POLICY BRIEFS SERIES

Deploying the Once-Only Policy

A Privacy-Enhancing Guide for Policymakers and Civil Society Actors

Naeha Rashid
David Eaves, *Series Editor*

NOVEMBER 2020

HARVARD Kennedy School
ASH CENTER
for Democratic Governance
and Innovation

POLICY BRIEFS SERIES

Deploying the Once-Only Policy

A Privacy-Enhancing Guide for Policymakers and Civil Society Actors

Naeha Rashid
David Eaves, *Series Editor*

NOVEMBER 2020

A PUBLICATION OF THE

Ash Center for Democratic Governance and Innovation
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

617-495-0557
ash.harvard.edu

About the Ash Center

The Roy and Lila Ash Center for Democratic Governance and Innovation advances excellence and innovation in governance and public policy through research, education, and public discussion. By training the very best leaders, developing powerful new ideas, and disseminating innovative solutions and institutional reforms, the Center's goal is to meet the profound challenges facing the world's citizens. The Ford Foundation is a founding donor of the Center. Additional information about the Ash Center is available at ash.harvard.edu.

This research paper is one in a series published by the Ash Center for Democratic Governance and Innovation at Harvard University's John F. Kennedy School of Government. The views expressed in the Ash Center Policy Briefs Series are those of the author(s) and do not necessarily reflect those of the John F. Kennedy School of Government or of Harvard University. The papers in this series are intended to elicit feedback and to encourage debate on important public policy challenges.

About the Author

Naeha Rashid has worked at the intersection of financial inclusion, social entrepreneurship, and technology for the last several years. She is passionate about leveraging technology solutions to improve the quality and character of people's lives. While a 2019–20 digital governance fellow at Harvard Kennedy School's Ash Center, Rashid analyzed issues related to technology and innovation in government. Previously, Rashid worked for CGAP—a member of the World Bank Group—leading her team's work in Pakistan to catalyze innovation and scaling of digital financial services. She was also a core member of the start-up team for Karandaaz Pakistan, an organization funded by the Bill and Melinda Gates Foundation. Rashid holds a Master in Public Policy from Harvard Kennedy School and undergraduate dual degrees in International Development (honors) and Economics from McGill University. Find her online.

About the Series Editor

David Eaves is a lecturer of Public Policy at the Harvard Kennedy School where he teaches on digital transformation in Government. In 2009, as an adviser to the Office of the Mayor of Vancouver, David proposed and helped draft the Open Motion which created one of the first open data portals in Canada and the world. He subsequently advised the Canadian government on its open data strategy where his parliamentary committee testimony laid out the core policy structure that has guided multiple governments approach to the issue. He has gone on to work with numerous local, state, and national governments advising on technology and policy issues, including sitting on Ontario's Open Government Engagement Team in 2014–2015.

In addition to working with government officials, Eaves served as the first Director of Education for Code for America—training each cohort of fellows for their work with cities. Eaves has also worked with 18F and the Presidential Innovation Fellows at the White House providing training and support.

Acknowledgments

Financial support for this paper was provided by the Council of Arab Economic Unity (CAEU) of the League of Arab States. The CAEU was not involved in the research required
to prepare this report and had no role in shaping the findings presented.

I am deeply grateful to my advisor, Harvard Kennedy School lecturer of public policy David Eaves, for giving me the freedom to immerse myself in the world of digital government this past year. Without his unfailing support and weekly guidance, the end result would have been far poorer.

Thank you to all the public servants who took time out of their busy work and family schedules multiple times—both pre and post the global pandemic—to give me the benefit of their knowledge and experience. Specific thanks to Teresa D'Andrea, director general for digital enablement at the Treasury Board of Canada Secretariat; Felicity Hitchcock, product manager for Tell Us Once and Platforms in Australia's Digital Transformation Agency; Diane Leggo, former head of Tell Us Once Delivery Partnerships in the United Kingdom's Department for Work and Pensions; and Wouter Welling, coordinating policy officer for the Netherlands' Ministry of the Interior and Kingdom Relations. My conversations with them strengthened this project immeasurably.

Finally, thank you to the many individuals who slogged through dozens of pages of material to provide invaluable feedback on multiple versions of this work, including Lauren Lombardo, Nagela Nakuna, Nicolas Diaz Amigo, Blanka Soulava, Angelo Mikael, Westerley Gorayeb, Michael McKenna Miller, Emily Rapp, Imara Salas, and Tommaso Cariati.

Overview

The once-only policy (OOP)[1] is increasingly seen by some digital government experts as central to establishing a national digital government strategy and as a gateway to next-generation government services. Once-only is so called because users (citizens, residents, and businesses) have to provide diverse data only one time when in contact with public administrations; after the initial data transfer, different parts of government can internally share and reuse this data to create public value and better service for users.

Members of the digital government community are excited by the potential of OOPs to create public value and reduce the cost of government, and I want to help governments harness this potential. I am also deeply concerned by the potential for OOPs to concentrate and increase state power and the negative impact this could have on individuals' privacy, freedoms, and capacity to dissent.

The goal is to harness the benefits of OOP while minimizing the risks, to create a world in which the power of the state is counterbalanced by the power of its citizenry. This document outlines the key policy questions and concerns that must be addressed by governments intending to implement an OOP. It is designed to help stakeholders—including policymakers in government and interested parties in civil society—ask key questions during the development of OOP-facilitating infrastructure, specifically **identity- and data-sharing mechanisms**, and the development of OOP strategy.

This document is not to intended to encourage or prescribe a specific pathway of development, but to consolidate and present a compendium of the key considerations at each stage. This work is based on an extensive literature review across the areas of privacy, identification, data sharing, and OOP; interviews with experts in the field; and mini case studies highlighting different lessons of implementation from five countries—the Netherlands, Estonia, the UK, Canada, and Australia—with diverse approaches and at very different stages of OOP maturity.

I believe this work will be valuable for:

- Policymakers who are considering deploying OOP within their own contexts and would find it useful to see a general roadmap for both its underlying infrastructure and the policy itself;
- Policymakers who are just beginning to explore digital identification and data-sharing arrangements in government, and who would like to understand and counter the major criticisms against these systems; and,
- Civil society actors who are concerned about the privacy implications of advanced data sharing within their countries and want to help keep the government accountable as these systems are designed and implemented.

[1] I am calling it the once-only policy as opposed to the once-only principle because I believe that the latter denotes a specific approach (see *Chapter 2*).

Contents

1. Introduction

Imagine a world in which online forms for interacting with governments are pre-completed with all the correct information or where governments automatically initiate services—say sending you a baby bonus check after your child is born—without any forms or requests at all. Further, imagine that this user-centric approach actually streamlines internal government processes and creates savings for both the state and taxpayers alike. This world is within reach with the aptly named once-only policy.

With OOP in place:

- Citizens of the Netherlands can apply for government certificates, benefits, and other services at the push of a button simply by using their national ID.
- In Estonia, residents, their doctors, and appointed representatives can access their entire health history by logging into the e-patient portal using their digital ID.
- UK residents can inform all necessary departments across central and local governments of a birth or death by opting into the service offered by the Department for Work and Pensions online, over the phone, or in person.

These examples are the result of almost two decades of experimentation with OOP across Europe. More than a dozen other countries, including Canada and Australia, are considering OOP implementations.

1.1 What Is Once-Only Policy?

Under OOP, users (citizens, residents, and businesses) **provide diverse data only once when in contact with public administrations**. Beyond the initial data transfer—assuming that consent is explicitly given—departments across all tiers of government (national, provincial, and local) can then share and reuse that data to create public value and better service the user.[2]

While OOP is a combination of technical implementation, standards, and policy, it is **predicated upon the existence of two key systems: an identification mechanism and a seamless data-sharing mechanism**.

An identification mechanism is predicated upon either one or many unique identifiers that allow individuals to be distinctly identified within a system. An identification mechanism is a base facilitator for advanced data sharing in government. The most common kind of identification mechanism is a foundational unique identifier such as a national ID. By contrast, a data-sharing mechanism encompasses the technical and policy standards that must be in place to allow information about unique individuals to be shared across all levels of government.

1.2 The Opportunity: Why You Would Implement OOP

OOP's **goal is to reduce the administrative burden for both users and governments.**[3] Users are disburdened because they must communicate diverse fields of data only once instead of being forced to repeatedly provide the

[2] TOOP, "Once-Only: TOOP.EU," accessed August 7, 2019, http://toop.eu/once-only. Note that to make OOP possible, data does not have to be centralized, as long as it is accessible and can be used across multiple departments. Different models of data storage and exchange, including centralization, are described in *Chapter 5*.

[3] European Commission, "EU-Wide digital Once-Only Principle for citizens and businesses—Policy options and their impacts," Shaping Europe's digital future, February 1, 2017, https://ec.europa.eu/digital-single-market/en/news/eu-wide-digital-once-only-principle-citizens-and-businesses-policy-options-and-their-impacts.

same information to multiple actors. Governments are disburdened because it is easier and cheaper for departments to exchange data that has already been collected than to make multiple requests for the same data and store the same data over and over in various silos. In the EU, where OOP is a component of the digital single-market strategy, OOP is expected to create a net savings of approximately 5 billion euros annually through disburdening alone.[4] **However, the true benefits of OOP go far beyond simple administrative improvements that enhance convenience and efficiency**.

When done right, OOP has the potential to fundamentally transform government operations. This is because OOP implementation necessitates the development and use of its underlying elements—identity- and data-sharing mechanisms—across multiple layers of government. Subsequently, these elements can be leveraged for any number of additional purposes. Thus, OOP is not a stand-alone policy but **fits into the broader conversation about government digitization, particularly Government as a Platform** (GaaP). In fact, though OOP is often sold to the public as merely user-centric, it can also be a way of helping governments make the transition to GaaP.

GaaP is considered the foundation for next-generation public services, and it goes far beyond simple digitization. Instead of merely changing the primary medium of interface between government and citizens from paper to digital, GaaP aims to transform the fundamental purpose of government from a system that delivers outputs in exchange for inputs into a "convener and an enabler" and a "vehicle for coordinating the collective action of citizens."[5] While there is no universally accepted definition of GaaP, I like the working definition proposed by former Kennedy School senior fellow Richard Pope: "Reorganizing the work of government around a network of shared APIs [application programming interfaces] and components, open-standards and canonical datasets, so that civil servants, businesses and others can deliver radically better services to the public, more safely, efficiently and accountably."[6] **With OOP and its underlying elements in place, several GaaP goals are realized, especially in the following areas:**[7]

- **Service delivery:** Because OOP is fundamentally about user centricity, it can transform service delivery by aligning supply of services with demand for services both in terms of method (how government services are accessed and delivered) and form (the type of government services that are offered).
- **Data and information:** The data-related requirements under OOP mean that reliable data would be made more accessible to government servants, thereby making data-driven decisions much easier.
- **Platform governance:** OOP creates a technical basis for advanced interoperability and the development of platform services across government.
- **Government modernization:** With a successful OOP deployment in place, orienting governments to becoming more digital, adaptable, and transparent will become easier.

[4] "EU-Wide digital Once-Only Principle for citizens and businesses."
[5] Tim O'Reilly, "Gov 2.0: The Promise Of Innovation," Forbes, August 10, 2009, https://www.forbes.com/2009/08/10/government-internet-software-technology-breakthroughs-oreilly.html.
[6] Richard Pope, "A Working Definition of Government as a Platform," Medium, July 29, 2019, https://medium.com/digitalhks/a-working-definition-of-government-as-a-platform-1fa6ff2f8e8d.
[7] Inspired by Jamie Boyd's remarks at "The Future of Digital Governance in a Post-Pandemic World," Policy Crunch, Institute on Governance, May 5, 2020, https://www.youtube.com/watch?v=ySrjliVqCRc&feature=youtu.be&t=1277s.

Table 1: Summary of OOP benefits to users and government

	Benefits to users	Benefits to government
Basic benefits of OOP	• More consistent user experience • Time savings • Cost savings • Reduction of frustration and stress	• Optimized internal government processes • Increased efficiency (lower costs and higher effectiveness) • Improved fraud prevention
Additional benefits of OOP related to GaaP	• Improved service delivery • Better availability and use of data and information • Platform governance • Changing how government works	

1.3 The Challenge: Why You Wouldn't Do It

There are serious privacy and security implications that need to be reckoned with regarding OOP implementation.

Even as OOP and its underlying elements create new opportunities to transform how government operates, **they also create additional risks related to government use of people's personal data, making data easily accessible, and keeping institutions accountable.**[8] These risks stem from the fact that OOP gives governments the ability to stitch together sensitive information about an individual and conclusively link it to a single profile, thus making users permanently visible to and trackable by the government. At an aggregate level, such enhanced state capabilities can be used to influence and control entire populations. In the absence of meaningful controls, OOP can create structures that are ripe for exploitation and abuse to the detriment of freedoms and democracies. This is deeply concerning for nations that have poor accountability track records, and it creates new risks for even relatively responsible regimes.

However, these privacy and security risks do not mean that OOP is inherently harmful, simply that **the power OOP grants the state must be shackled by enshrining privacy and security protections proactively throughout the design of all interlinked policies and systems, and by giving civil society actors the knowledge they need to advocate for "good" design**. In this case "good" means established with individual consent, protecting user privacy, and ensuring people control over their own personal data.[9]

Though security and privacy go hand in hand, the **privacy tradeoff is of particular concern** to me and is a focus of this paper. Not only does privacy have huge potential ramifications for public trust and safety, but it is also significantly exacerbated by technologies that are fundamentally rooted in people's personal data. **Understanding how to ethically use personal data to advance service delivery while creating sufficient protections for individuals is a core challenge for all governments in the 21st century**.

---

[8] Richard Pope, "Government as a Platform, the hard problems: part 5—identity and trust," blog, August 5, 2019, https://medium.com/@richardjpope/government-as-a-platform-the-hard-problems-part-5-identity-and-trust-575a13e8c255.

[9] My ideas of good design derive from the investment firm Omidyar's definition of "Good ID." For more information see "Omidyar Network Unpacks Good ID: An Update to Our Point of View on Digital Identity," May 16, 2019, https://omidyar.com/omidyar-network-unpacks-good-id-update-our-point-view-digital-identity/.

1.4 Purpose of this Paper: A Proposal to Minimize the Challenges

To capture the benefits and manage the risks outlined above, this paper examines how a privacy-enhancing OOP deployment can be achieved and shows how **the full enabling ecosystem—the key underlying elements ending with the OOP policy itself—can be optimized and responsibly built** (see Figure 1).

Chapter 2 provides a grounding in OOP basics, specifically exploring OOP variants and highlighting the in-country conditions that disallow all-of-government OOP implementation.

