Data Trust Research

Data Trust Terminology

Here are some commonly used terms for data trusts:

- **Data co-ops:**
- **Data trusts:**
- **Civic Data trusts:** Sidewalk Labs proposed this as a model for stewardship and management of data and digital infrastructure that approves and controls the collection and use of data for the benefit of society and individuals. It heavily relies upon their idea of “urban data.”
- **Civic Digital trusts:** Andrew Clement and MaRs proposed a *digital* trust to remind people that the digital layer includes many assets beyond data… focusing solely on data is insufficient, since data is not "owned" in the same way as other types of assets. What is being governed is the data flows and uses
- **Data-sharing agreements:**
- **Prescribed entities:** Used in Ontario’s PHIPA as a third party that can use and disclose Personal information without consent because of its predetermined privacy practices.
- **Information fiduciary:** proposed by Jack Balkin and Jonathan Zittrain to describe a person or business that deals not in money but in information.
- **Data commons:**
- **Institutionalized Trust:** The Silicon Valley Regional Data Trust uses defines this as a “formal entity requiring a stable structure of agreements and data governance policies that exist beyond the individuals within each agency and provide coherent access.” (SVRDT, n.d.)
- **Data Collaborative:** “refers to a new form of collaboration, beyond the public-private partnership model, in which participants from different sectors—including private companies, research institutions, and government agencies—can exchange data to help solve public problems.” (Verhulst, Sangokoya, and the GovLab, 2015)

Data Trusts in Canada

This section examines existing data trust formats in Canada. It first examines health data exchanges in Canada, looking at the designation of prescribed entities in Ontario's Personal Health Information Protection Act (PHIPA) since 2005. It then looks at the Smart Metering entity (SME) from Ontario's Independent Electricity System Operator (IESO). Finally, it examines data practices from the First Nations Information Governance Council (FNIGC)'s First Nations Data Centre.

The key point in these Canadian case studies is that these entities can manage data without individual consent because of pre-approved privacy practices. In the case of prescribed entities under Ontario's PHIPA, these practices are approved by the Information Privacy Commissioner of Ontario (IPC) every three years.

Ontario: Prescribed Entities

The Personal Health Information Protection Act (PHIPA) regulates how health data can be used in Ontario. The prescribed entity authority gives third parties the authority to use and disclose personal health information (PI) about their patients *without consent* because it has practices and procedures to protect the privacy of individuals' health information, and maintain its confidentiality. As a result, prescribed entities could be seen as a type of data trust because health information is disclosed and entrusted to a third party who can disclose health information if the research context is approved. There are four prescribed entities under PHIPA: Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences, and the Pediatric Oncology Group of Ontario.

Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A, <http://canlii.ca/t/534v7>

- **Section 45(1)** "A health information custodian may disclose to a prescribed entity personal health information for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services, if the entity meets the requirements under subsection (3). 2004, c. 3, Sched. A, s. 45 (1)."
- **"45(3)** A health information custodian may disclose personal health information to a prescribed entity under subsection (1) if,
    - (a) the entity has in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of the information; and
    - (b) the Commissioner has approved the practices and procedures, if the custodian makes the disclosure on or after the first anniversary of the day this section comes into force. 2004, c. 3, Sched. A, s. 45 (3).

    - (4) The Commissioner shall review the practices and procedures of each prescribed entity every three years from the date of its approval and advise the health information custodian whether the entity continues to meet the requirements of subsection (3). 2004, c. 3, Sched. A, s. 45 (4).

Information Privacy Commissioner of Ontario (IPC). (2015). Frequently Asked Questions: Health Information Protection Act. *IPC.* Retrieved from https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

- "custodians are permitted to disclose personal health information to without consent for purposes of planning, management and analysis of the health system" (p. 12)
- "In certain circumstances, with a research plan approved by a research ethics board, these prescribed entities are permitted to use and disclose personal health information for research purposes as if they were custodians." (p. 12)
- "A prescribed entity is permitted to disclose personal health information to a prescribed person who compiles or maintains a registry of personal health information, and to another prescribed entity for purposes related to the planning, management and analysis of the health system." (p. 12)

- The regulations require that the following must be publicly available (p. 12):
    - "a plain language description of the functions of the entity and
    - a summary of the practices and procedures to protect the privacy of the individuals whose personal health information they receive and to maintain the confidentiality of the information."

IPC. (2016). Manual for the review and approval of prescribed persons and prescribed entities. *IPC.* Retrieved from https://www.ipc.on.ca/wp-content/uploads/2016/08/MANUAL-FOR-THE-REVIEW-AND-APPROVAL-OF-PRESCRIBED-PERSONS-AND-PRESCRIBED-ENTITIES.pdf

This is an in-depth guide for prescribed persons and prescribed entities (141 pages). The original version was published ahead of the new reviewing processes that were put into effect on January 31, 2010. The file was last updated in 2016. The manual is extremely helpful to understand how prescribed entities work, and the minimum level of documentation necessary to pass IPC review.

