InfoNetworks Response to Request for Comments
Department of Commerce, National Telecommunications and Information Administration

Developing the Administration's Approach to Consumer Privacy

I. Introduction

InfoNetworks appreciates the opportunity to provide this submission in response to the Department of Commerce ("DOC") and the National Telecommunications and Information Administration's ("NTIA") Request for Public Comments on Developing the Administration's Approach to Consumer Privacy.

Over the last two and half years, InfoNetworks has undertaken an in-depth, global analysis of regulatory approaches to consumer privacy, as it specifically relates to "digital identity" solutions and solutions for the exchange of personal data in online transactions. InfoNetworks has looked particularly closely at ecosystems where parties having "limited trust" with each other nevertheless have a common need to share certain transaction data (whether regulatory or commercially driven). In such ecosystems, we see significant potential benefits, for example, from the use of digital identity frameworks where personally identifying information is not transferred and aggregated with each provider in a traditional manner as part of certain transactions, but rather is itself validated and/or accessed on a transactional basis under an established set of rules. Such approaches provide significant adaptability and potential for lower risks for data breach with respect to conventional "centralized" models, which, in turn, can enable organizations to provide greater value to consumers as well as more adeptly balancing consumer privacy and commercial drivers with other considerations (such as national security and law enforcement needs, due process and evidentiary requirements, data residency and similar requirements), which may also vary across jurisdictional borders.

To put this in context, one example of such a "limited trust network" is ICANN's proposed Unified Access Model for Continued Access to Full WHOIS Data,[1] driven in large part by data privacy concerns under the European Union's General Data Protection Regulation ("GDPR"). For each top-level domain (e.g.,".INFO"), domain name registration and related services are typically offered by multiple Registrars that compete with one another and who each control access to the customer data that they collect—for competitive reasons, to prevent abuse of that data, for monetization, etc. These competitive Registrars must nevertheless collectively provide access to certain domain name registration data, such as for law enforcement, for intellectual property disputes, or other legitimate business reasons. The use of a federated system for accessing personal data associated with the domain name registrations will afford

[1] https://www.icann.org/news/blog/data-protection-privacy-update-seeking-community-feedback-on-proposed-unified-access-model.

these Registrars (many of which are smaller businesses with significant resource constraints) the ability to collectively reduce data protection costs and risks, greater flexibility in adapting data access to varying global requirements, and greater opportunity for innovating value-added services for their customers.

Based on our research in such ecosystems, InfoNetworks is providing the following comments for the NTIA's consideration.

II. The NTIA's Outcome Objectives

In its background to the Request for Comments, the NTIA notes that the United States has historically taken a sectorial, risk-based legislative approach to data privacy, certainly at the federal level and in large part among the states as well. This is in contrast to more comprehensive, rights-based privacy frameworks with implementing regulations that have been taken in the European Union and elsewhere. The United States shares common guiding principles with respect to consumer privacy, such as the *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* promulgated by the Organization for Economic Co-Operation and Development,[2] with those principles adapted to this risk-based approach under the U.S. Privacy Shield Framework[3] (and its Safe Harbor predecessor).

Against this backdrop, the NTIA has worked with other U.S. agencies within the Administration to in developing a voluntary risk-based Privacy Framework as an enterprise risk management tool for organizations. In developing this Privacy Framework, the NTIA is soliciting specific information for further consideration in achieving its proposed "user-centric privacy outcomes" that should underpin the protection provided by any Federal action on consumer-privacy policy and "high-level goals that describe the outlines of the ecosystem that should be created to provide those protections." As stated in the RPC, the NTIA's desire is to create "principle-based" approaches to data privacy that are focused on "the outcomes of organizational practices, rather than on dictating what those practices should be." These would be operationalized through a risk-management approach that affords organizations flexibility and innovation in how to achieve these outcomes.

The NTIA's approach is guided by the understanding that protecting both privacy and innovation requires balancing flexibility with the need for legal clarity and strong consumer protections, such as through solutions that yield "a reasonably informed user, empowered to meaningfully express privacy preference," as well as "products and services that are inherently designed with appropriate privacy

[2] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[3] https://www.privacyshield.gov/welcome.

protections, particularly in business contexts in which relying on user intervention may be insufficient to manage privacy risks."