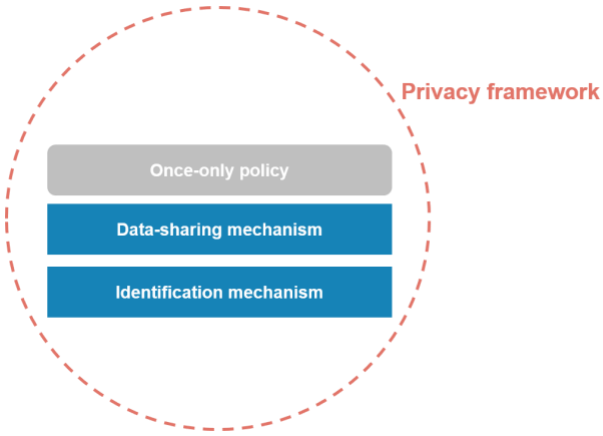
Chapter 3 delves deeper into the topic of privacy as a necessary prerequisite to a successful OOP deployment, showing how the unique privacy threats created by government use of personal data can be identified and addressed through a multimodal privacy framework.

Chapter 4 unpacks the concept of identification mechanisms—the key that unlocks all other data and data-sharing functions in government—as they relate to OOP, discusses various manifestations of these mechanisms, and outlines the pros and cons of each.

Chapter 5 takes readers through the data-sharing mechanism that creates the rules and rails for data collection, storage, and exchange.

Finally, *Chapter 6* discusses how countries can successfully operationalize an OOP policy in their own contexts.

Figure 1: The enabling ecosystem for the once-only policy



Throughout the discussion of the enabling ecosystem, I will examine the consequential decisions that governments make along the way and the outstanding questions that exist at each stage. I **see this paper as a guiding document** for governments and civil society organizations in countries that are either considering or in the midst of implementing a once-only policy arrangement. I believe this document will also be valuable to stakeholders in countries that are more generally exploring unique identifiers and data-sharing mechanisms with a privacy lens.

This document is distinct from previous research efforts in the OOP space in the following ways:

- **It situates OOP within a broader system**. While there is research on OOP benefits, barriers, and requirements, there is less literature on articulating the broader system within which OOP operates. This is

an important gap as it is impossible to understand OOP in isolation from the critical elements that comprise it. In fact, OOP is always designed and implemented as part of a wider interoperability package, even when OOP itself may be the ultimate goal of such a package. In this paper, I hope to give a sense of the interconnected system at play when it comes to OOP and the key considerations related to that broader system. By doing so I also hope to point to both *when* OOP should be operationalized and *how* it can be operationalized.

- **It explicitly links OOP and GaaP thinking**. Though the administrative optimization benefits of OOP are well understood, there is less acknowledgement of the link between OOP and GaaP. By laying out this connection I hope to bolster the argument for OOP implementation.
- **It approaches OOP system-design from a privacy perspective**. Unlike existing OOP research, much of which treats privacy as an important but peripheral concern, this work examines each aspect of an OOP deployment from a privacy lens to help governments create OOP systems that maximize privacy.

This work is based on three primary research methods: an extensive literature review across the areas of privacy, identification, data sharing, and OOP; interviews with experts in the field; and mini case studies highlighting different lessons of implementation from five countries with diverse approaches and at very different stages of OOP maturity. These countries are Estonia, the UK, the Netherlands, Canada, and Australia.

2. Some OOP Basics

Guiding questions:

- How is OOP defined in your country?
- What are the options for OOP implementation? Principle vs. program
- Which OOP approach makes the most sense within your country context?

2.1 Understanding OOP Variants

As highlighted earlier, the core concept of OOP is that users need to provide diverse information only once when in contact with public administrations.

However, implementation of this core concept varies across countries. In the five countries this paper examines most deeply, two primary determinants impact implementation variations: the nuances of in-country OOP definitions and which OOP approach—principle or program—countries choose to pursue.

2.1.1 Defining OOP

There is a distinction between collecting data once and storing data once. While there is broad consensus that, under OOP, collection should only happen once, some countries take the policy a step further and require that data storage also happen only once. Often these policies are enshrined in OOP-specific regulation.

> **Where we see this:** Under Estonia's once-only policy, data can be collected only once and stored once, in a designated database.
>
> By contrast, under the UK's Tell Us Once program, though data can be collected only once, each record can appear in multiple repositories across governments.

Though neither option is objectively better than the other, these distinctions are important and materially impact the design choices that are available to OOP-implementing governments, specifically regarding the underlying infrastructure that must be developed.

2.1.2 The Two OOP Approaches

2.1.2.1 Principle Approach

Under the principle approach, OOP is seen as a foundational principle to be implemented across all government systems where feasible. Scale is a critical concern under this approach, and as a result, the principle approach tends to be a longer-term play and often requires transforming legacy systems or even creating systems from scratch. Based on the experiences of the countries I examined, this approach focuses on creating wholly interoperable back-end government systems from a data perspective as well as user-facing interfaces that users can access to manage their information and data permissions.

To achieve this, governments need to put in place an identification mechanism (*see Chapter 4*) and a future-state data-sharing arrangement (*see Chapter 5*). While user value is still extremely important under this approach, the ultimate goal of a programmatic OOP approach skews toward transforming how the government works at the back end.

Where we see the principle approach: In Estonia, OOP is a universal principle, enshrined in various acts and applicable across most administrative tasks within the public sector. A once-only law was passed in the early 2000s that stated, "the same information should not be asked twice."[10] This definition of once-only was further refined under the 2007 Public Information Act, which states that departments are forbidden from establishing separate databases for the collection of the same data.

In Estonia, OOP is made possible by:

- The existence of unique identifiers for citizens and companies (see Section 4.1).
- A system of base registries (see Section 5.2).
- A data-exchange system in the form of the X-Road platform, which allows for harmonized data sharing across almost a thousand public organizations (see Section 5.3.2).

Since OOP is so widespread it's hard to put a dollar value on the benefits it has seeded in Estonia. However, X-road—which forms the backbone of interoperability and thus once-only in Estonia—is said to have saved Estonians 844 years of work time annually.[11]

2.1.2.2 Program Approach

The program approach is use-case-focused. Under this approach, departments identify tightly defined use cases that can benefit from an OOP ethos. OOP programs are not necessarily designed to scale beyond the specific use case they are targeting. Partly because of this reason, OOP programs tend to be more opportunistic about implementation, leveraging systems that already exist instead of building new systems from scratch. Implementing teams will focus on creating basic, limited-use interfaces for both users and governments and data-sharing connections only between relevant bodies.

To achieve this, departments will at a minimum require a program-specific unique identifier (see Chapter 4) and bilateral data-exchange agreements (see Chapter 5) between the implementing departments and partner bodies. The ultimate goal of a programmatic OOP approach skews toward creating and proving value for users.

Where we see the program approach: In the UK, the OOP or Tell Us Once program has been in place since 2007. The OOP experience in the UK is somewhat unusual in that it has been limited to two simple use cases: birth and death notification across relevant government bodies. Tell Us Once is led by a team in the Department for Work and Pensions, which had received a number of complaints related to these use cases.

Tell Us Once is offered in partnership with both central and local government bodies, and is considered a truly joint effort, with 96 percent of councils in the UK now integrated into the service.[12] Key features of the program include the establishment of a single cross-central and

[10] "Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementation," *Digital Opportunities for Better Agricultural Policies,* OECD iLibrary, 2019, *https://www.oecd-ilibrary.org/sites/510a82b5-en/index.html?itemId=/content/component/510a82b5-en#back-endnotea14z4*.

[11] "X-Road," *e-Estoni*a, accessed June 11, 2020, *https://e-estonia.com/solutions/interoperability-services/x-road/*.

[12] Matt Briggs, "The Benefits of Tell Us Once," *Guardian*, December 16, 2011, *https://www.theguardian.com/government-computing-network/2011/dec/16/tell-us-once-matt-briggs*.

local-governance model, funding breakdowns according to contributions, and a wholly opt-in ethos directed at both local governments and users.[13]

The program represents value to both government and citizens. Benefits from 2011 to 2021 are estimated to total £255.8 million—£172.6 million for the government and £83.2 million for the public as a result of accessing government services faster as well as saving money through the process.[14] These numbers don't include second order benefits that are likely to accrue during this period such as tackling benefit fraud by making it harder for someone to steal a deceased individual's identity.

2.1.2.3 Pros and Cons of the Two Approaches

Based on the descriptions of the principle and program approaches, I have identified and summarized the pros and cons of the two approaches in Table 2 below.

Table 2: Benefits and drawbacks of the two OOP Approaches

	Benefits	Drawbacks
Principle approach *OOP is treated as a foundational principle implemented across all of government*	• Captures transformative benefits of OOP in line with GaaP thinking • Allows users greater control over their own data through the creation of user-facing interfaces	• Requires updating or replacement of legacy systems • Relatively longer-term play • Relatively expensive to implement • Requires a high level of political capital • Requires a high level of buy-in across all government departments
Program approach *OOP is treated as a program that is limited to specific use cases*	• Provides quick proof of concept • Can be achieved leveraging existing systems • Relatively cheap • Relatively short-term play • Buy-in of implementing departments only is required	• Is not necessarily scalable • Does not require system transformation and thus as a stand-alone will not advance movement toward GaaP

Given our interest in GaaP, countries may assume that the principle approach is the preferred or recommended one. That is not the case. The program approach is a great way of testing OOP policies in-country and may be a good way of sequencing toward the principle approach. Which route countries choose is dependent upon country-specific considerations such as the country's privacy threat profile (see Section 3.1.2), goals, and resources.

Table 3 provides a summary of OOP cases in our sample countries.

[13] "The Benefits of Tell Us Once."
[14] Lyn McDonald, "Tell Us Once makes it easier to inform the authorities about a birth or death," *The Guardian*, November 10, 2011, *https://www.theguardian.com/public-leaders-network/2011/nov/10/tell-us-once-birth-death*.

Table 3: OOP cases in sample countries

	Maturity	Approach	Components
Netherlands	High	Principle	• General data protection regulation (GDPR) • Foundational unique identifier and authentication • System of base registries
Estonia	High	Principle	• GDPR • Foundational unique identifier and authentication • X-Road
UK	Medium	Program	• Birth and death notification • Programmatic unique identifier • Bilateral data-exchange arrangement
Canada	Nascent	Principle	TBD
Australia	Nascent	Principle	• The Privacy Act • Foundational unique identifier and authentication • Existing federated exchange at the federal level

2.2 Baseline Conditions that Disallow All-of-Government OOP Implementation

Previously I noted that if left unmanaged, OOP will have serious negative implications on privacy. I will explore the primary threats to privacy under OOP in the next chapter (see Section 3.1.2). However, certain in-country conditions make all-of-government OOP implementation entirely unfeasible despite relatively strong controls, thus greatly exacerbating the negative ramifications of OOP systems.

I have identified three conditions of particular concern. These have been partially derived from research on national digital ID systems,[15] but I believe the findings are transferable to OOP. Countries with one or more of these conditions should limit their OOP efforts to a programmatic approach. These conditions are:

- **Weak rule of law**. Countries with a weak rule of law instead have variants of "rule by law," where the enforcement of laws depends upon the relative power of the affected parties. The main difference between contexts with and without a rule of law is that, without it, laws may be formulated, interpreted, and enforced in biased ways, creating qualitatively different outcomes in terms of the scale and severity of the exclusion of relatively weak parties.

  For example, in circumstances where the rule of law is weak, if the enhanced data availability and analysis that is accessible due to OOP is exploited by politically powerful individuals or firms, weaker individuals and small businesses will not be able to access just legal channels.

- **High risk of new and unanticipated power asymmetries**. Asymmetries in both political and market power can be exacerbated to the detriment of weaker parties as a result of OOP and its underlying systems being put into place.

[15] Mushtaq Khan and Pallavi Roy, "Digital Identities: a political settlements analysis of asymmetric power and information," ACE SOAS Consortium, October 2019, *https://ace.soas.ac.uk/wp-content/uploads/2019/11/ACE-WorkingPaper015-DigitalIdentities-191004.pdf*.

For example, power asymmetries are likely to be exacerbated as powerful political actors gain access to surveillance tools linked to OOP that make collective action and mobilization more difficult than before.

- **Weak counterpower of civil society**. Civil society organizations provide noninstitutional oversight to government schemes by helping to raise the voices of users and creating pressure on governments to address critical areas of concern. In countries where civil society is either weak or does not have the expertise needed to provide oversight in the unique identifier domain, it cannot act as a counterpower to the state.

  In the absence of a strong civil society that can provide oversight, institutional bias can creep into OOP systems. Civil society organizations play a central role in cataloguing system failures, gathering resident feedback, and giving individuals a structured way of making their voices heard. All of this keeps pressure on governments to resolve problems. Without civil society organizations that can act as this correcting mechanism, governments would remain blind or unresponsive to user needs.

3. Privacy

Guiding questions:

- What are the general concerns related to government use of personal data?
- What are the most urgent threats to government use of personal data in your country?
- Has your country adopted a multimodal approach, or framework, toward privacy?
- Is your privacy framework sufficiently strong?
- What are the broader considerations that impact the development of the privacy framework in your country?

Further reading:

The United Nations, Universal Declaration of Human Rights, Article 12
The European Union's General Data Protection Regulation, Key Issues
Ann Cavoukian's Privacy by Design: The 7 Foundational Principles
The World Bank's Privacy by Design: Current Practices in Estonia, India and Austria
Office of the Privacy Commissioner of Canada's Guidelines for Obtaining Meaningful Consent

The right to privacy is enshrined within Article 12 of the UN's 1948 Universal Declaration of Human Rights.[16] Modern conceptions of privacy can be traced to a seminal 1890 paper by Samuel Warren and Louis Brandeis in the *Harvard Law Review*. They defined privacy as the idea that **people have the right "to be let alone" and the right to disclose information about themselves on their own terms**.[17] For the purposes of this document, I view privacy as a fundamental right while recognizing that the degree of privacy individuals require is often contextually dependent and thus highly variable.[18]

In the digital world, the right to privacy is translated as the need to keep personal data—that is, data that identifies or can be used to identify an individual—under the control of that individual. Since **OOP and its underlying technical components—namely identity- and data-sharing mechanisms—are essentially rooted in the use of personal data, a natural tension exists between the implementation of this policy and the need to maintain data privacy**.

Defining personal data
"Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Source: Guide to the General Data Protection Regulation (GDPR), UK Information Commissioner's Office

Any OOP implementation will necessitate tradeoffs with privacy and should be rolled out while preserving privacy as much as possible. This means creating standards around two questions:[19]

- **Data privacy:** Who has authorized access to personal data, and how can they use this data from a legal standpoint?
- **Data protection:** How is data secured from a technological standpoint?

[16] "Universal Declaration of Human Rights," https://www.un.org/en/universal-declaration-human-rights/.
[17] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy." *Harvard Law Review*, vol. 4, no. 5 (Dec. 15, 1890): 193–220. *https://jstor.org/stable/1321160*.
[18] Louis Menand, "Why Do We Care So Much About Privacy?" *The New Yorker*, June 11, 2018, *https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy*.
[19] Rick Robinson, "Data Privacy vs. Data Protection," January 30, 2020, *Defrag This*, *https://blog.ipswitch.com/data-privacy-vs-data-protection*.