There are four areas of required documentation (table of contents p. 8-14):

- **Privacy:** General privacy policies; transparency; collection of personal health information (PI) ; use of PI; disclosure of PI; data sharing agreements; agreements with third party service providers; data linkage and data de-identification; privacy impact assessments; privacy audit program; and privacy breaches, inquiries and complaints.
- **Security:** General security policies; physical security; retention, transfer, and disposal; information security; security audit program; information security breaches

- **Human resources:** privacy training and awareness; security training and awareness; confidentiality agreements; responsibility for privacy and security; termination of relationship; and discipline.
- **Organizational and other documentation:** governance, risk management, and business continuity and disaster recovery.

Cancer Care Ontario

Cancer Care Ontario "is the Ontario government's principal cancer advisor and a division of CCO. We equip health professionals, organizations and policy-makers with the most up-to-date cancer knowledge and tools to prevent cancer and deliver high-quality patient care" (Cancer Care Ontario, n.d.). They "collect and analyze data about cancer services and combine it with evidence and research that is shared with the healthcare community in the form of guidelines and standards" (Cancer Care Ontario, n.d.). The 2017 IPC review of their practices provided no major revisions to improve their practices but had seven other recommendations. The major one is to "require, at a minimum, the person or organization to which de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an individual, as required by the Manual" (IPC, 2017).

Further Reading

- CCO 2017 Prescribed Entity Review
- IPC approval letter for Prescribed Entity Review

Canadian Institute for Health Information (CIHI)

The Canadian Institute for Health Information (CIHI) is "an independent, not-for-profit organization that provides essential information on Canada's health systems and the health of Canadians" (CIHI, 2019). Their data, privacy, and security practices are extensive, covering multiple jurisdictions. The 2017 IPC review of their practices had no major suggestions to improve their data practices. There was one generic suggestion that was given to all prescribed entities to review their procedures at least once before scheduled reviews.

Further Reading

- CIHI 2017 Prescribed Entity Review
- IPC approval letter for Prescribed Entity Review

Institute for Clinical Evaluative Sciences (ICES)

The Institute for Clinical Evaluative Sciences (ICES), a non-profit corporation that allows researchers access to health data. They are a prescribed entity under PHIPA. ICES a community of researchers, data experts, and clinical experts who works to allow researchers evaluate health care delivery and outcomes in Ontario.

There are six ICES locations: Campus of Sunnybrook Health Sciences Centre in Toronto (Central), Queen's University in Kingston (ICES Queen's), University of Ottawa (ICES uOttawa), University of Toronto (ICES UofT), Western University in London (ICES Western), McMaster University in Hamilton (ICES McMaster), Health Sciences North Research Institute in Sudbury - partnership with Laurentian University and the Northern Ontario School of Medicine (ICES North).

Institute for Clinical Evaluative Sciences (ICES). (n.d.) Working with ICES data. *ICES.* Retrieved from https://www.ices.on.ca/Data-and-Privacy/ICES-data/Working-with-ICES-Data [accessed February 17, 2019]

- Personal health information is "for statistical analysis in order to evaluate and monitor aspects of the health system. ICES may also use personal health information under the authority of PHIPA s. 44 for approved research projects. Data custodians outside the health sector may disclose personal information to ICES for specified use under the authority of FIPPA or other data-governing statutes."
- "A data sharing agreement (DSA) with each data partner governs the privacy and security of the information in the ICES data inventory. Most of the core health services data are governed under a DSA between ICES and the Ministry of Health and Long-term Care."

Coding the Data:

- "Most data collected by ICES are record level with direct personal identifiers — usually health card number and/or last name, first name, date of birth, gender and postal code. This is necessary for the accurate assignment of a unique, confidential ICES number — or "code". Each person in Ontario is assigned his/her own ICES number. This ICES number (IKN) is the key to successful linkage across data sets."
- The first step when ICES collects data is the removal of direct personal identifiers and assignment of a confidential code, the IKN, to each record. An IKN exists for every Ontario resident who has been eligible for health care over time.
- This identifier is created using a secure ICES algorithm that is based on the Ontario health card number.
- Once records in a data set have an IKN assigned, the directly identifying information is stripped off the file and the data become part of the ICES data inventory – uniquely coded and linkable across health services databases within the inventory.
- Researchers have access only the ICES data inventory that contains coded data.