Based on our study of various approaches to consumer privacy in data sharing ecosystems, InfoNetworks wishes to highlight some additional considerations for this outcome-driven Privacy Framework:

- The benefits of NTIA led coordination of consumer privacy efforts among both U.S. and non-U.S. agencies in regard to uses of digital identities solutions on the Internet
- The benefits of the U.S. government fostering private-public partnerships in regard to free-market driven digital identity solutions to advance public interest and innovation for consumer privacy
- The opportunity for innovation and adaptability afforded by fostering federated and decentralized digital identity solutions that provide controls for use of personal data on a transactional basis, as opposed to the constrictions created through reliance on predetermined universal privacy settings
- The opportunity for innovation and adaptability afforded by privacy solutions that incorporate established rules governing access to personal data
- The benefits of well-defined privacy "safe harbors" for digital identity providers to spur greater adoption across a diverse range of market places
- The benefits to consumer privacy for solutions that appropriately delineate protections as between natural and legal persons

These considerations are illustrated below in the discussion of some specific examples.

III. Discussion

A. NTIA-Led Coordination of Efforts in Certain Areas of Consumer Privacy.

With an increasingly global online marketplace, it is critical that the United States take a tightly coordinated approach to both the national and international aspects of consumer privacy online for U.S. consumers and businesses. There needs to be continued coordination among various government agencies at the federal and state level, and with non-U.S. agencies to effectively tackle the complex issue of consumer privacy. But we note particularly that the NTIA's interest in driving outcome-driven approaches to consumer privacy may be well-served by the NTIA taking a lead coordination role with respect to consumer privacy in certain key areas.

The NTIA has been the lead agency to coordinate unified responses on behalf of the United States government in connection with issues involving ICANN and broader International Internet Policy.[4] With the publication and use of DNS data being a significant area of inquiry by the European Data Protection Board with respect to the GDPR, NTIA may wish to undertake a similar coordination role with respect to

[4] https://www.ntia.doc.gov/federal-register-notice/2018/comments-international-internet-policy-priorities.

other aspects of Internet-related consumer privacy as well—such as in regard to the evolution of digital identity solutions.

To underscore this point, this RPC is being coordinated by the NTIA under the authority of the Department of Commerce, yet there are also several key points of intersection between this RPC and the Treasury Department's recent report on economic opportunities arising from innovation in the financial sector.[5] While the Treasury Department's report did not focus on consumer privacy *per se*, it did consider the fundamental role that the evolution of digital identity technologies will have in driving economic growth, and the pivotal role of a comprehensive consumer privacy framework in that context intersects directly with the NTIA's outcome-driven approach to its proposed Privacy Framework.

B. Federated and Decentralized Digital Identity Solutions

The principle of empowering consumers with more direct control over the use of their personal data was recently enshrined in *A Contract for the Web*, an initiative by Tim Berners-Lee to promote core principles that governments, companies and citizens could adopt to protect the open web as a public good and a basic right.[6] To date over fifty companies, including Google and Facebook, and the French government have signed this contract. One of the core principles enumerated for companies was the right to respect consumers' privacy and personal data. In discussing this principle in greater detail, Berners-Lee noted that "The idea of control over your own data is not just about me being my own silo, locking everything away. … It's actually having the joy of being able to share it with whoever."[7]

With traditional centralized digital identity solutions (really access authentication systems), each service provider relative to a transaction holds all of an individual's personal data in their data sources and each service provider separately manages (and is separately responsible for) that individual's personal data in their possession. However, technologies that first developed for federated access authentication (such as single-sign-on solutions) are expanding into digital identity solutions that incorporated federated management of personal data by Identity Providers under the concept of Identity as a Service ("IDaaS").

These IDaaS solutions are further evolving to incorporate the ability for consumers to retain more direct control over the use of their personal data and the ability to make individual, contextual determinations in regard to who has access to their data, for how long and under what circumstances. InfoNetworks believes

---

[5] See *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, a report authored by Treasury Secretary Steve Mnuchin and Counselor to the Secretary C Craig S. Phillips in response to President Trump's Executive Order 13772 on Core Principles for Regulating the United States Financial System. https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

[6] https://contractfortheweb.org/.

[7] https://www.cnn.com/2018/11/05/tech/tim-berners-lee-contract/index.html.

these federated digital identity approaches are not only more robust and scalable solutions, but also provide potentially significant benefits in reducing data protection costs and in mitigating data breaches.

There are several technological approaches to federated identity. Some solutions incorporate an extension of OAuth / OpenID, which leverages existing, well-tested technology that has previously been reliably deployed at scale. An initiative within the domain name space illustrating a use of this is ID4me.[8] This initiative, which was original conceived within the German domain name community, looks to leverage OAuth / OpenID and the discovery services of the traditional domain name system.