I have explored these topics from a policy angle.

Ultimately, robustly determined and enforced **standards covering both data privacy and data protection will determine the foundational rules and rails for the broader environment within which OOP operates** and establish needed limits on the use of personal data by the government. Countries considering OOP implementation should seek to understand the concerns around government use of personal data and shore up their privacy standards accordingly before building any technical infrastructure.

3.1 Understanding Concerns around Government Use of Personal Data

3.1.1 General Issues

Traditionally, people have somewhat willingly given governments the power to gather and retain data in exchange for better social outcomes; however, in our increasingly digital age there seem to be serious doubts about the ability of governments to use data safely and ethically. In the US, a 2019 survey found that 64 percent of the public were very or somewhat concerned about how the government uses their data,[20] while in the UK only 30 percent of the public said they believed that central or local governments would use their data ethically in 2018.[21] Similarly, a 2015 survey in Australia revealed that 48 percent of those surveyed believed that the government would compromise their data.[22]

These are concerning statistics especially considering that these examples are from relatively advanced digital economies. The government's monopoly on both service delivery and the use of legal and paralegal force means that even in circumstances where governments abuse personal data, individuals are largely unable to opt out of the gaze of the state. However, the follow-on effects of such misuse of the public trust are likely significant. Given that trust translates to citizen cooperation and compliance, it is the bulwark of a well-functioning society, integral to the success of public policies, economic activities, and the law.[23]

To combat this, at a minimum, governments must:

- **Obtain meaningful consent**, so that people have a say about what data is collected on them and how it is used and disclosed.[24] Meaningful consent occurs when individuals make informed decisions, and their choices are properly recorded and maintained.[25] Under meaningful consent, the scale and scope of consent is clear.

  Obtaining truly meaningful consent is not a clear-cut or easy process. Though consent is the cornerstone of privacy and data protection around the world, most current models of consent overly burden the individual who is giving consent by forcing people to read through opaque online contracts, license agreements, terms

[20] Brooke Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Internet, Science & Tech* blog, Pew Research Center, November 15, 2019, *https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/*.

[21] Open Data Institute, "Nearly 9 in 10 people think it's important that organisations use personal data ethically," Nov. 12, 2019, *https://theodi.org/article/nearly-9-in-10-people-think-its-important-that-organisations-use-personal-data-ethically/*.

[22] Tim Binsted, "Australians Don't Trust Government or Telcos to Protect Their Data: Survey," *Sydney Morning Herald*, July 1, 2015, *https://www.smh.com.au/business/australians-dont-trust-government-or-telcos-to-protect-their-data-survey-20150701-gi2arn.html*.

[23] OECD, "Trust in Government," accessed June 25, 2020, https://www.oecd.org/gov/trust-in-government.htm.

[24] Deloitte, "2017 Global Mobile Consumer Survey: US edition," Deloitte Development LLC, 2017, *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf*.

[25] Office of the Privacy Commissioner of Canada, "Guidelines for Obtaining Meaningful Consent," May 2018, *https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/*.

of service, and so forth. Research by Deloitte shows that 91 percent of individuals consent to these terms without reading them.[26]

Modern approaches to meaningful consent must try to shift the burden away from consumers to ensure a forward-looking approach to privacy. [27] The office of the Privacy Commissioner of Canada has developed some useful guidelines to ensure meaningful consent. They include foundational principles of consent, such as providing consumers with simple yes or no options and making consent a dynamic and ongoing process, and rules to help establish the form of consent needed in different situations; for example, whether express or implied consent is required.[28]

- **Increase transparency around data collection, storage, and use** to decrease the knowledge asymmetry between governments and users. As government data collection increases, people risk feeling they have less control over who has data about them, what type of data is collected, how this data is kept, and what can be done with it. People's inability to easily answer any of these questions—to quickly see what immutable facts (e.g., biometric data) and historical facts (e.g., traffic violations etc.) governments hold on them and what they're doing with it—is disempowering.
- **Ensure trust in data-use today and in the future**. In the absence of explicit and meaningful controls, when individuals give an entity their data, they are allowing the entity to use this data in perpetuity. Thus, the question isn't just whether the entity be trusted to protect personal data now, but more broadly, whether the entity be trusted to never abuse personal data. Managing the relationship between data, permanence, and trust is perhaps one of the most critical issues of our time and is particularly important within the context of government institutions.
- **Disclose risks** related to the government's use of personal data within a specific context and share how these risks are mitigated. To do this governments will first have to conduct a comprehensive privacy-threat assessment.

3.1.2 Country-Specific Issues: Conducting a Privacy-Threat Assessment

Five main threats impact the use of personal data by the government. I have broadly defined these and analyzed how failures in securing personal data against these threats could impact trust in government and service delivery.

Threat 1: Misuse of residents' data by government, both now and in the future

Examples:

- Legal institutional surveillance would undermine trust and safety.
- Illegal institutional surveillance, such as monitoring calls and internet history without any legal backing or proof of the need for it.
- Illegal surveillance by unauthorized government personnel. For instance, while police officers should be able to see an individual's criminal record, a librarian should not. Furthermore, even police officers should not be able to see a resident's personal data for personal purposes under any circumstances, or for professional purposes in the absence of a compelling legitimate reason.

[26] "Data Protection and Financial Inclusion."

[27] David Medine and Gayatri Murthy, "3 Data Protection Approaches That Go Beyond Consent," CGAP, January 7, 2019, https://www.cgap.org/blog/3-data-protection-approaches-go-beyond-consent.

[28] "Guidelines for Obtaining Meaningful Consent."

One prominent example of this may occurred in 2014, when former Toronto mayor Rob Ford's medical records were inappropriately accessed by staff members not involved in his care for a rare form of cancer.[29] These breaches were considered illegal under Canada's Personal Health Information Protection Act. In total, Mayor Ford's records were violated four times by three hospitals.

Cost of failure: Ranges from some erosion of trust in government to complete decimation of trust; likely low impact on service delivery.

Solution: Secure a sense of privacy from the state itself.

Threat 2: Misuse of data by third-party government contractors

Example: The UK's National Health Service raised concerns about passing personally identifiable data on 1.6 million patients to the UK-based artificial intelligence company DeepMind when the app was being developed, without people's knowledge or consent.

Cost of failure: Erosion of trust in government; likely low to medium impact on service delivery.

Solution: Secure privacy from actors contracted by the state.

Threat 3: Misuse of data from military-level incursions by malicious outside states

Example: In 2007, Estonia faced a series of Russian state-sponsored cyberattacks. Numerous Estonian public institutions were targeted, including the parliament and various ministries. The result was that cash machines and online banking services were sporadically out of service, government employees were unable to communicate internally via email, and news outlets were unable to deliver the news. The attack lasted 22 days and impacted the entire resident population of the country.[30] Notably, though, the Estonian data-exchange infrastructure—the X-Road—was targeted in the attack, it managed to keep working.

Cost of failure: If successful, such a breach may result in lowered trust in government and will likely have a significant impact on service delivery. The worst-case scenario would be a debilitating and devastating attack on a nation's government and its residents.

Solution: Protect privacy against foreign state actors.

Threat 4: Misuse of data by individuals and organizations (e.g., businesses and political parties) that seek to benefit from it:

Example: In March 2018, a massive breach of Aadhar, the unique identification authority of India, was discovered that impacted more than a billion people. Private data was stolen including names, 12-digit ID numbers, and information on connected services like bank accounts.[31]

Cost of failure: This event had an uncertain impact that could range from erosion of trust in government to an unlawful and insidious influencing of people's democratic choices. Likely low impact on service delivery.

Solution: Protect privacy against nonstate actors.

Threat 5: Misuse of data by individuals' family and friends

---

[29] Olivia Carville, "Privacy of Rob Ford's medical records breached by third hospital," *The Star*, February 12, 2015, https://www.thestar.com/life/health_wellness/2015/02/12/privacy-of-rob-fords-medical-records-breached-by-third-hospital.html.

[30] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/.

[31] Zack Whittaker, "A new data leak hits Aadhaar, India's national ID database," ZDNet, March 23, 2018, https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/.

Example: Individuals may want to discover the private medical or financial data of their loved ones.

Cost of failure: It is unclear what the impact on trust in government and service delivery would be from such actions.

Solution: Protect individuals' privacy from people they know.

These five threats are by no means a comprehensive list and understandably, the urgency of each of these risks may vary from country to country. Despite these limitations, by identifying the threats, understanding the relative costs of failure, and assessing the probability of these events taking place, governments can start to build tailored privacy frameworks with appropriate resources allocated and deployed. Additionally, conducting such a threat assessment allows the government to identify some of the key issue areas that must be defined in their privacy standards. Some initial guidance on how countries may go about doing so is presented in Table 4.

Table 4: Summary of privacy threat assessment

	COST OF FAILURE	LIKELIHOOD	KEY ISSUES (e.g.)
Threat 1: State	Trust: High potential impact on trust in government Service delivery: Low impact	Assess likelihood of each threat on a scale of low to medium based on the country context. Rank threats accordingly.	• Consent for data use • What type of data is collected? • Who can access collected data?
Threat 2: Third party contracted by state	Trust: Medium to high erosion of trust in government Service delivery: Low to medium impact		• Consent for data reuse and processing • Knowledge about third-party permissions
Threat 3: Foreign state actors	Trust: Medium to high erosion of trust in government Service delivery: High impact on service delivery; ranges from some services being crippled to the entire government being crippled		• Where is data held?
Threat 4: Nonstate actors	Trust: Medium to high erosion of trust in government Service delivery: No to low impact		• Where is data held?
Threat 5: Personal network	Trust: No to low impact of trust in government Service delivery: No to low impact		• Who can access collected data?

It's important to acknowledge that beyond accounting for the specific threats described above, privacy erosion can occur due to issues of implementation, particularly things the government does wrong in this sphere—for example failing to secure data adequately—thus leading to incidents like private data leaks, and/or things the government

ends up doing badly, such as not maintaining adequate transparency when it comes to the question of who is using personal data. These must also be accounted for in the development and deployment of strong privacy standards.

3.2 Creating a Privacy Framework

A multimodal approach to privacy standards is needed to address the concerns regarding government use of personal data. I use the term "privacy framework" to denote a multimodal approach comprised of three prongs:

- A strong set of regulations
- A commitment to adopting a privacy-by-design approach across government
- Creating strong enforcement mechanisms around privacy-related issues

Though these prongs are not mutually exclusive and in fact often interact with and strengthen one another, I will describe each one individually below.

3.2.1 Strong Regulations

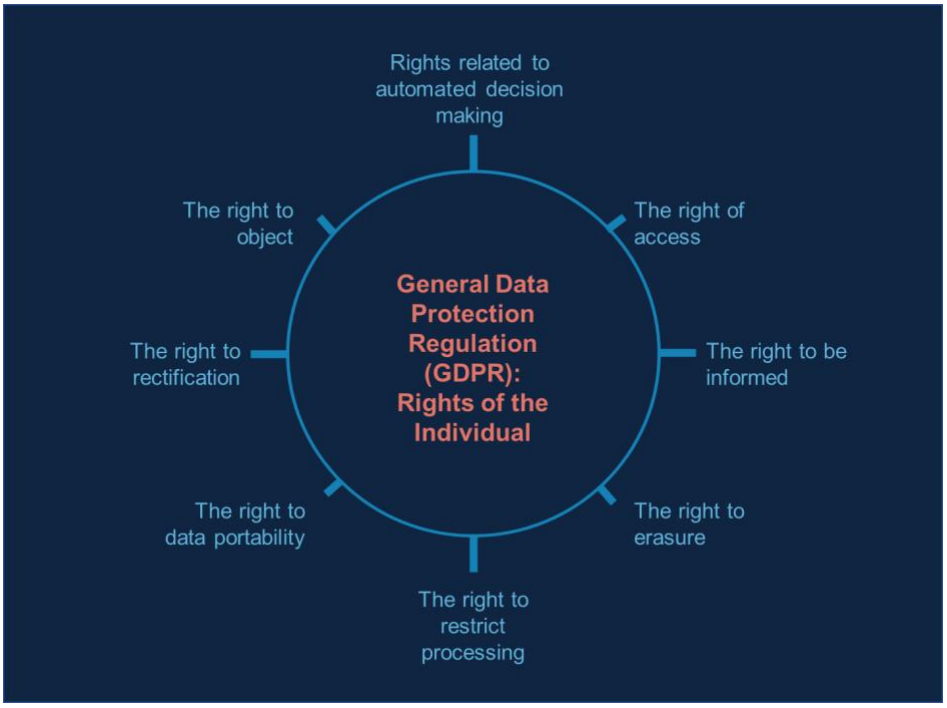
As highlighted earlier, there are at least two issues that need to be addressed by strong regulations: data protection and data privacy. Local, regional, and national governments use a combination of regulations to determine what constitutes private data and how it can be collected, held, used, and accessed. While it is almost impossible for a single regulation to cover every circumstance, certain elements make some data protection regulations, such as the EU's GDPR, stronger than others. Three such elements are:

- **Principles that guide the legislative approach.** These principles inform the entire legislation and thus provide a foundation from which all future rules follow. It is understood that compliance with the principles is key to maintaining the privacy rights of individuals. Principles have the distinct benefit of anticipating both current and future use cases as they embody the spirit rather than the specifics of the legislation. Among the GDPR's principles, for example, as seen in Figure 2, are purpose limitation, data minimization, and storage limitation.

Figure 2: Six basic principles of data processing in GDPR

- **Establishment of the inalienable rights of the individual**. These lay out the specific data rights of individuals vis-à-vis any party that collects their personal data (see Figure 3). The privacy of an individual is therefore predicated upon upholding these enumerated rights. The GDPR has done a particularly good job of creating a short but powerful list of rights, such as the right to erasure and the right to data portability, which have widespread implications for how privacy is to be maintained.

Figure 3: Rights of the individual under GDPR



- **Accountability and governance mechanisms**. Clear paths to accountability and the bodies responsible for ensuring said accountability are laid out for the benefit of both residents and organizations. The data collector knows the compliance requirements and the consequences of noncompliance.

Beyond the specifics of the regulation, it is important that countries adopt modern data-privacy regulations. By modern, I mean forward-thinking regulations that center on user rights and values and not only provide protections for today's world today, but also anticipate future challenges to privacy that may arise as new technologies (Internet of Things, AI, etc.) begin to find applicability in the public sector. This can be achieved by building adequate adaptability and flexibility into the regulatory approach. One important aspect of building in sufficient flexibility is to ensure that regulations are not just built in the abstract but can be adapted once they're reality-tested.

