加單一、死板的萬用型系統。堅持採用單一身分證，可能會有嚴峻的後果。如同祕魯與印度的經驗顯示，不具有特定身分證件，或該身分證驗證失敗，可能導致最弱勢的族群，無法取得必要服務或福利。當我們探討數位身分的優劣形式時，必須審慎地以多樣選擇及免於迫害為依歸。

▷ 數位身分自構想階段，便應規劃避免其淪為賦予和強化政府及私人監控的工具。各國應嚴加檢視驗證紀錄之必要性，並確實制定法規，限制驗證紀錄之留存、取用與分享。留存在私人

公司資料庫上的國民身分證字號使用紀錄，可用來剖析各個公民，而如此用途必須經過公開討論並加以規範。在不同資料庫中，藉由身分證件之使用，相互關聯的能耐，可大大強化私人公司的追蹤能力，應由法律禁止或約束至最低程度。根據政府發行的身分（特別是具有開放 API 的系統）所創造的私人生態系，必須受到嚴格檢驗；特別是將個人資料用於掠奪式用途的應用方式，可輕易將賦予人民權力的身分系統，轉變成剝削人民的身分系統，更須詳加檢查。這樣的生態系，必須受更高的責任義務及公共課責之法律標準約束。

▷ 在推行任何國家級生物辨識身分專案前，需先具備資料保護法，且有強大、獨立的執法人員。這些法律框架，若只是個亡羊補牢的措施是不夠的，必須在推行國家生物辨識身分專案前便已完備。

▷ 身分系統的技術，必須可由獨立的外部實體進行稽核，以確保信任、安全與共融。特別是透過稽核，確保身分證系統在技術上，符合監管該系統及個人資料的法律框架。利用開放程式碼的國民身分系統，更多了一層透明度，也納入了課責。大體而言，儘管開放的 API 設計（如同印度的 Aadhaar 的設計），就各種用途的互通性好處上，是受歡迎的，此技術特點，並不能保證整個系統的課責與信任。我們建議所有的國民身分系統都應開放原始碼。

▷ 可驗證之共融性，應為數位身分證系統設計的重心之一，任何違反此原則之相關實體，都應負起責任。例如：沒有人該因人口學特徵或身體特徵而受到排除。身分系統必須顧及不同族群的數位素養能力，也必須在低連線能力環境下保持穩定。每個人都不可因未持有特定身分證件，或系統無法運作，而無法使

用必要的服務。理想上，加上可自由使用替代的非數位身分證件，便可達成此目的。

- 所有人在使用自己的身分證件時，必須可以剔除特定類型的資料分享，特別是揭露時，可能會造成傷害的敏感資訊。

- 自專案的設計階段開始，政府須在身分系統的技術性、法律性和政策性選擇上，進行廣泛的諮詢。值得注意的是，在英國、法國及澳大利亞等已開發國家中，生物辨識身分系統，在諮詢階段遭遇到強烈的反對後，便在實行前止步。如此彰顯出，這些專案的設計階段之透明度與關注的重要性，方便公眾參與探討，除了如何實行這些系統的方式，還有要不要實行的問題。諮詢外部專家及受影響族群諮詢時，必須包含：

    - 在設計與範圍定義階段的建言，以理解將來的使用方式，包括評估邊緣化及高風險族群使用系統的相關顧慮。
    - 針對適用於系統的法律及政策框架的回饋。
    - 採購要求及採購流程的透明度。
    - 鑒於其中個人資料的敏感性，公開最終中選的執行身分專案之廠商。
    - 特別是在引入新功能或使用案例時，強化共融相關之公共課責義務。

儘管身分系統可賦予人民更大的能力，它也具有難以置信的濫用潛力，可能是無可制衡的監控、詳細剖析、社會排除、拒絕福利，甚至在某些不幸的案例中，導致死亡。在數位身分系統設計上，一連串技術性及政策性選擇，決定了該系統是賦能，抑或是剝削和排外。儘管有幾個組織，針對數位身分證發佈了相關原則，這些原則對於全球各地無止境地推廣數位身分，卻往往無法有效約束。開放性可作為引導和批判這些選擇的有效框架，同時確保身分系統以人民為優先。