Another, more nascent, technical approach is distributed ledger technology ("DLT") or "blockchain." The W3C currently has a Decentralized Identifiers (DID) Community Group that is evaluating a new form of identifier and data model for digital identity, under which personal data is further decentralized—it remains primarily under control of the individual themselves, substantially independent of any centralized registry, identity provider, or trusted authority. The use of DLT in connection with decentralized identifier based digital identity is being explored by a number of organizations, such as Uport (Consensys), Sovrin, and Veres.One.[9] In connection with the previous recommendation regarding fostering inter-agency collaboration within the USG, it should be noted that the United States Department of Homeland Security's Science and Technology Directorate have funded some portions of DID specification under contracts HSHQDC-16-R00012-H-SB2016-1-002 and HSHQDC-17-C-00019.[10]

One other approach worth noting is Solid,[11] a project led by Tim Berners-Lee. The Solid approach employs conventional technology of the world wide web (HTTP, REST, HTML) and WebID, combined with a personal data architecture incorporating data "pods" for the retention or portability of personal information.

All of these non-centralized approaches share the common feature that personal data can be segregated from transactions in which it is used, so that access to and use of that personal data can be controlled more granularly, more uniformly, and without undue proliferation of that personal data across data sources across the Internet. A significant concern with traditional centralized management of personal data is also that it results in "honey pots" that may become high-profile targets for hackers and other

[8] https://id4me.org.
[9] See Uport website (https://www.uport.me), Sovrin website (https://sovrin.org/) and Veres.One website (https://veres.one/)
[10] See https://w3c-ccg.github.io/did-spec/ "Status of this Document"
[11] https://solid.inrupt.com.

criminal activity. According to a recent report by Gemalto's Breach Level Index, over 4.5 billion records were compromised in the first half of 2018.[12]

User frustration with countless user IDs and passwords combined with rampant phishing have also made centralized networks much less secure. To further limit this threat vector, federated digital identity solutions naturally incorporate multi-factor authentication and lend themselves to use in connection with mobile devices that incorporate biometric authentication—such as envisioned by NIST 800-63 Digital Identity Guidelines[13] and by FIDO.[14]

With traditional centralized approaches to data protection, organizations impacted by data breaches have suffered significant reputational harm, potential fines and legal liability, and impacted consumers have been harmed by having their personal data bartered on the dark web and otherwise misused. InfoNetworks believes that federated identity frameworks not only empower consumers to be the ultimate guardian of their data, but also provide better opportunity for organizations to come together to collectively reduce the risks (and costs) inherent with centralized aggregation of, and separate management of, personal data, and to better innovate value-added services for their respective customers.

C. Public-Private Partnerships to Foster Digital Identity Solutions

The NTIA may also wish to consider the comprehensive public-private partnership approach to digital identity being promulgated by the Australian Digital Transformative Agency (DTA). The DTA has invested substantial time and resources in connection with its national digital initiative (myGovID), which co-exists within a complex consumer privacy legal landscape that involves a commonwealth government, six state governments, and two territories. The public-private framework that Australia has proposed incorporates several discrete actors: Identity Providers (IdP); Attribute Providers (AP); Identity Exchanges (IdX); and Relying Parties. This eco-system allows the individuals to retain control over their data and the through the use of Identity Exchanges—the government does not know what services a myGovID user is accessing; i.e., it is a "double blind" exchange. This eco-system provides a series of checks and balances to minimize any potential abuse by one or more actors.

The benefits of fostering public-private partnerships for digital identity was also discussed in the U.S. Treasury Report:

> Both the government and the private sector have important roles in establishing a trustworthy U.S. digital identity ecosystem. In the United States, the private sector is generally relied upon to develop innovative identity products, services, and business models, while the federal government is

[12] https://breachlevelindex.com/.
[13] https://pages.nist.gov/800-63-3/.
[14] https://fidoalliance.org.

> ultimately responsible for establishing the minimum substantive requirements for proving legal identity, including core attributes and acceptable attribute evidence. Federal and state government authorities also provide the official government registration and the related official root identity evidence (e.g., birth certificates, passports) on which legal identity currently depends.

Recognizing that the United States private sector was a primary economic driver behind the initial commercialization of the Internet, the U.S. government should be looking to provide a regulatory framework where the private sector can innovate and bring to market new services that consumers want, as opposed to top-down solutions imposed upon them by the government.

D. Free-Market Approaches to Public-Private Partnerships for Federated Digital Identities

Outcome-driven privacy solutions should also foster innovation and economic growth through a vibrant free market system where consumers and businesses should be able to have choice between which providers they use (IdP, IdX, CSP, etc.). There are several examples of public-private partnerships for digital identity that been put forth in other countries to foster free-market information.