3.2.2 Privacy by Design

Privacy by design goes beyond the privacy and data-protection policies of regulatory compliance by advancing the view that privacy assurance "must ideally become an organization's default mode of operation."[32] Inspired by design thinking, privacy by design is based on adherence to seven core principles.

- **Proactive and preventativ**e. Unlike retroactive approaches, privacy by design proactively builds privacy into the whole system and/or process.[33] It anticipates risks and doesn't try to solve them after the fact.
- **Privacy by default**. The highest privacy setting is afforded by default to anyone who uses a particular system or process. This automatically gives data subjects a choice about how their data is used.
- **Embedded**. Privacy is built into the system as a core functionality. The logic is that when organizations think upfront about what personal data they want to use, for what purpose, and how to do this legitimately, it reduces the chance of later discovering that embedding privacy is technologically challenging, expensive, or even impossible
- **Positive sum**. This approach seeks to accommodate all legitimate interests and objectives in a win-win manner and avoids the presentation of false dichotomies such as privacy coming at the expense of security.
- **Lifecycle protection**. Secure lifecycle management of data, where data is securely retained and destroyed in a timely manner at the end of the cycle, is essential to upholding privacy.
- **Visible and transparent**. Component parts of the product or service are visible and transparent to users and other overseers, and are subject to independent verification.
- **User-centric**. The needs of the user are at the core of this approach, and measures like strong privacy defaults and appropriate notices are implemented.

3.2.3 Enforcement

Strong enforcement is predicated upon having processes in place for various scenarios and empowering designated bodies to pursue legal action and provide oversight, which collectively can help deal with privacy violations. Users should know what the process flow is if they want more information or what they should do in the event of a privacy invasion, and both in-department and governmentwide oversight bodies should be instituted to help ensure enforcement of regulations and privacy-by-design approaches.

3.3 Accounting for Considerations beyond Privacy

While governments must help individuals maintain their privacy to the highest extent possible, there are some additional practical considerations that go into the privacy-approach planning process. Accounting for and planning around these considerations is critical to managing expectations and avoiding chaotic outcomes when it comes to privacy. Some of the most significant considerations are as follows.

Maintaining usability. While privacy is an important consideration, fundamentally, government services must continue to work for residents under all circumstances because confidence in government can be undermined if services or public benefits are delivered in a manner that does not meet residents' expectations. Over time, with the advances in the private sector, the minimum standard of service that residents expect from their governments has risen. Such high standards can be particularly hard to maintain when very real issues of security must also be addressed. This means that getting the balance right between the somewhat competing goals of privacy, security, and usability is key.

---

[32] Ann Cavoukian, "The 7 Foundational Principles," The International Association of Privacy Professionals, October 8, 2018, https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf.

[33] "The 7 Foundational Principles."

Acting in the public interest. Despite an individual's right to anonymity, there are circumstances in which this right is outweighed by the need to safeguard the collective. Most of these circumstances related to national security, but a less typical real-world example is the UK cancer registry. Every cancer patient in the UK is automatically enrolled in the registry, which records and shares "how many people are diagnosed with cancer, what treatments they have, how long they live, and whether this is getting better or worse."[34] The information in the registry has the potential to help plan cancer services and identify where further progress is needed for all. Exceptions like the cancer registry should be clearly laid out and appropriate safeguards related to transparency and democratic accountability put in place to ensure that an exception is not inappropriately created without credible cause, and without following proper procedure.

Working within limited government resources. While some residents may have specific desires when it comes to data privacy, such as to receive and personally approve a request every time a government department or ministry uses data about them, this may not be practically feasible. The government faces practical constraints in the form of limited monetary resources and limited trained personnel. Working within these limitations, and placing resources where they are most needed, is a key consideration for governments.

[34] "What Is Cancer Registration?" Cancer Research UK, October 21, 2016, https://www.cancerresearchuk.org/health-professional/treatment-and-other-post-diagnosis-issues/about-cancer-registration/what-is-cancer-registration.

4. Identification Mechanisms

Guiding questions:

- Why does an identification mechanism centered around unique identifiers need to be put in place for OOP?
- What type of unique identifier makes the most sense for your OOP approach and context: foundational or functional?
- What are the pros and cons of each?
- Is your country ready for a foundational unique identifier?

Further reading:

World Bank Group, ID4D Practitioner's Guide
Cato Institute, The New National ID Systems
Mushtaq Khan and Pallavi Roy, Digital Identities: A Political Settlements Analysis of Asymmetric Power and Information
McKinsey Global Institute, Digital Identity: A Key to Inclusive Growth
World Economic Forum, A Blueprint for Digital Identity
Centre for Internet and Society India, Towards a framework for evaluation of Digital ID

An identification mechanism is required for OOP deployment.

Since users only give their information to the government once, when necessary, under OOP, government departments need some way to request and receive the **right user's** information. To successfully do this, governments must establish a way to identify individuals across multiple government systems. It would be extremely difficult to operationalize OOP without such an identification mechanism.

Consider the following example. At a departmental level, government bodies uniquely identify users. However, if User A is identified by a national insurance number under the health department and a national tax number under the revenue bureau, it will be very cumbersome for these two departments to reconcile the information they have about User A to ensure that she is the same person. Magnify the reconciliation problem by several million people and it becomes clear that **some type of identification mechanism that allows for rapid deduplication of siloed identifiers, works both in person and online, and can be used across all relevant government departments must form the technical basis of the enabling ecosystem that allows for advanced data-sharing in government**.

4.1 The Need for a Unique Identifier

As the above example shows, **unique identifiers lay at the heart of the identification mechanism required for an OOP deployment**.[35] A unique identifier is a numeric or alphanumeric string that is guaranteed to be associated

[35] It has been hard to disentangle the concept of unique identifiers from the broader conversation on identification systems, which usually have a unique-identifier component. I have attempted to separate identifiers as much as possible because, as evidenced by Tell Us Once in the UK, I don't believe OOP programs require a full-fledged identification system to work. However, given that identification systems—particularly digital ones, with their powers of remote authentication and verification—may be especially useful when deploying principle approaches to OOP, it is likely that many countries will

with only a single entity (e.g., individual or business) within a system.[36] This string, in turn, is linked to some core set of attributes that describe an entity and determine the transactions in which that entity can participate. While the total existing set of attributes is endless, they can be broadly categorized into three groups: inherent (intrinsic attributes such as gender or age), accumulated (developed attributes such as an individual's health record), and assigned (attributes that are attached to an entity such as address or phone number).

A unique identifier can be either:

- **Foundational**, meaning that it is a multipurpose identifier that provides universal coverage and can be used across all of government, or
- **Functional**, meaning that it is created for specific sectors or uses, generally only covers a limited population, and typically can be leveraged by only one or a few departments or ministries.

Either of these can be used for OOP and each comes with its own benefits and limitations; I will be exploring both identifier types in turn.

The Necessity of a Unique Identifier: OOP in Australia

In Australia, OOP or Tell Us Once is a central part of the government's Digital Transformation Strategy, which sets a countrywide direction until the end of 2025. Considered a whole-of-government platform service, OOP is part of Australia's vision of building "government services that are easy to deal with, informed by you [the citizen] and fit for the digital age," and doing so while simultaneously delivering on privacy.

I learned more about this from Felicity Hitchcock, who is the product manager for Tell us Once along with several other cross-government platforms. "The pilot stage of Tell Us Once in Australia is limited to fully examining a single scenario," she said, "giving users the ability to advise the government of a change in circumstances or personal information *once*. Users can also join multiple agencies on that one occasion across the federal, state, and local levels. For example, informing the tax system and traffic authority of a change of address."

From a technical perspective, to successfully deploy Tell Us Once the government must be able to tag a user with one identifier and then aggregate the information on that user by using the same identifier across all relevant government departments. Till now, such an identifier has not existed in Australia.

The Australian identity system is federated by design and includes participation by agencies at the federal, state, and local levels. A points system, known as the 100-point check, is used for identity verification. Under this, users must provide a combination of federal- and jurisdiction-issued documentation totaling 100 points. Each piece of documentation is worth a certain number of points and at least one primary document (such as a birth certificate, passport or driver's license) must be included as part of the 100 points.

choose to leverage these systems, if possible. Of the five countries whose OOP regimes I have examined in detail, only two—the UK and Canada—provide guidance on how to do OOP without leveraging a full-fledged ID scheme. Ultimately, much of the research presented here draws from the literature on both unique identifiers and ID systems; this work is particularly indebted to the literature on digital ID systems.

[36] "unique identifier (UID)," IoT Agenda, accessed October 4, 2020, https://internetofthingsagenda.techtarget.com/definition/unique-identifier-UID.

Knowing that digital government service delivery would be strengthened by an e-identity, the Australian government, in collaboration with both state and local governments, is currently piloting a new e-ID system called Digital Identity or MyGovID. MyGovID is essentially the 100 point check in digital form, but with it, users must upload their identity documents for verification only once rather than having to submit them for each use case.[37] MyGovID is linked to a unique identifier, which can be used across several services, integrates with existing forms of identification (both federal and provincial), and is a completely opt-in service.

The Digital Identity system enables the digital verification of government-issued identity documentation, and is also completely opt-in. Privacy is a key concern for the system and is being addressed with the use of unique tokenized identifiers that protect privacy and prevent the tracking of user behaviors on the system. Digital Identity will act as the infrastructure atop which Tell Us Once can operate. With it in place, the Tell Us Once program will be able to create a truly seamless and scalable multilevel system for the user.[38]

4.2 Foundational Unique Identifiers

4.2.1 The Benefits and Challenges of Foundational Unique Identifiers in the Context of OOP

A foundational unique identifier can be leveraged by governments to ensure that an identity is unique, identify an individual against an existing record, and even potentially authenticate an individual against an existing record. As a result, foundational unique identifiers can be leveraged for both the OOP principle and program approaches.

> **Where foundational unique identifiers are being used:** In the Netherlands, each citizen and resident is assigned a unique national number. This national number is the central identifier by which every governmental service is linked to a specific citizen and is the core unique identifier leveraged for OOP. The national number is also reflected on individuals' driver's licenses and national IDs. While the national number is connected to an individual's digital ID, it is not reflected on it.

With a foundational unique identifier in place, the state's capabilities are significantly advanced across three primary dimensions:

- Scale: A foundational identifier permits data across several databases to be linked, thus allowing for large-scale, population-level data capture and analysis.
- Speed: A foundational identifier can give governments a snapshot of people's movements, which may be useful in contexts such as contact-tracing during a pandemic.
- Scope: A theoretically endless number of use cases can be connected to the unique identifier.

Unfortunately, these benefits are also accompanied by risks. Foundational unique identifiers that link individual identities across multiple databases can lead to a loss of privacy that is not justified by improvements in security or service-delivery outcomes. Threats exist at three levels:

[37] MyGovID, accessed October 15, 2020, https://www.mygovid.gov.au/.

[38] While theTell Us Once program is being executed at the federal level in Australia, there are also state level efforts to mobilize once-only policies. New South Wales recently released the Australian Death Notification Service, which allows individuals to "notify multiple organisations online that someone has died so their accounts can be closed or transferred." The service currently has fourteen participating organizations including banks, communications companies, and energy providers.

Known risks. That is, risks to anticipate and plan for at this stage.

- The system is hard to implement. Because unique identifiers are linked to personal data, they inherently demand stringent controls to mitigate potential misuse and associated risks. Essential elements include robustness and transparency regarding what data fields they are linked with, rigorous cybersecurity standards to protect related stored data, and mandatory explicit user consent for all data.
- The use of a unique identifier risks creating a permanent and immutable record that people cannot change or get rid of. To avoid this problem, policymakers must build in strong rules that facilitate the change and revocation of information linked to the unique identifier.
- The very nature of a unique identifier linked to multiple databases increases an individual's shared fate risk. Shared fate risk applies to data that, if compromised, would cause further and extensive data compromise from multiple (even unrelated) sensitive systems. Since a unique identifier used widely across government systems would allow access to potentially sensitive information, it is a ripe target for misuse. To avoid this, any unique identifier plan must be accompanied by built-in safeguards.
- Foundational unique identifiers are accompanied by a high risk of overuse that can result in creating a honeypot of related data. Since a unique identifier is both useful and risky, some governments are thinking about how they can make it less important in societal use. One way of reducing the exposure of a unique identifier would be to make it usable only by governments.
- A foundational unique identifier can significantly increase the government's surveillance capabilities. Enshrining mechanisms into law to counter this power is critical to the long-term democratic functioning of a society.

Known-unknown risks. These are risks developers know could arise in the future but are unsure how they will manifest.

While it is difficult to clearly identify the appropriate use of a foundational unique identifier, in the absence of controls once a unique identifier system is in place it is hard to limit its use, resulting in **mission creep**. Mission creep is perhaps the most significant known-unknown risk for a country implementing a unique identifier. For this reason, countries must clearly articulate the intended purpose of the system both in the short and long term, ideally both defining and limiting what information is connected to the unique identifier. This is challenging but important.

Globally, unique identifiers are plagued with mission-creep issues. In the United States, the Social Security Number (SSN), which was originally a functional identifier meant to track people's accounts within social security programs, is now linked to taxation records, financial records, credit cards, and more. In India, the unique 12-digit Aadhaar number issued to all residents was initially billed as a system that would give those living in poverty an official identification document, but it has become a mechanism for tracking transactions, employment verification, and terrorism prevention.

Once mission creep occurs it is almost impossible to reverse. Moreover, scope creep results in additional risks, including:

- Higher chance of exclusion as the identifier's use is both linked to and required across a broader range of use cases
- Increasing privacy -related concerns due to the creation of a wider footprint
- Negative impact on the power balance between state and civil society

Unknown-unknown risks. These risks are completely unanticipated at this stage and include the range of things that may become uncontrollable in the future as a result of a foundational unique identifier being introduced. This is the category that is most worrying for both policymakers and civil society actors.

4.2.2 Assessing a Country's Readiness for Foundational Unique Identifiers

Not every country is appropriate or ready for a foundational unique identifier. Here, I've attempted to identify some of the major prerequisites that must be taken into consideration prior to embarking on such a venture. Beyond the baseline considerations highlighted in Section 2.2, there are some prerequisites that each country must aim to have in place prior to launching a foundational identifier.

Stakeholder buy-in

Public readiness: Public engagement and consultation, where members of the public can provide input on the development and design of a digital ID, will enhance the value of the system as a whole. It will allow the government to understand and mitigate existing context-specific barriers. Moreover, giving the people more knowledge about the system will create greater trust in the system as a whole. As a related but separate issue, governments should help civil society organizations get involved with the oversight process by helping them build the requisite expertise and experimenting with public-private oversight arrangements.

Government readiness: Ensuring that the government has sufficient fiscal, technological, and administrative capacity to build and operate a unique identifier is critical to its success. Moreover, given how ambitious a unique identifier is, there is a need for strong political will and coordinated effort between a range of stakeholders to ensure that it is successfully launched and operated.