Using ICES Data

- ICES data provides the flexibility to link individual records across a large breadth of data. This allows it to be used ICES data for a wide variety of topics.
    - For example, analysts can link physician claims, emergency visits and inpatient hospital records with drug claims information to see how many heart attack sufferers were hospitalized and treated in a timely fashion and how many had

subsequent appointments with specialists and were prescribed appropriate medications on a follow-up basis.
    - The same study might also integrate updates on outcomes, such as subsequent health service visits or death, recorded five or ten years later.
- It's that ability to link data and create a story over time that makes ICES data so rich. The ICES data inventory is stored on servers housed within a closed computing system at ICES-Central on the campus of Sunnybrook Health Sciences Centre in Toronto.

Resources for Further Reading

- The ICES data dictionary provides a list of datasets with detailed descriptions of variables and values.
- ICES Privacy and Policies 2017 Report (forms the basis of IPC review)
- IPC letter of approval for ICES' 2017 report, with recommendations to further enhance practices

Pediatric Oncology Group of Ontario (POGO)

The Pediatric Oncology Group of Ontario (POGO) is a collaboration of care providers and stakeholders that works to ensure access and availability to cancer care for Ontario children. It is the Ontario government's source of information on planning and caring for children with cancer (POGO, 2019). They are a prescribed entity under PHIPA.

The Pediatric Oncology Group of Ontario Networked Information System (POGONIS) database and registry has captured data on childhood cancer cases in Ontario since 1985. The "database contains detailed clinical information and specifics about children's diagnosis, treatment, complications and long-term outcomes" (POGONIS, 2019).

As a note, their in-depth privacy practices are "by request" to the POGO privacy chair despite their open access in the IPC database.

Pediatric Oncology Group of Ontario (POGO). (n.d). POGONIS Childhood Cancer Database. *POGO.* Retrieved from https://www.pogo.ca/research-data/pogonis-childhood-cancer-database/ [accessed February 17, 2019]

Types of Health Information Collected:

- "POGO receives personal health information abstracted from medical records of hospitals in the province of Ontario who treat childhood cancer patients or childhood cancer survivors. POGO also receives personal health information from other administrative databases, registries and surveys, such as those from patients and their families and Vital Statistics Canada. In addition, POGO receives personal health information from other entities and persons"

Further Resources

- Privacy and Data Security Code 2016
- Types of Data in POGONIS database
- POGO Privacy and Policies Report 2017 for the IPC
- IPC letter of approval for POGO Privacy and Policies Report 2017

Smart Metering Entity at the IESO

"The Smart Metering Entity (SME) maintains and operates the province's smart meter data repository that processes, stores and protects electricity consumption data used for consumer billing by Ontario's local distribution companies" (IESO, 2019). Smart meters allow "customers to actively manage their electricity consumption. More than that, smart meters also produce large volumes of data related to consumption patterns that can be leveraged in ways that stimulate new value creation" (IESO, 2019).

The Independent Electricity System Operator (IESO) is Ontario's designated Smart Metering Entity. They are "responsible for the implementation and operation of the province's ***Meter Data Management/Repository (MDM/R)***.
In addition to this, "the SME operates under licence by the Ontario Energy Board (OEB). In its role as the SME, the IESO is responsible for the implementation, integration and operation of province's Metering Data Management/Repository (MDM/R)" (IESO, 2019d). "The MDM/R is a central hub, providing a common platform for storing, processing, validating and managing hourly electricity consumption information to support local distribution companies (LDCs)' billing processes – all in a highly secure environment" (IESO, 2019).

Moreover, "with nearly five million smart meters sending hourly data to the MDM/R, and more than 60 LDCs integrated into the system, Ontario's MDM/R is one of the largest shared systems in the world, adding 100 to 120 million records every day" (IESO, 2019).

Third Party Access Implementation Plan

The IESO would like to share this electric consumption data with third-party companies. They launched a stakeholder engagement related to third-party access to the MDM/R data in 2016 that ended March 2019. This process was supported by two stakeholder committees (IESO, 2019c):

- A Data Strategy Advisory Council (DSAC) that provided expert support and advice to the SME. This Advisory Council was made up of stakeholders representing various sectors across the Province.

- The IESO Stakeholder Advisory Committee whose members are appointed by the IESO Board of Directors to provide policy-level advice and recommendations directly to the IESO Board of Directors and Executive Leadership Team.

"At the core of the implementation plan is a data de-identification methodology that is the gold standard in the disclosure control community" (IESO, 2019). A Data Strategy Advisory Council has been established to support, advise, and inform the engagement efforts (IESO, 2019b). The IESO uses the Information and Privacy Commissioner of Ontario's De-identification Guidelines for Structured Data as their methodology.