In the Netherlands, the banking community has worked over the past several years in creating a joint infrastructure that has issued over 3.9 million BankIDs.[15] These BankID digital identities are now used by consumers in the Netherlands to access all the country's banks, public digital services and an increasing number of other enterprise services. This approach to digital identity and the potential innovation it can generate was specifically mention in Secretary Mnuchin's Treasury's report:

> Digital identity products and services hold promise for improving the trustworthiness, security, privacy, and convenience of identifying individuals and entities, thereby strengthening the processes critical to the movement of funds, goods, and data as the global economy races deeper into the digital age. Digital identity systems also have the potential to generate cost savings and efficiencies for financial services firms. For instance, trustworthy digital identity systems could improve customer identification and verification for onboarding and authorizing account access, general risk management, and antifraud measures.

The United Kingdom implemented UK.GOV Verify, a federated digital identity framework in which the British government has accredited numerous private and public entities (e.g. Barclays, Experian, the U.K. Post Office, and others) to serve as federated Identity Providers across a range of government services. Individuals may obtain their digital identity from the list of accredited Identity Providers, for use in accessing these government services.[16]

The NTIA may also consider the effort the Danish Internet Forum (DIPO), the non-profit organization which oversees DK Hostmaster, the registry for Denmark's .dk ccTLD, undertook to enhance online trust

[15] https://www.bankid.no/en/company/.
[16] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

and consumer confidence by minimizing the trafficking of counterfeit goods and services. In response to an increased trend of .DK domain names being used as a platform for Intellectual Property Rights (IPR) violations in connection with fake e-commerce websites, DIPO implemented several changes to its registry operations. Specifically, DK Hostmaster began verifying .DK Registrants at the time of registration using eID for all Danish customers (both natural and legal) and a separate risk- based assessment for all foreign registrants.

As a result of this program the number of e-commerce websites within the .DK zone engaged in IPR violations went from 0.28% (Nov 2017) to 0.0%, (June 2018), whereas as general websites within the .DK zone suspected of IPR violations went from 6.73% (Nov 2017) to 0.12% (June 2018). Interestingly, notwithstanding the implementation of GDPR in Europe, DK Hostmaster still maintains a public Whois database relying upon the national Domain Names Act that requires them to publish the name, address and telephone number of all registrants.[17] In recognition of their efforts to ensuring citizen safety by maintaining transparent WHOIS data, proactively enforcing identity accuracy policies to increase consumer trust and safety online, DK Hostmater was awarded the annual Internet Pharmacy Safety E-Commerce Leadership Award by the nonprofit Alliance for Safe Online Pharmacies (ASOP Global) at the recent ICANN regional meeting in Barcelona.[18]

E. Managed Access to Personal Data in Federated Digital Identity Solutions

While the Australian framework limits the government's access to underlying transactional data through the use of Identity Exchanges (that are double blind), there are considerations under which Relying Parties may have a legal right access to the Identity Exchange personal data of a consumer, such as to investigate identity fraud or suspicious transactions, for law enforcement investigations, national security reasons, or legal disputes.

In 2016, InfoNetworks submitted a white paper to the United Nations Office for Project Services (UNOPS) in connection with their Request for Comment in connection with a digital identity framework utilizing DLT.[19] While the first part of this white paper focused on the specific technical capabilities of DLT, the primary focus of the paper was on the need for an appropriate private-public governance model for digital identity solutions, particularly as used internationally. One of the key drivers of this was the need for appropriate due process and other access safeguards in connection with cross broader disputes. At that time, InfoNetworks noted that any "governance model also must be trusted to satisfy the

[17] https://www.dk-hostmaster.dk/en/node/473.
[18] http://www.circleid.com/posts/20181023_dk_hostmaster_wins_award_for_transparency_and_trust_online/.
[19] https://www.infonetworks.global/papers/InfoNetworks_UNOPS_RFI_submission.pdf.

respective due process rights of citizens of different sovereignties when transacting internationally, while—at the same time—precluding any sovereign government from exceeding the bounds of its sovereignty."

Another important aspect in the white paper submitted by InfoNetworks was the recognition that the "legal and political challenges in governance of digital identities [would] be better addressed through an appropriate public-private framework." We continue to believe this principle remains the optimal path forward and is consistent with the Treasury Report as discussed elsewhere in these comments.