Policy regulatory infrastructure

Privacy framework: For a full discussion about the privacy framework please refer to Chapter 3.

Unique identifier regulation: A critical piece of the puzzle is that the unique identifier system function based on validly enacted legislation. The digital ID evaluation framework developed by the Centre for Internet and Society in Bangalore provides guidance on what elements must be part of a sufficiently strong law.[39] Though this guidance has been developed for digital IDs, it is also applicable to the foundational unique identifier conversation. A summary of this guidance across the areas of rule of law, rights, and risks can be seen in Appendix 1.

Set of standards and general principles: While the standards and general principles that a nation chooses may vary from context to context, these are some of the most important.

Transparency should start at the design and procurement phase to ensure that the unique identifier is not developed in a silo and that all decisions are understood by the public. There must also be transparency around the roles and responsibilities of various entities within the system. Finally, transparency should be designed as an integral part of the unique identifier system instead of being made available as an afterthought. Core to this is ensuring that all users are clear on what information the identifier is linked to, and what purposes it is used for. Clear and accessible explanations will prevent ambiguity and enhance user trust in the system.

Users should have control over opting in and out of the system, and choosing what types of information the identifier is linked to. Informed consent is essential to any use of the identifier.

[39] For more on this see Appendix 1.

Tokenization

Privacy-enhancing technologies and strategies must be built throughout a foundational unique identifier system. One particularly compelling measure is tokenization.

Tokenization significantly reduces the exposure risk of sensitive information that accompanies a unique identifier connected to several databases. Under tokenization, when shared, the sensitive, unique identifier is substituted with a non-sensitive, unique "token" that has no exploitable meaning or value.[40] These tokens represent individuals in different databases, and they cannot be backward-mapped to the unique user without access to the tokenization system.

There are two types of tokenization. In front-end tokenization, the user creates a token that can be used in a transaction as a substitute for the original identifier. This type of tokenization is user-dependent and requires some level of digital literacy to implement. As a resultant, it is less effective compared to back-end tokenization in achieving the policy goal of reducing sensitive information exposure.

In back-end tokenization, the unique identifier provider automatically tokenizes the identifier before it is shared with another system. This form of tokenization limits the exposure of the original identifier and limits data correlation across sectors. In full back-end tokenization, as used by Austria, the core identifier is not exposed; in partial tokenization, as used by India, the core identifier is exposed only to a few service providers.

Estonia and the Netherlands use no tokenization, so the core identifier is exposed and used as-is by all service providers.

4.3 Functional Identifiers

Since functional identifiers are limited to specific use cases, they do not automatically link identities across databases. On the plus side this means they avoid many of the pitfalls of foundational identifiers noted above such as shared fate risk, risk of overuse, etc. On the other hand, the limited functionality of such identifiers means that:

- They are easy to launch but hard to scale beyond the specific use case that they are developed for
- They are typically less inclusive than foundational identifiers in terms of the population covered
- They are not automatically interoperable with other systems

From an OOP perspective, functional identifiers are particularly suited to executing scope-limited OOP programs.

> **Where we see this:** As mentioned earlier, by and large the UK's Tell Us Once program has been extremely successful. Though it lacks a foundational unique identifier scheme, Tell Us Once (TUO) has leveraged several different functional identifiers to achieve its goals. To examine this let's look at the journey of users wishing to record a birth or death.
>
> Users must first go to the local registrar's office. If TUO is available in the area, they are given a reference number that they must use to file their case online, in person with a TUO representative,

[40] Julia Clark et al., "Practitioners Guide," World Bank's Identification for Development Initiative, October 2019, http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.

or by telephone to a dedicated service. In addition, the user needs to have the following information:[41]

- Multiple identity credentials for their deceased loved one, including their date of birth, National Insurance number, driving license number and passport number.
- Specific information on the services that need to be cancelled such as benefits/pensions, or local authority services like blue badges.
- Information on the next of kin of the person dealing with the deceased's estate.

Ultimately, the UK Tell Us Once program has eliminated the need for a foundational identifier by requiring the user to share various functional identifiers linked to the deceased. While this system has worked for this tightly defined use case, under the current system design, (1) additional burden is put on users as they for example must identify the services used by the deceased; and (2) scaling up to add additional services under the program would be a significant challenge.

Though functional identifiers are most suited to the programmatic OOP approach there is some nascent evidence that they can be leveraged for the principle approach if a sufficiently strong **identity-stitching mechanism** is in place. An identity-stitching mechanism allows an individual's records across different departments to be cross-checked and ratified. While foundational identifiers inherently have a stitching mechanism built in, functional identifiers do not.

Where we see this: Between 2019 and 2020, Canada's Treasury Board Secretariat (TBS), the central agency that reviews and approves spending by the Canadian government, prototyped an initial OOP solution. The purpose of this experiment was to explore the ideal user experience and to understand what was technically feasible.

Broadly, the Canadian Digital Exchange Platform (CDXP) team has four main goals:

- to set the direction for interoperability standards for the federal government,
- to take a leadership role by sharing information about who's doing what in both the public and private sector and in setting policies and standards,
- to build out a robust digital ecosystem with CDXP, which is similar to Estonia's X-Road (see Section 5.3.2)
- to experiment with products and services to help inform direction-setting.

The purpose of this work is to ensure that any solutions implemented actually work. It is with this backdrop that TBS began its OOP experimentation. Its focus was on two main aspects of OOP deployment: technical integration and the user experience. To examine these TBS looked at four key interactions that are critical to the functioning of an OOP system (see Appendix 2.1). Dealing with the identification question was a core part of the work.

From the pilot, TBS has ascertained that an API-based identity-management system that stitches and maps clients across different services—all of which use their own functional unique identification systems—in the back end is technically feasible. Under this the system mapping is

[41] "Brief Guide to the Tell Us Once Service," Golden Charter, February 2, 2017, https://www.goldencharter.co.uk/news-and-info/2017/brief-guide-to-the-tell-us-once-service/.

not automatically initiated; a client is mapped only when a user initiates an interaction with a once-only service. The client's full identity profile is known only to the system and is not stored anywhere it can be accessed by a government official; thus, the anonymity of the client is theoretically well-maintained. At this point such a system is still in its experimental phase, so it is unclear what the limitations to scaling up will look like.

From this pilot TBS hopes to get robust data that will further the board's understanding of what works and what doesn't. The pilot will also help create reasonable expectations about the benefits and risks of such a program in the Canadian context. The analysis and recommendations from this pilot will go to the senior officials to decide where the OOP program goes next.

5. Data-Sharing Mechanisms

Guiding questions:

- Why do countries need a data-classification framework and how can one be developed?
- What is the governance arrangement for data classification in your country?
- What are base registry systems, and what key decisions must be made when establishing them? What is a data-exchange system, and which data-exchange model makes the most sense given your country's OOP goals and current level of data-sharing maturity?

Further reading:

Carnegie Mellon University, Information Security Office, Guidelines for Data Classification
European Union, Access to Base Registries: Good Practices on Building Successful Interconnections between Base Registries
European Union, New European Interoperability Framework

At the core of OOP is the principal that personal data need only be collected once. Consequently there must be a mechanism by which data collected about individuals can be accessed by other government agencies.[42] Based on the countries examined in this report, two components are typically required to enable this capability:

- **Data classification:** This includes data structure—a set of standards to ensure that data is semantically uniform and thus understandable and usable across all departments and ministries—and data sensitivity, or a common set of rules across government departments that materially impact data access.
- **Data exchange:** A system of standard agreements and technical infrastructure across departments that make data exchange between government (and possibly nongovernment) actors possible.

For OOP to work beyond a few limited-use cases and to work across all of government, it is not enough to develop these components in an ad hoc manner. They must be—or at least must have the capacity to become over time—uniformly applicable across all government departments; this is what we refer to as a data-sharing mechanism that has achieved "future state" maturity. It is only when the overall data-sharing mechanism achieves such future-state maturity that OOP can be done at scale like one sees in Estonia and the Netherlands. To ascertain how mature the data-sharing mechanism in your country currently is, please refer to Table 5 below.

[42] Though this paper is primarily concerned with the data-sharing mechanisms used for personal data, this information can also be applied to public data.

Table 5: Maturity of the data-sharing mechanism

	Maturity of Data-Sharing Mechanism			
	Low	Medium	High	Future State
Data classification	No formal plans to develop standard systems and agreements.	Some departments are using the same data-classification standards, but they are one-offs.		Data classification across government is based on a common standard.
Data registries (personal data)		Data-sharing agreements are in place between a few departments, but they are one-offs	A few government departments have created private data registries that they make available to other departments	Data sharing between government departments is governed by standard rules and agreements and common practices among all departments
Data exchange		Data-exchange agreements are in place between a few departments, but they are one-offs	A few government departments have created private data registries that they make available to other departments	Data exchange between government departments is governed by standard rules and agreements and common practices among all departments

Source: Adapted from Eaves and McGuire[43]

5.1 Data Classification

Data classification refers to the process of organizing data using structure and sensitivity standards so that it may be used interoperably and in a way that considers its value. The classification process creates the foundational rules of how data is defined (i.e., the meta data, or what the data tells us), the data schema (i.e. the format it should have), how it should be stored, and how it can be retrieved and used. In light of the core privacy challenge that arises as countries implement OOP, data classification is of particular importance as it helps with data utilization, risk management, compliance, and security.

5.1.1 Moving Away from ad Hoc Approaches to Data Classification

In the absence of OOP, the ministerial and department sovereignty approach toward data classification holds sway. Under this, countries follow a decentralized, ad hoc model when it comes to developing a data-classification framework. In a once-only world, where use of data will be harder to pin on a specific ministry, stronger and more standardized guidance will be needed. The challenge is, few countries that have either already adopted or are advocating for a once-only policy currently have such standards in place.

[43] David Eaves and Ben McGuire, "Part 2: Proposing a Maturity Model for Digital Services (2018)," Medium, September 27, 2018, https://medium.com/digitalhks/part-2-proposing-a-maturity-model-for-digital-services-9b1d429699e7.

To move toward a more standardized data-classification model, data stewards—those responsible for the management and proficiency of data stored in an organization—across government departments involved with OOP must work together to create a common data-classification framework.

5.1.2 Developing a Common Data-Classification Framework for Data Sensitivity[44]

All data, including personal data, exists along a spectrum of open/shared/closed (see *The Data Spectrum*); where data is placed on the spectrum determines authentication and access rules. While some personal data, such as health data, may obviously belong at the closed end of the spectrum where only the data subject and a designated medical professional are permitted access, other personal data types are not so easily categorized. To better understand where various types of personal data is placed on the data spectrum, three primary questions must be answered:

- **Identifiability:** How easily can this data be used to identify an individual?
- **Vulnerability:** How much damage could be done if this data were to reach the wrong hands?
- **Scarcity:** How readily available is this data?

Generally, the sensitivity assigned to a particular collection of data is predicated upon the goals the classifying body is trying to achieve. Three major goals that are likely to be embedded in most sensitivity-classification approaches are confidentiality, integrity, and availability.[45]

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- **Availability:** Ensuring timely and reliable access to and use of information.

Combining the above goals with the data spectrum, I have developed a basic data sensitivity classification framework for personal data. This can provide a starting point for countries beginning to grapple with the issue of standardizing data-classification across government. This framework draws from the approaches of a range of public institutions, especially universities. The classifications range from "public" to "strictly confidential" and can be seen in greater detail in Table 6 below.[46]

Table 6: General data classification framework

	Public	Restricted	Confidential	Strictly confidential
Data identifiability, vulnerability, and scarcity	Low or no	Moderate	High	Severe
Data type	Data intended for public access	Data released on a need-to-know basis	Data with a statutory requirement of	Data that creates extensive "shared-fate" risk[47]

[44] The topic of data structure is a highly technical one. I have chosen not to address it separately in this document and instead have focused on the topic of data sensitivity.

[45] Jim Breithaupt and Mark S. Merkow, "Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability," *Information Security Principles of Success*, Pearson IT Certification, July 4, 2014, https://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=3.

[46] Some guidance as to how governments can place data collections within a single classification can be derived from the Creative Commons Open Data Release Toolkit. While this toolkit is meant to help countries decide when and how to release deidentified data, its Open Data Release Form shows how a similar framework can be developed internally for data classification more broadly. This document can be accessed at https://docs.google.com/document/d/1_K59q9ik5eEw9_-iiPCbQ8WSlGk0FovNz1uLajVHoi0/edit.

[47] Shared-fate risk applies to data that, if compromised, would cause further and extensive data compromise from multiple (even unrelated) sensitive systems. Information that is classified as a special category of

			notification if breached	
Data-type examples	Public information Public directory Scrubbed census data	Education records Driver's license	Unique identifier Financial information	Health and medical information Religious views Criminal activity
If disclosed or accessed without proper authorization	Are unlikely to cause harm to the individual or negatively impact the government's capacity to function	Are likely to cause minor harm or negative impacts to individuals or groups	Are likely to cause serious harm or negative impacts and/or harm the government's work	Are likely to cause severe harm or negative impacts and/or impede the work of the government
If improperly modified or destroyed (or if adequate standards of nonrepudiation and authenticity are not maintained)	Unlikely to cause harm	Likely to cause minor harm	Likely to cause serious harm	Likely to cause severe harm
If timely and reliable access to information is not granted	Unlikely to cause harm	Likely to cause minor harm	Likely to cause serious harm	Likely to cause severe harm
Government-wide access	Anyone can access or licensed public access	Group-based access allowed but only with authentication	Only named access is permitted with authentication	Not allowed or only allowed under extreme and tightly defined circumstances; most stringent safeguards in place
Individual access by data subject	Fully accessible	Accessible via low barrier for authorized individuals	Accessible only by authorized individuals (generally self) via login to prove identity	Accessible via extremely high barrier to access

The major concern that determines what sensitivity level a collection of data is assigned is the level of harm that it causes to the individual and/or the work of the government across the core goals of the system. However, what constitutes harm within the context of the framework is open to deliberation, and not an easy judgment to make. Averaging harm is difficult because what constitutes harm changes depending upon the country context and the perspective of the entity considering the issue (e.g., government department vs. individual user). Fundamentally, harm is a sliding scale as opposed to an absolute measure. Equally important, as society becomes used to the idea of making personal data public due to widespread use of social media, its conceptions of where certain types of data fit will change over time.

When assigning data-sensitivity classifications, data stewards should consider following some simple procedures:

- A collection of data that is common in purpose or function should be assigned a single sensitivity. During sensitivity classification of a collection, the most restrictive sensitivity classification of any of the individual elements should be used.

personal data according to Article 9 of the GDPR (including data relating to race, religion, sexual life, health, genetics, and biometrics) and personal data related to criminal activity and offenses according to Article 10 of the GDPR are likely to have a "severe" data-sensitivity rating.

- The assigned data-sensitivity classification of a collection should be reviewed periodically to help ensure it is in line with the most up-to-date legal framework and/or prevailing perceptions of the value of the data to all concerned parties.