Endnotes

1 Aadhaar Seeding Fiasco: How To Geo-Locate By Caste and Religion In Andhra Pradesh With One Click, Aman Sethi, Huffington Post India, 25 April 2018. Available at: https://www.huffingtonpost.in/2018/04/25/aadhaar-seeding-fiasco-how-to-geo-locate-every-minority-family-in-ap-with-one-click_a_23419643/

2 Vélez, Alejandro. "Insecure Identities. The Approval of a Biometric ID Card in Mexico." Surveillance & Society 10.1 (2012): 42-50.

3 Nadra-linked criminal database becomes operational, Munawer Azeem, Dawn, 29 July 2016. Available at: https://www.dawn.com/news/1273886

4 Government Defends Move To Make Aadhaar Mandatory For Mobile SIM Cards, Arpan Chaturvedi, BloombergQuint, 3 May 2018. Available at: https://www.bloombergquint.com/aadhaar/government-defends-move-to-make-aadhaar-mandatory-for-mobile-sim-cards

5 How private companies are using Aadhaar to try to deliver better services (but there's a catch), M Rajshekhar, The Wire, 22 December 2016. Available at: https://scroll.in/article/823274/how-private-companies-are-using-aadhaar-to-deliver-better-services-but-theres-a-catch

6 Why do you need Aadhaar to investigate a lost package?, Rachita Taneja, Mozilla Blog. Available at: https://blog.mozilla.org/netpolicy/2017/11/16/need-aadhaar-to-investigate-lost-package/

7 Justice K. S. Puttaswamy v Union of India - WP (C) 494/2012, Supreme Court of India. Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

8 Identification for Development Strategic Framework, World Bank, January 25, 2016. Available at: http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf

9 Identification for Development (ID4D), World Bank. Available at: https://id4d.worldbank.org/

10 Lyon, David. Identifying citizens: ID cards as surveillance. Polity, 2009.

11 It should be noted that in these countries the "photograph" a form of biometric has been part of identity documents like drivers licenses issued by the state for 50 years.

12 National Identification Cards: Why Does the ACLU Oppose a National I.D. System?, American Civil Liberties Union (ACLU). Available at: https://www.aclu.org/other/national-identification-cards-why-does-aclu-oppose-national-id-system

13 Success Story: Dismantling UK's Biometric ID Database, Electronic Frontier Foundation (EFF). Available at: https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database

14 National ID Cards, Canadian Internet Policy and Public Interest Clinic (CIPPIC), Available at: https://cippic.ca/en/national-id-cards

15 Biometric ID database found unconstitutional, European Digital Rights (EDRi). Available at: https://edri.org/edrigramnumber10-6french-biometric-database-unconstitutional/

16 Biometrics project scrapped after massive delays and budget blowouts, Matthew Doran, ABC News, 15 June 2018. Available at: https://www.abc.net.au/news/2018-06-15/biometrics-project-scrapped-after-delays-and-budget-blowouts/9876068

17 National digital identity programmes: what's next?, Access Now, 21 March 2018. Available at: https://www.accessnow.org/national-digital-identity-programmes-whats-next/

18 The Nail Finds a Hammer: Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World; Michael Graglia, Christopher Mellon, Tim Robustelli. Available at: https://www.newamerica.org/future-property-rights/reports/nail-finds-hammer/

19 ID4D Principles, World Bank. Available at: https://id4d.worldbank.org/principles

20 Identity in a Digital World: A new chapter in the social contract, World Economic Forum. Available at: https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract

21 See Note 17

22 The Laws of Identity, Kim Cameron, May 2005. Available at: https://www.identityblog.com/?p=352

23 The Path to Self-Sovereign Identity, Christopher Allen, 25 April 2016. Available at: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

24 See World Bank ID4D principles, Kim Cameron's Laws of Identity.

25 Vendor lock-in means there is only one vendor whose IDs work within the system and the government must exclusively source from that vendor going forward.

26 Reuben, William, and Flávia Carbonari. "Identification as a national priority: the unique case of Peru." Center for Global Development Working Paper 454 (2017).