Similarly, we believe that a key principle for the development of privacy solutions by U.S. organizations is the extent to it which protects U.S. consumers transacting business abroad as well as within the U.S., much like the European Union has incorporated extraterritorial provisions into the GDPR. One approach to this in the context of federated digital identity solutions, is the pseudonymization of transaction data (particularly data that may be shared in an ecosystem of providers—such as the WHOIS example provided in the introduction to these comments).

Under this approach, personal data for parties to a relevant transaction may be segregated (such as using a federated or decentralized digital identity solution) and access to, or validation of, this personal data may be managed on a transactional basis under an established set of rules that comport with various legal constraints (e.g., due process, data residency laws, differing data protection laws) and commercial constraints (e.g., value-added data services, consumer reward programs, risk allocation terms among providers in the ecosystem).

F. The Distinction Between Natural and Legal Persons

Many consumer privacy frameworks outside of the United States, such as the GDPR, extend protection to natural persons only. It is important that U.S. consumer privacy solutions consider the differences between the protections necessary for natural persons and for legal persons. To illustrate, ICANN's implementation of the Temporary Specification has an overly broad data protection construction that permits a Registrar to restrict third parties with a legitimate interest from accessing registrant directory data associated with legal person registrants.

In seeking to help establish the appropriate balance as to the rights of natural persons versus legal persons in outcome driven solutions, organizations might consider how some generic and country code top-level domains have operationalized this distinction. For example, the Registry Operator for .NYC has implemented an EPP code that requires Registrants at the time of registration to designate their Nexus requirement within that TLD as either an Individual (IND) or an Organization (ORG). The Registry

Operator of the .CAT TLD implemented a similar EPP code that permits the Registrant to designate themselves as either a natural person or a legal person. However, the .CAT Registry Operator has also implemented an additional EPP code that permits a natural person to either consent or withhold consent to having their Registrant Data published.

There are a couple of other additional notable points in regard to the .CAT implementation. First, if a Registrant designates themselves as a natural person but uses the domain name in connection with commercial activity, the .CAT policy requires that the Registrant Data be published. In the situation where a natural person registers a domain name and withholds consent for publication, but nevertheless uses the domain name in commercial activity in violation of the .CAT policy, the Registry Operator as part of their compliance activity can switch the consent flag off, forcing the Registrant Data to be published. This policy was implemented by the Registry Operator after consultation with the Spanish Data Protection Agency (DPA) and was approved by the ICANN Board.

A growing number of Country Code TLD Managers are implementing the distinction between natural and legal persons into their business practices. In some cases, this distinction involves the provisioning of government issued identification numbers or digital identities, which permit the authentication of the Registrant and any representations they are making.

G. Well-Defined Safe Harbors to Foster Nascent Digital Identity Solutions

The U.S. government should consider legislation that provides a liability "safe harbor" for nascent / emerging digital identity services. The Treasury Report specifically recognizes there should be "business models and liability allocation appropriate for establishing portable legal identity" and that the "U.S. market would be well served by a solution developed in concert with the private sector that addresses data sharing, standardization, security, and liability issues."

It may also be useful to consider the "safe harbor" provision that was incorporated into the Anti-Cybersquatting Consumer Protection Act (ACPA) back in 1999. The ACPA amended the Lanham Act in connection with trademark infringement involving domain names to exempt domain name registration authorities from financial liability for damages where they had implemented a reasonable policy preventing the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark. This safe harbor was critical in providing business certainty to the fledgling domain name industry which has now evolved into a multi-billion dollar business.

Similarly, following the 9/11 attacks, Congress passed the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, 6 U.S.C. §§ 441-444 (the "SAFETY Act"). The SAFETY Act created liability

limitations for claims resulting from an act of terrorism where Qualified Anti-Terrorism Technologies (QATTs) have been deployed. To date the Department of Homeland Security has approved hundreds of technologies, including several that deal with verification of digital identities. These safe harbor provisions provided for in the SAFETY Act and the ACPA, highlight the need for the USG to provide a safe harbor for emerging technologies and business models.

IV. Conclusion

InfoNetworks appreciates the opportunity to provide these comments to assist the NTIA and the DOC in considering new approaches to digital identity solutions and the benefits of those approaches in fostering a risk-based Privacy Framework and an enterprise risk management tools for organizations. We appreciate the government's outreach on these important issues and would welcome the opportunity to work with NTIA and the DOC in considering how best to address the benefits and challenges for digital identities and consumer privacy in the future.

Respectfully submitted,

/s/ Michael D. Palage

Michael D. Palage

InfoNetworks, Inc.
601 Heritage Drive, Suite 462
Jupiter, FL 33458
USA
+1 561 747 7820
9-November-2018