5.1.3 Registries: An Example of Robust Data Classification

Registries are trusted and authoritative sources of information under the control of a public administration or organization.[48] Registries are distinguished from other data repositories, such as databases, reports, and lists, as they are the only "authoritative list of a specific type of thing."[49] Registries can be formed around data on persons, vehicles, licenses, buildings, and more.[50]

Registries expose the data held within APIs to agreed-upon open standards and have appropriate governance and ownership in place. Separately or in combination, registries form the cornerstone of public services and are an enabler for OOP. They provide quality data upon which other services can then be built. As authoritative sources of trustworthy core data they provide a standard way of defining, accessing, and using needed information and thus are an example of robust data classification in terms of both data structure and data sensitivity. More specifically, registries allow for version control, data availability, and format consistency. Over time, departments aiming to leverage the benefits of data-sharing should replace individual databases and lists with common registries.[51]

> **Where we see this:** In the Netherlands, a system of base registries, or *Basisregistratie*, sits at the heart of the country's data-sharing infrastructure. The system has ten registries, each describing a specific data domain within the government such as large-scale topography (buildings, roads, waterways, etc.), income-tax filings, land ownership, vehicles, and so forth. Every registry has a source holder—a municipality or the water board, for example. These source holders collect the data, check it, and make it available to the registry. All government agencies must connect to the base registries to make use of this data.
>
> One of the 10 registries, the *Basisregistratie Personen* (BRP), or Personal Records Database, tracks the personal data of all Netherlands residents. For each individual the BRP includes name, date and place of birth, address, and familial relationships. This is by far the most leveraged of the ten base registries, being accessed by everything from pension funds to research and educational institutions.
>
> The registries were created as part of the 1998 Electronic Government Action Programme.[52] Each registry is governed by specific laws that lay out the conditions and limitations of its use, and a

[48] Paul Downey, "Registers: Authoritative Lists You Can Trust," Government Digital Service, September 1, 2015, https://gds.blog.gov.uk/2015/09/01/registers-authoritative-lists-you-can-trust/.

[49] Paul Downey, "The Characteristics of a Register," Government Digital Service, October 13, 2015, https://gds.blog.gov.uk/2015/10/13/the-characteristics-of-a-register/.

[50] "Access to Base Registries: Good Practices on Building Successful Interconnections between Base Registries." European Commission, 2016. https://ec.europa.eu/isa2/sites/isa/files/publications/access-to-base-registries-good-practices-on-building-successful-interconnections-of-base-registries.pdf.

[51] Ade Adewunmi, "Making Data a Public Asset through Infrastructure," Government Digital Service, November 3, 2015, https://gds.blog.gov.uk/2015/11/03/making-data-a-public-asset-through-infrastructure/.

[52] eGovernment Factsheets, "eGovernment in The Netherlands," April 2014, https://joinup.ec.europa.eu/sites/default/files/document/2014-06/eGov%20in%20NL%20-%20April%202014%20-%20v.16.pdf.

single government system catalogue shows what data the base registry system contains, what the data means, and how the system is interconnected.[53]

[53] "System Catalogue," *Digital Government*, Netherlands, accessed September 29, 2020, https://www.nldigitalgovernment.nl/dossiers/system-catalogue/.

5.1.4 Characteristics of Base Registries

Not all data can go into a registry. Registries are not suitable for data that is primarily used by a single department for internal use. Data linked to outcomes (for example, organizations that can sponsor H1B visas in the United States) or reference data—such as the building ownership registry—are the most appropriate for registries.[54]

Several characteristics typify a base registry:[55]

- **It's canonical and has a clear purpose**: Is the only authoritative list of a specific type of thing. As the primary source of information, it is kept accurate and up to date. The core role or function that its existence fulfills is clear.
- **It has a minimum number of viable datasets**: Only ever holds the data it was created to record, meaning that mission creep almost never occurs. It does not duplicate information held in other registries though it can link to other registries. To make this happen, "each record in a registry must have a stable, unique identifier."
- **It's a live list of usable data**: Is digital, accessible, and searchable via API. From a user experience point of view all registries should follow a standard querying and reading format.
- **It can provide data integrity**: Each individual entry is immutable, thereby acting as a digital proof of record.
- **It contains raw, not derived, data**: Only holds factual raw data not any form of derived data, or other information.
- **It must have a custodian**: A single government department / ministry / agency is responsible for the maintenance and upkeep of each registry.
- **It's classified as open, shared, private, or closed**: This classification aligns with the data spectrum shared earlier and is similar to that shown in Table 7 below.
- **It can be linked or unlinked**: While linked registries simplify the data that a single organization needs to hold, they also demand trust and coordination across various organizations. Semantic agreements and technical standards must be in place for linked registry models to emerge.
- **It uses standard names consistent with other registries**: Reuses standard names for fields to enable discovery across linked registries.

Table 7: Registry classification

Registry classification	Description	Access
Open	The registry is public	Can be accessed by anyone
Shared	Registry allows access to a single register entry	Some form of access-control is instituted
Private	Cannot be accessed directly by services	Some form of access-control is instituted. That is, only answers to simple questions are provided; the full registry is not exposed
Closed	Is private to a single organization	Locked away and not connected to a digital service

Finally, to maximize its value, a base registry must be:

- **Highly visible**: It should be easy for users and organizations to discover if a registry exists, and to understand the process they need to follow to access the registry.
- **Open to public scrutiny**: There should be a clear process for challenging data held in the registry, with high standards for transparency, adjudications, and the processing of other issues easily discovered by users with data in the registry.

5.1.5 Creating a System of Base Registries

To get the maximum value out of a system of base registries, governments should settle on a clear governance mechanism and lay out a clear process for the development of base registries.

Creating centralized governance for base registries. Under this governance system, a central body facilitates the creation of registries across government by providing valuable guidance, ensuring that registries are kept up to date, and maintaining a master catalogue of all registries. This body helps to develop and institute the various legal, organizational, technical, and semantic standards that must be adhered to create a registry-rich ecosystem.

Four categories of standards need to be addressed to create a system of base registries:[56]

- Legal: Compliance with legislation, bridging legislation, service terms and conditions, data-sharing principles
- Organizational: Organizational structures, collaboration, service-level policies, governance processes, business models
- Semantic: Vocabularies, code lists, glossaries, identifiers
- Technical: Network for data transports, interconnection architecture, standards for data exchange, security

Establishing a process for creating a new registry. When considering creating a new registry, departments should answer the following questions to maximize effectiveness:

- What is the purpose of the registry?
- Does the registry duplicate existing data?
- Does the registry constitute a minimum viable dataset?
- What is the registry classification?
- Where would the registry reside?
- How will the registry be kept up to date?

Where we see this: In the UK, registries are centrally governed by the Government Digital Service (GDS). Departments that want to make a registry out of data they own must submit a formal request to GDS. [57] Assuming the registry meets a user need and is managed by the right department, GDS will accept the request and appoint a departmental custodian who is responsible

[54] "Making Data a Public Asset through Infrastructure."
[55] Paul Downey, "The Characteristics of a Register."
[56] "Access to Base Registries: Good Practices on Building Successful Interconnections between Base Registries," European Commission, 2016, https://ec.europa.eu/isa2/sites/isa/files/publications/access-to-base-registries-good-practices-on-building-successful-interconnections-of-base-registries.pdf.
[57] Government Digital Services, "Creating a register," gov.uk, July 29, 2016, https://www.gov.uk/guidance/creating-a-register.

for the day-to-day upkeep. GDS will work with the custodian to define the registry, ensure it is not duplicative, and build it according to the technical standards laid out by GDS. The registry will ultimately be published by GDS, which will grant the custodian access to a registry-management tool so that the registry may be kept up to date.

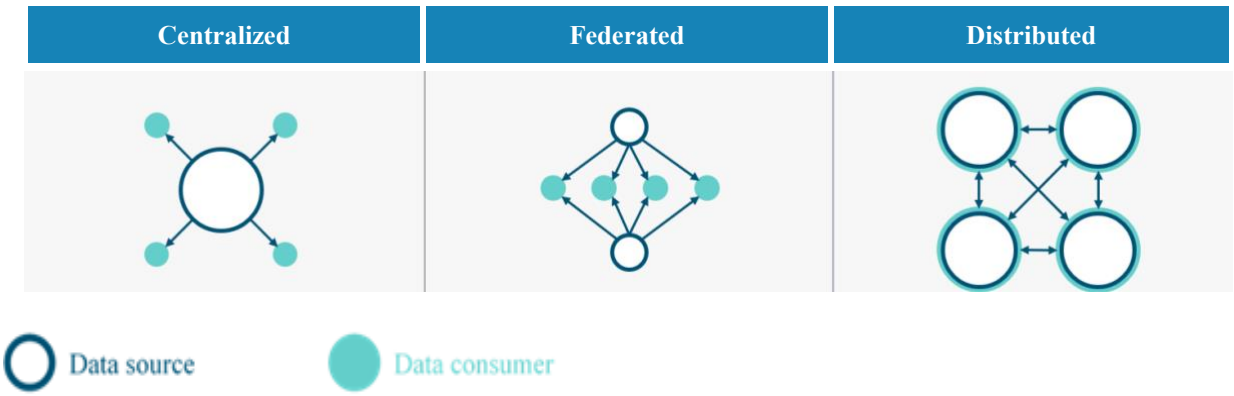
5.3 Data Exchange

The data exchange is the system that allows government departments to build a pipeline of data-collaboration projects with other departments across various layers of government (e.g., central, provincial, local).

5.3.1 Data-Exchange Approaches

There are three distinct data-exchange and accompanying governance approaches that countries can adopt (see Figure 4). Each of these comes with its own unique benefits and drawbacks as it relates to OOP implementation.

Figure 4: Data-exchange approaches



Source: Tell Us Once Data Sharing Models, TBS Canada[58]

5.3.1.1 The Centralized Approach

Under this model all data is centralized under a single data authority, which is the only reliable source of resident data. Parties that rely on the data make direct requests to the authority for data access.

Benefits: Under a centralized approach there is no need to standardize processes and systems, since this is an automatic feature. Any data changes can be quickly reviewed and approved by the data authority. Users can easily configure their data-sharing consent settings once.

Drawbacks: A centralized system is hard to institute and operate, particularly for countries that have traditionally followed ad hoc data-exchange solutions. At a basic level, buy-in and strong intergovernmental cooperation is required. Since centralized systems create a single honeypot of data, robust security is a must. Additionally, a strong technical solution is needed to support centralized systems, since there is likely to be a great deal of pressure on them as the only reliable source of resident data. The requirements of robust security and a strong technical basis

[58] Treasury Board Secretariat of the Government of Canada, "Tell Us Once Data Sharing Models EN.Docx: GCcollab," April 16, 2019, https://gccollab.ca/file/view/2134475/tell-us-once-data-sharing-models-endocx.

will make the system expensive to implement and operate. Under a centralized exchange the data authority has a complete picture of a user, which dramatically increases the power of the state and the risk to the user.

Assessment from OOP standpoint: Though a centralized data exchange approach would streamline OOP implementation efforts and work for both foundational and functional OOP approaches, it is **not recommended** from a privacy or feasibility standpoint. While there are examples where a centralized approach is used internally by individual government departments or services, to our knowledge the centralized approach has not emerged at a federal or governmentwide level and so is **largely theoretical**.

5.3.1.2 The Federated Approach

Under the federated approach a canonical data source is designated for each piece of resident data (e.g., home addresses). Each data source lies with a specified data authority that is responsible for the management, administration, and reconciliation of data under its purview. All data sources are independent but linked and are queried when needed by the party relying on the data.

> **Where we see this:** Estonia's X-Road—an open-source software and ecosystem solution that provides unified and secure data exchange between organizations,[59] while precluding the need for data centralization (see Section 5.3.2)—is the definitive example of a data-exchange solution that links several data authorities in a federated environment. A system of base registries (see Section 5.1.3) underlies X-Road.

Benefits: The federated approach is a balance between the convenience of the centralized approach and the privacy-optimization of the distributed approach. Under a federated approach no single honeypot of data is created as different "sources of truth" rest under different departments and authorities. By and large, data is held only once in this model, though some basic information may have to be recreated. A central, crossroads interface such as X-Road is required to make the federated model work and is relatively cheap to implement. Data exchange will be possible with less standardization than is required for interoperability under a distributed approach.

Drawbacks: As noted earlier, some information will have to be recreated by each department; the manner in which this is done, and the information stored, could have an adverse impact on privacy and security unless appropriately governed. Since the system is highly dependent on canonical sources, these will have to be sufficiently strong and based on high-quality data. Additionally, the canonical sources will have to be kept updated, with any changes reflected in real time or close to real time.

Assessment from OOP standpoint: In my view, a federated data exchange is the optimal way of implementing OOP, especially the principle approach.

5.3.1.3 The Distributed Approach

Under the distributed approach, every department has its own version of resident data. Mechanisms for data sharing are not built into the system and thus must be developed anew for each department. This model usually evolves in an ad hoc manner and is not necessarily intentionally designed as a distributed system.

Benefits: No single honeypot of data is created.

Drawbacks: Departments must hold relatively complete profiles of individuals to service them; from a privacy and security standpoint this creates additional weaknesses in the system. Since data-sharing channels are not automatically built into the distributed approach, both technical and semantic standards must be standardized across departments to allow data sharing to begin.

[59] "X-Road Data Exchange Layer," accessed October 4, 2020, https://x-road.global.

Assessment from OOP standpoint: While not appropriate for a principle approach to OOP, programs based on limited bilateral or multilateral data-exchange arrangements may be launched under such a system.

5.3.2 X-Road: An Example of Federated Data Exchange

Introduced in 2001, [60] X-Road is the backbone of the Estonian digital government, ensuring secure and direct internet-based data exchange by creating an enabling technological and organizational environment within which members can interact. Inherently modular, X-Road allows both public- and private-sector organizations to join the system.

X-Road allows members to obtain master data from canonical data sources. Originally used to query separate databases and computer systems, X-Road now also has the ability to write to multiple databases, transmit large data sets, and perform searches across several databases. Each X-Road member has its own secure server, and an "adaptor" or translator that sends and receives information in the X-Road format (see the schematic structure of the X-Road).[61]

X-Road is:

- **Autonomous**: Members define the data services they want to use and who interacts with them;
- **Confidential**: Only authorized parties are sent information;
- **Secure**: All received data is tagged with an e-signature to prove its source;
- **Interoperable**: The adaptor ensures that all X-Road members can interact;
- **Ensures no vendor lock-in**: Members do not have to use a specific type of database or software provider to leverage X-Road;
- **Open source**: X-Road is open source and has been published under an MIT license since 2016;
- **Cheap**: X-Road is cheap to set up and operate; the entirety of the system, including maintenance costs, salaries, and investments, costs the Estonian government less than $68 million a year in a total budget of $8 billion.[62]

[60] "Estonian data exchange layer for information systems (X-Road)," SCOOP4C, accessed June 21, 2020, https://scoop4c.eu/cases/estonian-data-exchange-layer-information-systems-x-road.