27 For India's poorest, an Aadhaar card can be the difference between life and death, Mayank Bhardwaj, Reuters, 12 September 2018. Available at: https://in.reuters.com/article/india-election-starvation/for-indias-poorest-an-aadhaar-card-can-be-the-difference-between-life-and-death-idINKCN1LS0HO

28 Mozilla Statement on Recent Reports of Aadhaar Data Being Breached (again), Jochai Ben-Avie, 1 May 2018. Available at: https://blog.mozilla.org/netpolicy/2018/05/01/mozilla-statement-on-recent-reports-of-aadhaar-data-being-breached-again/

29 BC's Citizen Engagement: A Model for Future Programs, Kaliya "Identity Woman" Hamlin, re:ID, Spring 2017. Available at: https://identitywoman.net/wp-content/uploads/2011/09/reid_spring_14-BC.pdf

30 See Note 18

31 The Canadian Provincial Government work includes British Columbia which has the VonX project http://www.vonx.io and the Alberta Government Credential Ecosystem https://www.aceprogram.ca.

32 Currently being standardized at the W3C. See https://github.com/w3c-ccg/did-wg-charter for more information on formation of the Decentralized Identifier Working Group. The Verifiable Credential's Working Group has been working for 2 years and progressed to a candidate recommendation: https://www.w3.org/2017/vc/WG/

33 See Sarah Igo, the Known Citizen: A history of Privacy in Modern America, 2018

34 See cover story on The Atlantic in November 1967 was The National Data Bank; News Week Cover Is Privacy Dead, July 1970

35 Social Security Number Task Force, Social Security Administration, Report to the Commissioner (1971), Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973.

36 U.S. Department of Justice, United States Department of Justice Overview of the Privacy Act 1974, 2015 Edition, E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

37 Chapter 16: The Social Security Number. Personal Privacy in an Information Society, The Report of The Privacy Protection Study Commission, Personal Privacy in an Information Society, The Report of The Privacy Protection Study Commission, July 1977

38 'Government as a data model' What I learned in Estonia, Peter Herlihy, 31 October 2013. Available at: https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

39 Modular Open Source Identity Platform (MOSIP). Available at: https://www.mosip.io/

40 See Note 28

41 UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm - Rachna Khaira, Aman Sethi and Gopal Sathe, Huffington Post India, 11 September 2018. Available at: https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/

42 Ethnicity and Politicization In Kenya (2018), Kenya Human Rights Commission. Available at: https://www.khrc.or.ke/publications/183-ethnicity-and-politicization-in-kenya/file.html

43 Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India, Menaka Rao, Scroll, 17 November 2017. Available at: https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar

44 SC upholds Aadhaar as Money Bill: Here is what experts, govt said back then, Business Standard, 26 September 2018. Available at: https://www.business-standard.com/article/current-affairs/sc-upholds-aadhaar-as-money-bill-here-is-what-experts-govt-said-back-then-118092600734_1.html

45 Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process, The Centre for Intellectual Property and Information Technology Law; Dr. Robert Muthuri, Francis Monyango and Wanjiku Karanja. Available at: https://www.cipit.org/images/downloads/CIPIT-Elections-and-Biometrics-Report.pdf