[61] Wen Hoe, "E-Stonia: One Small Country's Digital Government Is Having a Big Impact," Government Innovators Network, June 7, 2017, https://www.innovations.harvard.edu/blog/estonia-one-small-country-digital-government-having-big-impact-x-road.

[62] "E-Stonia: One Small Country's Digital Government Is Having a Big Impact."

6. Developing an OOP Roadmap

Guiding questions:

- How can countries lay the foundation for a multiyear OOP roadmap?
- Who is leading the work?
- How can countries choose the "right" use case?
- What are the key service design choices, interactions, and tools related to OOP deployment?
- In the long run, how can countries plan for scale, streamline, and get ready for large-scale OOP deployment?

Further reading:

European Union, Study on eGovernment and the Reduction of Administrative Burden
European Union, EU-Wide Digital Once-Only Principle for Citizens and Businesses

Implementing OOP is a herculean effort—one that will take years, possibly decades. Doing so at scale across government, where OOP is the default for all appropriate services and can thus create the GaaP benefits articulated in Section 1.2, is an even tougher proposition.

To achieve OOP at scale, besides the development and implementation of the core elements—namely a privacy framework, an identification mechanism, and a data-sharing mechanism—a broader, staged OOP roadmap that outlines key questions and issues, policy areas, and strategic considerations over time is needed.

6.1 Staged OOP Roadmap

For simplicity's sake I have divided the roadmap into two phases: short-run and long-run. Additionally, five key policy areas (see Section 6.1.3) will have to be addressed on an ongoing basis across both phases.

6.1.1 Short Run: Laying the Foundation

To begin their OOP journey, countries should attempt to define the endpoint they want to achieve by creating a vision for the next 10 years. According to the current state of the core elements privacy, identification, and data sharing, countries can determine whether starting with a principle or program approach is most appropriate and create a plan to strengthen that approach over time. Beyond this, to launch OOP, key issues to be addressed include the following.

Creating a governance model

A study across OOP-implementing European countries noted a trend of centralizing OOP governance efforts under one or more departments or ministries that are committed to leading OOP efforts.[63] The designated government body provides leadership, direction, and guidance to all interested departments, often in combination with a "whole-of-government" approach, integrating various administrations' online services and establishing some form of one-stop government can take place in tandem.

[63] European Commission, "Final Report: Study on EGovernment and the Reduction of Administrative Burden (SMART 2012/0061)," Shaping Europe's digital future, April 8, 2014, https://ec.europa.eu/digital-single-market/en/news/final-report-study-egovernment-and-reduction-administrative-burden-smart-20120061.

Choosing the "right" use case

Part of the short-run strategy will be deciding on a use-case identification procedure and figuring out how to sequence the development of OOP use cases. There are several options for choosing the "right" use cases, and countries will have to assess what makes the most sense in their context. On the one hand, interested governments may choose to pursue use cases that are low-hanging fruit and can be executed relatively quickly and inexpensively. An alternative but still useful approach would be the one Canada chose—to demonstrate success by working with willing ministries and agencies across governments first, since they have already bought into OOP. Finally, OOP delivery units could choose to target OOP cases by assessing which cases represent the biggest pain points for users and are most likely to deliver results, as the UK did. Once a procedure is chosen, building out one or two use cases around which to adopt a test-and-iterate approach will help determine the future OOP development path.

Service design: Key choices, interactions, and tools

The way an OOP service is designed has a material impact on both the value of the system to the user and how privacy enhancing it is.

An early design choice must be made around the topics of enrollment and consent.

Enrollment refers to the question of how users enter an OOP service.

- Opt-in: Service users are asked if they want to be enrolled in any connected OOP programs at the point of use of a particular service. For example, when users provide their address for an OOP-enabled social service, they will be asked if they would like to also update their address across other services and will be able to specify which services they want to provide this permission for. This is the system that is currently being designed in Canada.
- Opt-out: All users of an OOP-enabled service are automatically enrolled in connected OOP programs and have the option of opting out if they want. This is the system that is currently being designed in Estonia and the Netherlands.

Consent refers to the question of how consent for use of an individual's private data for OOP is obtained.

- Program-based consent: Consent is given every time customers share or update their information with an OOP-enabled service to ascertain with which departments this new information can be shared and for what purposes it can be used.
- Blanket consent: If service users share or update their information with one OOP-enabled program, it is assumed they have consented to have this new information shared with all OOP-activated programs.

There are a few interactions that should be built into any OOP service. As identified by TBS Canada's OOP pilot project, the most basic interactions are:[64]

- Sign-in using a trusted identity authentication and verification method
- Self-service client profile management
- Information sharing
- Verifying relationships between different entities (e.g., allowing one individual to act on behalf of another, or allowing an individual to act on behalf of a business).

Beyond just building these interactions, implementers must consider two key perspectives when designing the system: the government-centric view and the user-centric view. A few useful tools that can help regulate and

[64] These interactions were identified by TBS Canada as part of its ongoing user-experience-focused experimentation around OOP. Some useful visual flows outlining these interactions can be found in Appendix 2.

enhance the experience for both parties; with each, it is important to find the right balance between providing much-needed value and overwhelming users with a huge amount of information.

- Platforms for personal access and control: One way to give users greater control of their data is to develop a multichannel platform or portal where individuals can log in to view all the data the government holds on them and monitor how it is being used.[65] This can provide enormous value by establishing transparency and thereby ensuring accuracy, trust, and safety. In addition, such a console can be used to let customers to change their consent settings pertaining to various data and even edit some fields of information, such as address, if needed.

  > **Where we see this:** In Estonia, citizens and residents can see—and correct if needed—almost all data about them held by the government by logging into the State Portal (eesti.ee). Users can also control which data is shared by whom.[66]

- Tamper-proof logs: To ensure that only authorized individuals can access users' personal data, all government use of an individual's data will be tracked, recorded, and shared on the centralized portal. This log will ensure that citizens become more comfortable with the use of their data, and that government employees will be held to account and prevented from misusing data.

  > **Where we see this:** In Estonia, users can see who has viewed their data on the state portal's Personal Data Usage Monitor. Any illegal viewing or tampering with an individual's personal data is punishable by law. According to some sources, proactive notification is sent to users if their information is accessed, but how this works functionally is unclear. An accessible open registry underpinning Estonia's state portal shows the "profile information that is held in each government system, what reason it is held for, and who it can be accessed by."[67]

6.1.2 Long Run: Planning for Scale

The goal of this second strategy is to refine OOP and ensure that a large-scale OOP deployment is feasible from the standpoint of both technology and equity. Note that while the specifics of the plan will change depending upon a country's particular context, the general issues highlighted are universally applicable.

Streamlining OOP

Streamlining makes interactions between government and users as simple and maximizes their value as much as possible. Realistically, this can happen only once the core underlying infrastructure and standards are in place, and the back-end system is successfully and integrated. The purpose of streamlining is to improve existing use cases, and leveraging the lessons learned from them to expand the number of total OOP use cases in the country. Concepts to examine in this phase include user-centered design, service personalization, and process simplification and reduction.

Ensuring OOP Feasibility at Scale

Both the general digital ecosystem and the OOP ecosystem must be sufficiently strong to make OOP at scale a feasible option. Key issues to examine in this phase include:

- Implementing widespread, high capacity, and affordable ICT infrastructures and systems;

[65] "Platforms for personal oversight," Identification for Development, The World Bank, accessed July 21, 2020, https://id4d.worldbank.org/guide/platforms-personal-oversight.

[66] Peter Herlihy, "'Government as a data model': what I Learned in Estonia," October 31, 2013, https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/.

[67] "'Government as a data model.'"

- Supporting individuals who are not digitally enabled by providing both access and equipping them with the necessary skills;
- Selecting an appropriate business case that will ensure the financial viability of OOP at scale.

6.1.3 Key Policy Areas

Five primary policy areas need to be addressed for successful OOP implementation in both the short and long term; [68] if left unaddressed they will create barriers to implementation.[69]

Legal basis: Ideally, special consideration and permissions for OOP should be built into the privacy framework and identity regulations. Additionally, countries should pass OOP-specific regulation that lays out the in-country definition and creates a legal basis for operation to ensure that OOP is sufficiently controlled.

Good governance: Strong governance helps account for the complexity and costs of an OOP deployment. Clear demarcation of authority positions and roles is important to ensure that coordination within and across departments flows smoothly.

Technical feasibility: Knitting together databases and turning them into registries will be challenging, and if the information in the registries is not high quality there is a significant risk that officials will opt out of using the system.

Public trust: Since OOP by nature is customer-facing and has serious implications for data privacy, it is important for the project that citizens be comfortable with how their data is used under this system. High levels of transparency will help create trust and long-term buy-in from the user end.

Political and implementer buy-in: Given the complexity of OOP, particularly the demands that creating and inserting new standards will create, at a high level a great deal of political buy-in is needed to ensure that different government departments will participate actively in this approach. Moreover, even if there is support at the top for OOP, many departments and ministries may resist losing "control" over data and not having their own "canonical" source. It is necessary to shift the culture to one of cross-departmental cooperation and to acknowledge that whole-scale OOP implementation is likely to transcend the term of a given political party. To combat this, broader political and public buy-in will have to be secured early on.

Beyond these policy areas, from a deployment perspective the privacy concerns related to OOP implementation and the need for broader buy-in to make it work in the long run mean that robust and continual monitoring of OOP, and identification and communication of related quick-wins, will be useful.

[68] These areas encompass the primary elements for a successful OOP deployment as identified by the EU's Stakeholder's Community of Once-Only Principle (SCOOP4C).

[69] European Commission, "EU-Wide digital Once-Only Principle for citizens and businesses—Policy options and their impacts," Shaping Europe's digital future, February 1, 2017, https://ec.europa.eu/digital-single-market/en/news/eu-wide-digital-once-only-principle-citizens-and-businesses-policy-options-and-their-impacts.

Strategic Considerations for the OOP Roadmap

Monitoring: Monitoring rollout is necessary to assess and quantify both the monetizable and nonmonetizable costs and benefits of OOP on an ongoing basis. Using a uniform approach—including the standard cost model, impact analysis, customer satisfaction surveys, and the business-case approach—will allow implementing bodies to compare and contrast different strategies.[70]

Quick wins: Quick wins will help propel OOP utilization in specified use cases across government. However, any quick wins must be undertaken with care to ensure that they do not impede long-term goals.

6.1.4 Bringing It All Together

To show how the composite pieces—phases, key policy areas, and strategic considerations—come together, I have developed a sample visual roadmap guide as depicted in Table 8 below.

Table 8: Sample OOP roadmap

	Short-run Laying the foundation	Long-run Planning for scale
	Begin OOP experimentation.	Refine OOP implementation and ensure that achieving scale is a feasible option.
	• Establishing a governance model • Choosing the right use case to start • Designing the service	• Streamlining and simplifying OOP deployments • Ensuring OOP feasibility at scale
Legal basis	Create a legal basis for OOP deployment.	Establish enforcement to ensure that OOP systems are used across government and that information is both collected once and stored once. Balance strong enforcement against clear exceptions to avoid digital exclusion.
Organizational changes and good governance	Ensure clear roles and authority demarcations between entities.	Ensure enforcement and coordination at the top; anticipate future problems by establishing mechanisms for change and risk management
Technical feasibility	Ensure that information in registries is high quality so that departments can move toward a "store once" model.	Maintain and improve upon high technical feasibility as an increasing number of services become OOP-enabled.
Public trust	Educate the public on OOP to create transparency around the system, and to engender knowledge and trust among citizens.	Ensure a high level of trust in ongoing OOP deployments by adapting service design according to the needs of users.

[70] "Final Report."

Political and implementer buy-in	Obtain long-term, high-level political buy-in for the OOP implementation. Identify willing implementers who are willing to be involved in the first use case.	Create the culture change that is needed to scale OOP across government
Monitoring	Create a standardized approach to track progress and make ongoing adjustments to service design and the business case. Examples of the metrics that should be monitored include where and how costs are incurred and identifying anything impeding results.	Continue monitoring efforts and adjust as needed. Examples of the metrics that should be monitored include which services are getting the most use and why.
Quick wins	Identity high-value, low-input OOP efforts and deploy accordingly.	Bring services using registry data and users with high service needs into the OOP net.

6.2 Conclusion

6.2.1 Lessons About Iteration from a Mature OOP Country

The Netherlands has one of the most mature OOP environments in the world. The Dutch OOP policy is built on three core enablers:[71]

- The **Dutch GDPR Implementation Act**, the broad data-privacy and data-protection law enforced by the Dutch Data Protection Authority (DPA).
- A unique **national number** that is the central identifier by which every governmental service is linked to specific citizens.
- A **system of base registries** that sits at the heart of the country's data-sharing infrastructure.

While the core enablers have been in place for a while and can be updated as needed, even in an OOP context as advanced as the Netherlands' there are still questions about how OOP is operationalized. Two outstanding questions that are constantly being debated in the public sphere are whether privacy is being adequately maintained and what level of data-visibility should be granted to citizens.

On the issue of maintaining privacy, over and above a set of core principles, it's clear that there is a need for constant oversight and review. For example, at one point, the Dutch tax agency started accessing and tracking data about citizens using commercially leased cars outside their radius to make tax rulings. This became extremely controversial and a standing policy now recognizes it as an unaccepted usage of data. Regarding other privacy issues, the Netherlands is still navigating its way forward. A major issue appears to be departments creating copies or shadow registries from the primary system. Making sure these are used in privacy-compliant ways is extremely difficult, but it's also hard to stop this from happening and force departments to use only one system.

On the issue of data visibility, the Netherlands recognized that individuals should have visibility control over their own data, but the degree to which this is feasible in practice is questionable. Through the centralized MyGov portal,

[71] To better understand the Netherlands' OOP environment, I spoke with Wouter Welling, a digital government policy officer working for the Ministry of the Interior and Kingdom Relations. For additional examples from the Dutch and Estonian OOP experiences, please refer to Appendix A2.2.

individuals can see what information is held about them in various registries, and they'll eventually be able to see when this information is accessed.[72] While there is a policy-level intention to proactively notify citizens every time their information is used, there are so many calls on data on any given day that this is not possible. Instead, the government allows people to send in a request for a paper review of their past year's personal data usage, which discourages excessive calls. Of course, if every citizen were to make a paper request, the entire system would likely collapse.

6.2.2 Looking forward

The examples above show that, as with any product or service, the creation of the core infrastructure, essential principles, and basic user experience are only the first step toward ensuring success.

Constant public debate and improvement are needed to ensure that user value continues to be created. Creating an OOP deployment is not an easy task, but it is one that can propel governments into the next phase of digitization. Governments around the world are increasingly experimenting with OOP. Some countries have made big advances in this space, but each nation will face its own set of challenges, especially vis-à-vis privacy, and an OOP model cannot simply be recreated without accounting for the local context.

I hope this document provides some guidance regarding the main elements countries need to put in place for successful OOP implementation and raises some questions that implementers and relevant civil society actors must ask themselves to ensure that each element is as privacy-optimizing as possible.

As always, continuous iteration is the key to success, and as OOP-implementing countries start on their journey, new areas of concern will appear, and strategies will have to change accordingly. A world in which users can reap the many benefits of OOP in a privacy-enhancing way lies before us.

[72] It is not yet possible to see every request for personal information in each registry. This functionality is currently under development. At the moment, citizens can see which organizations have access to their personal information and under what law.

Appendix 1

A1.1 Digital ID Evaluation Framework

This table is derived from the evaluation framework designed by India's Centre for Internet and Society.[73]

Rule of law tests	
Legislative mandate	Is the project backed by a validly enacted law?
Defining actors and purposes	Does the law clearly specify the actors and purposes?
Legitimate aim	Are all purposes flowing from a legitimate aim identified in the valid law?
Redressal mechanism	Does the law provide for adequate redressal mechanisms against actors who misuse the digital ID?
Accountability	Are there adequate systems for accountability of governing bodies, users of digital ID, and other actors?
Purposes	If legitimate aims for digital ID correspond to its specific purposes, does the project restrict itself to uses directly related to such purposes?
Mission creep	Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in use of digital ID?
Rights-based tests	
Necessary and proportionate privacy violations	Are the privacy violations arising from the use of digital ID necessary and proportionate to achieving the legitimate aim?
Access control	Are there protections in place to limit access to the digital trail of personally identifiable information created using digital ID by both state and private actors?
Data minimization	Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital ID?
Exclusions	Are there adequate mechanisms to ensure that the adoption of digital ID does not lead to exclusion or restriction of access to entitlements or services?
Mandatory use	Are there any valid legal grounds for making enrollment in and use of digital ID mandatory?
Risk based tests	
Risk assessment	Are decisions regarding the legitimacy of uses, the benefits of using digital ID, and their impact on individual rights informed by risk-assessment?
Proportionality	Do the laws on digital ID envisage governance in proportion to the likelihood and severity of the possible associate use risks?

[73] "Digital Identities: Design and Uses," accessed October 8, 2020, https://digitalid.design/evaluation-framework-02.html.

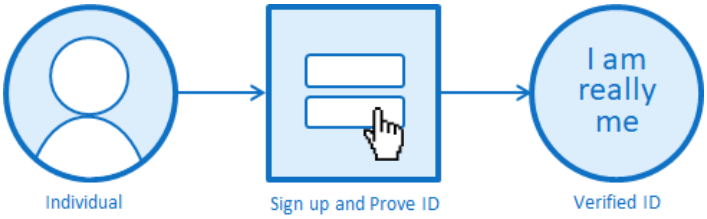
Response to risks	Are there mechanisms in place to prohibit or restrict the use of digital ID in demonstrably high-risk situations?
Differentiated approaches to risks	Do the laws and regulations envisage a differentiated approach to governing the uses of digital ID based on the likelihood and severity of risk?

Appendix 2

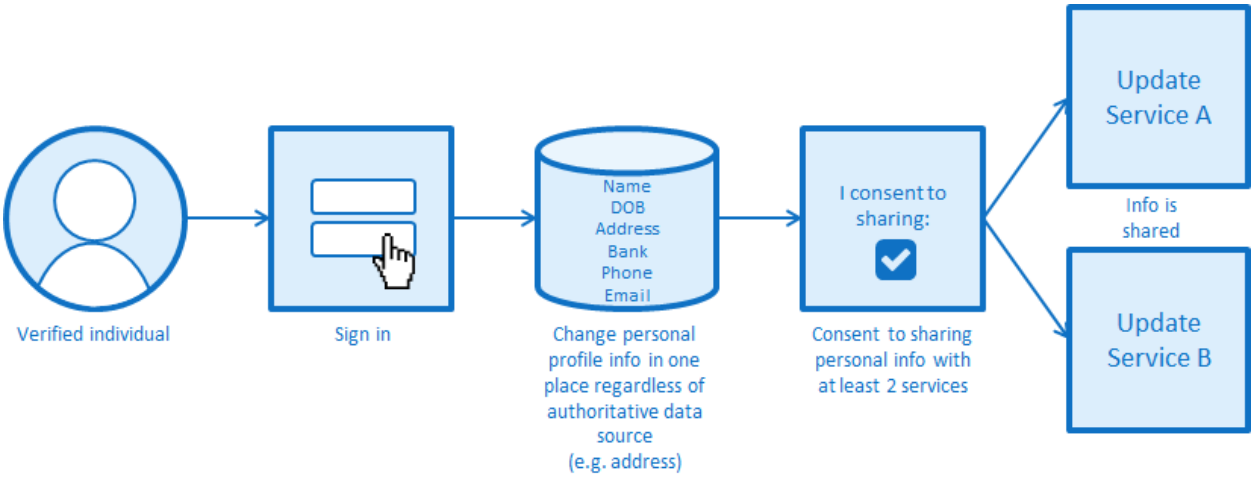
These interaction flows were identified and designed by the Treasury Board Secretariat team piloting the Once-Only Policy in Canada.[74]

A2.1 Mapping Core OOP Interactions

Sign-in using a trusted digital identity

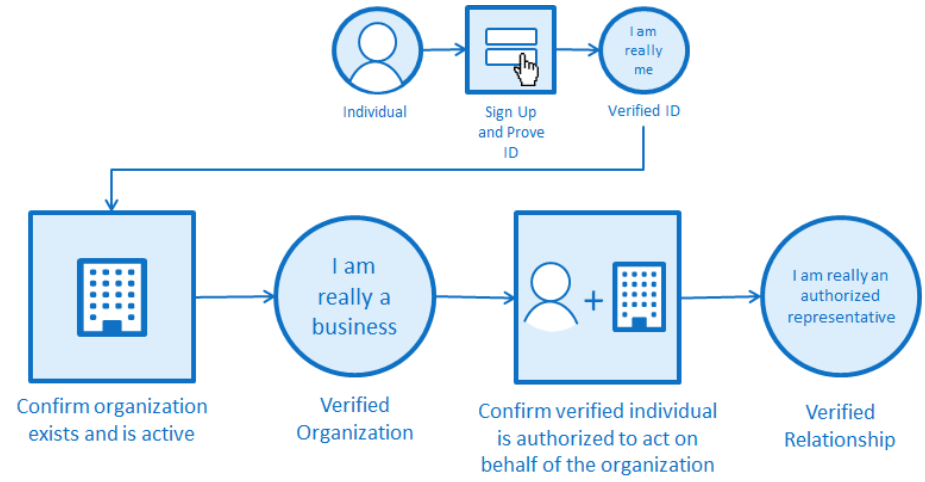


Self-Service Client-Profile Management

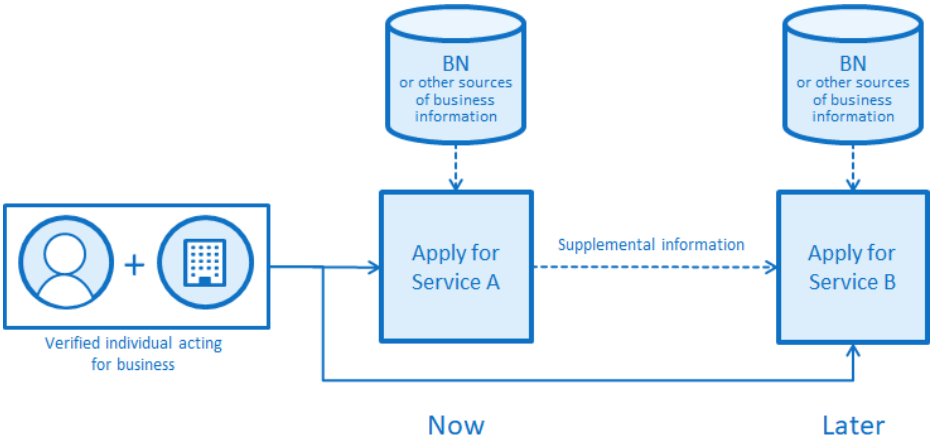


[74] Treasury Board Secretariat of the Government of Canada, presentation, "Tell Us Once Prototype Leadership Update," February 11, 2020.

Information-Sharing



Verifying Relationships between Various Entities



Note: "BN" in diagram above refers to "business number."

A2.2 Additional OOP Case Studies from the Netherlands and Estonia

These case studies are the result of additional research into the Netherlands' and Estonia's once-only landscapes.

Country	Netherlands	Estonia
Use case	Personal records database (BRP)	Health database
Privacy framework	GDPR The Dutch GDPR Implementation Act Enforcement by the Dutch Data Protection Agency	GDPR Personal Data Protection Act Enforcement by the Data Protection Inspectorate

Identification	Foundational unique identifier (*burgerservicenummer*) connected to DigiD for citizens Foundational unique identifier KvK, or Chamber of Commerce number, for businesses; it is linked to the eID for businesses known as the eHerkenning	Foundational unique identifier connected to eID, Mobile ID, or Smart ID
Data classification	Yes, via the BRP	Yes, via registries
Data exchange	Exchange based on the system of base registries	X-Road
Key tools used in use case	MyGovernment Portal Access to BRP is logged	e-Patient Portal Access is both limited to doctors and tracked.

A2.2.1 Personal Records Database (BRP) in the Netherlands

What is BRP?

- One of the ten basic registries in the Dutch system of base registries
- Contains the data of people who live in the Netherlands

Information collected:

- Name, date of birth, place of birth, place of residence, family relationships, travel document, and voting eligibility[75]
- Information is collected permanently

Legal basis and governance:[76]

- Established by the Base Registrations of Persons Act and now under the Personal Records Database Act
- Source holder: municipalities
- Lead supervisory authority: Data Protection Authority
- Provider: National Office of Identity Data

Accessibility limitations:

- Only organizations with a public or social function can access data held in the BRP, which sets the rules for access. Organizations can view only the data they need to do their work.
- Organizations can request access to BRP. These requests are reviewed by the National Office for Identity Data, which judges the organization's ability to access against a series of technical and policy requirements.

[75] Government of the Netherlands, "What Information Is in the Personal Records Database?" accessed October 12, 2020, https://www.government.nl/topics/personal-data/question-and-answer/what-information-is-in-the-personal-records-database.
[76] "BRP," Digitale Overheid, accessed September 27, 2019, https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/basisregistraties-en-afsprakenstelsels/inhoud-basisregistraties/inhoud-brp/.

If the requesting organization meets the requirements, the Ministry of the Interior and Kingdom Relations will create an authorization table for it that states which information is provided to the organization for which tasks.[77]

- Access to the BRP is tracked. To prevent abuse of the data, a record is kept of anyone who sees or changes it. A record of any organization that accesses the BRP is kept for 20 years.[78]

User (citizen and resident) access:

- Initial registration is in person at a municipality[79]
- After registering, citizens can access and even make some limited changes to their data through the MyGovernment portal

Recourse mechanism: Individuals who believe their record has been accessed unlawfully can submit an official complaint to the Data Protection Authority.

A2.2.2 Health Data in Estonia

In Estonia, health data is kept in a unique registry that is protected by Keyless Signature Infrastructure (KSI) blockchain.[80]

Primary method of accessing health data:

- Any person who has visited a doctor has an electronic health record. In essence, the e-Health Record integrates data from across various healthcare providers via the National Health Information System to create a single, standardized, common record for each patient. In this manner, the e-Health Record operates very much like a centralized, national database.[81]
- Users can access their e-Health Records via the patient portal.

System capabilities:

- On the patient portal, individuals can see their medical data, submit statements of intent, appoint representative(s), and act on behalf of persons they are representing.[82] They can also edit their information and submit additional information, and change the level of access others have to their information, closing it completely if they so choose.
- Doctors can use the patient portal to access a patient's entire medical record from a single electronic file using their own information system or the doctors' portal developed by the state. From doctors' information systems, patient data is transferred via X-Road to the National Health Information System,

[77] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "Toegang aanvragen tot de Basisregistratie Personen (BRP)," accessed October 12, 2020, https://www.rvig.nl/brp/aanvragen-toegang-brp.
[78] Government of the Netherlands, "Personal Records Database (BRP)," accessed October 12, 2020, https://www.government.nl/topics/personal-data/personal-records-database-brp.
[79] "How to Register in the Amsterdam Area | I Amsterdam," accessed September 27, 2019, https://www.iamsterdam.com/en/living/take-care-of-official-matters/registration/registration.
[80] "Estonia: the Digital Republic Secured by Blockchain," https://www.pwclegaltech.com/wp-content/uploads/2018/10/Estonia-the-Digital-Republic-Secured-by-Blockchain.pdf.
[81] "E-Health Records," e-Estonia, accessed October 8, 2019, https://e-estonia.com/solutions/healthcare/e-health-record/.
[82] "E-Patient Portal," digilugu.ee, accessed October 8, 2019, https://www.digilugu.ee/login?locale=en.

after which the information becomes accessible to both the doctor and the patient via the patient portal.[83] The NHIS system allows the Ministry of Health to compile national-level statistics.

Legal basis and governance:

- Provider: Estonian e-Health Foundation Board[84]
- Lead supervisory authority: Data Protection Inspectorate

Accessibility limitations:

- Patients have access to their own records, as well as those of their underaged children and others who have authorized them for access.
- Only doctors who are treating a patient can access the system, and each use by doctors is logged, again using KSI blockchain technology.

User access: Users can log into the patient portal using their ID card or mobile ID combined with their pin code. Authentication is based on the national universal public key infrastructure (PKI) that enables secure digital authentication and signing. To make changes to the patient portal, users must provide a digital signature, which acts as a second layer of authentication.

Recourse mechanism: Individuals who believe that their health record has been accessed unlawfully can submit an official complaint to the Data Protection Inspectorate.[85]

[83] "Estonia's e-Health Solution: All Data Combined in One Personal Health Record," October 16, 2017, https://scoop4c.eu/news/estonias-e-health-solution-all-data-combined-one-personal-health-record.
[84] Peeter Ross, "E-Health in Estonia," May 22, 2019, E-Governance Conference, Tallinn, https://2019.egovconference.ee/wp-content/uploads/sites/2/2019/02/Peeter-Ross-eHealth-in-Estonia.pdf.
[85] "Data Security—Health and Wellbeing Information Systems Center," accessed October 8, 2019, https://www.tehik.ee/tervis/patsiendile/andmete-turvalisus/.

A PUBLICATION OF THE

Ash Center for Democratic Governance and Innovation
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

617-495-0557
ash.harvard.edu

HARVARD Kennedy School
ASH CENTER
for Democratic Governance
and Innovation