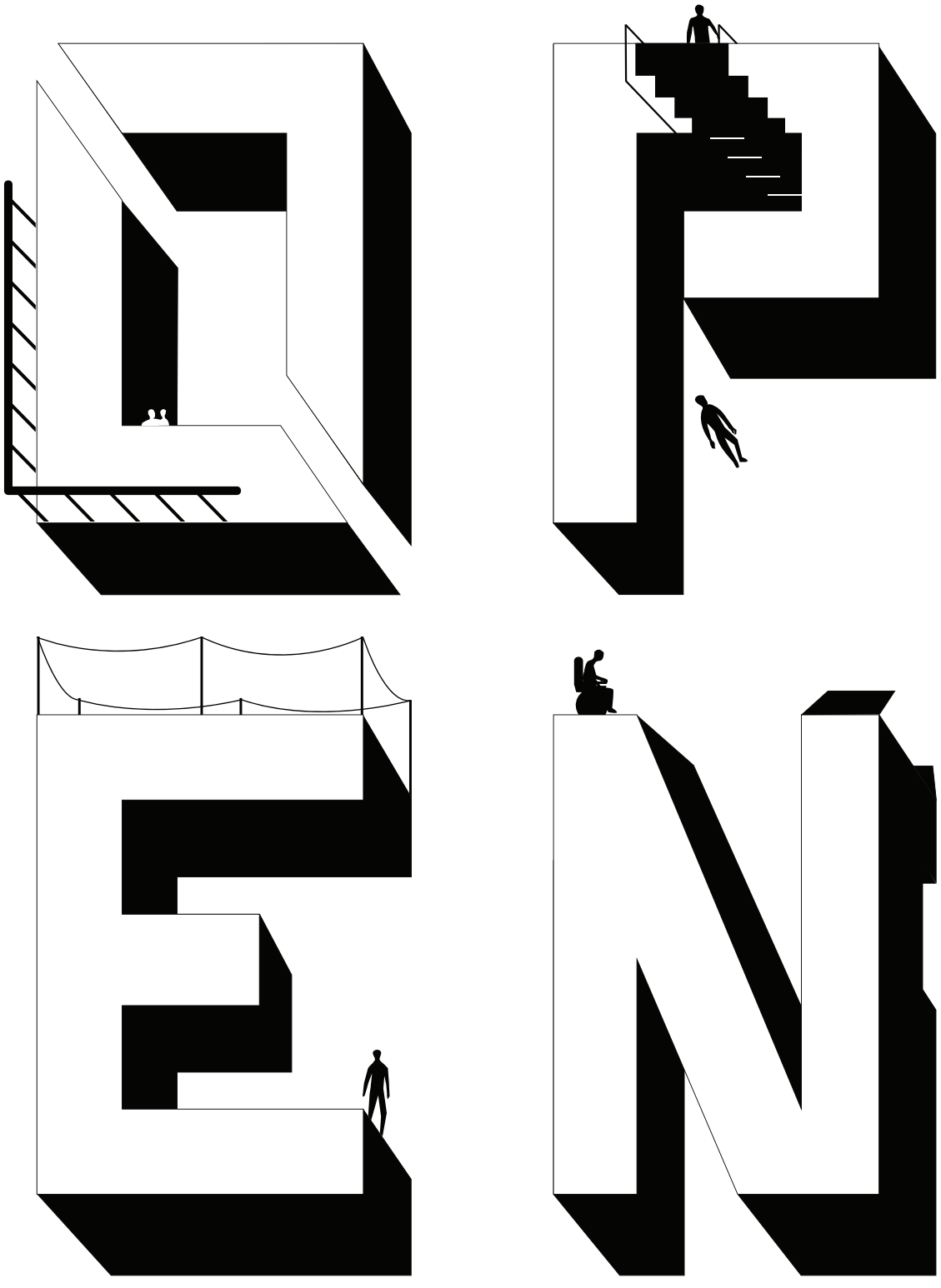
46 Did UIDAI share biometric data with its foreign vendors?, Sahil Makkar, Business Standard, 30 August 2017. Available at: https://www.business-standard.com/article/economy-policy/did-uidai-share-biometric-data-with-its-foreign-vendors-117083000682_1.html

47 See Appendix 1 Identity North Specialist Forum Proceedings https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/Appendix-I-Specialist-Forum-Report-v0225.pdf

48 Recommendation from the BC Services Card User-Panel. Final Report | December 2013 Prepared for the Ministry of Technology, Innovation and Citizens' Services https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/Appendix-II-Recommendations-from-BC-Services-Card-User-Panel.pdf

49 Digital Services Consultation Fall 2013, Ministers Response. British Columbia Ministry of Technology and Citizen Services, Published March 2014 https://engage.gov.bc.ca/app/uploads/sites/121/2017/02/DigitalServicesConsultation_report.pdf

選擇多樣化之開放
去中心化之開放
課責之開放
共融性之開放
透明及參與之開放



moz://a