First Nations Information Governance Centre (FNIGC)

The First Nations Information Governance Centre (FNIGC) conducts, holds, and allows access to data that is improves the health and well-being of First Nations people. It is *data collected by the First Nations people, for the First Nations people*. Surveys include the First Nations Regional Health Survey (FNRHS, or RHS) and the First Nations Regional Early Childhood, Education and Employment Survey (FNREEES, or REEES). These surveys are governed by the OCAP principles - Ownership, Control, Access and Possession. The FNIGC provides free access to aggregated survey data in the form of charts, tables and graphs as part of the FNGIC Data Online initiative with 222 tables and 171 charts online.

First Nations Data Centre

Within the FNIGC is the First Nations Data Centre (FNDC), a knowledge exchange service that shares their full, unpublished survey data with researchers, policymakers, and others.

FNGIC. (n.d.). First Nations Data Centre. *FNGIC.* Retrieved from https://fnigc.ca/fndc [accessed February 17, 2019]

- "the FNDC provides access to unpublished and record-level data from FNIGC's respected survey work, including the First Nations Regional Health Survey (FNRHS, or RHS) and the First Nations Regional Early Childhood, Education and Employment Survey (FNREEES, or REEES)."
- "The first service of its kind, the FNDC offers data access to individuals pursuing academic research, policy development, and program planning and evaluation on a pay-per-use basis. The data cannot be used for commercial purposes."

OCAP Principles

FNGIC. (n.d.) OCAP Principles. *FNGIC.* Retrieved from https://fnigc.ca/ocapr.html [accessed February 17, 2019]

- **"**The First Nations principles of OCAP® are a set of standards that establish how First Nations data should be collected, protected, used, or shared. They are the de facto standard for how to conduct research with First Nations."

- OCAP focuses on community rights towards data collection practices, and is meant to be a model that other indigenous groups around the world could use.
- “Standing for ownership, control, access and possession, OCAP® asserts that First Nations have control over data collection processes in their communities, and that they own and control how this information can be used.”
    - **“Ownership** refers to the relationship of First Nations to their cultural knowledge, data, and information. This principle states that a community or group owns information collectively in the same way that an individual owns his or her personal information.”
    - **“Control** affirms that First Nations, their communities, and representative bodies are within their rights in seeking to control over all aspects of research and information management processes that impact them. First Nations control of research can include all stages of a particular research project-from start to finish. The principle extends to the control of resources and review processes, the planning process, management of the information and so on.”
    - **“Access** refers to the fact that First Nations must have access to information and data about themselves and their communities regardless of where it is held. The principle of access also refers to the right of First Nations communities and organizations to manage and make decisions regarding access to their collective information. This may be achieved, in practice, through standardized, formal protocols.”
    - “**Possession** While ownership identifies the relationship between a people and their information in principle, possession or stewardship is more concrete: it refers to the physical control of data. Possession is the mechanism by which ownership can be asserted and protected.”

First Nations Information Governance Centre. (2013). Ownership, Control, Access and Possession (OCAP): The Path to First Nations Information Governance. *FNIGC.* Retrieved from https://fnigc.ca/sites/default/files/docs/ocap_pathways_to_fn_information_governance_en_final.pdf

- Due to the “federal Crown’s relationship and responsibilities in relation to First Nations, Canada collects and holds more information on First Nations people than perhaps any other group in Canada” (FNIGC, p. 28).
- “While the Privacy Act protects personal information, the Access to Information Act and the Library and Archives of Canada Act present legislative barriers to OCAP™.” (FNIGC, 2013, p. 28).
- **OCAP Principles:** “neither the Canadian government nor any institution thereof should be considered as a steward of First Nations data. This is because Access to Information Act and the policies and procedures that support it (ATIP) prevent First Nations from exercising control over the use and disclosure of First Nation-identifying data or information.” (FNIGC, 2013, p. 27)

- Access to Information Act Problems: “While the exemption categories under the Act may protect the personal privacy of First Nation members, it would not protect aggregate reports or demographic or survey data, nor would it protect any traditional knowledge, or reporting under contribution agreements. In fact, except for those few First Nations that the Act recognizes as “governments”, almost any information or data that First Nations provide to Canada, or that Canada collects from its members and other sources (as long as names and personal identifiers are removed) can be released to the public under the Access to Information Act.” (FNIGC, 2013, p. 28-29)
    - “As a result of the Access to Information Act, AANDC and other federal government institutions cannot withhold disclosure of a significant amount of First Nations information within their control. This is particularly true with the digitization of data, allowing records to be easily stripped of personally identifying information and then released to the requesting public” (FNIGC, 2013, p. 29)
    - This has already been exploited by pharmaceutical companies like Brogan Inc.
- As a result, FNIGC recommends that “First Nations to repatriate their own data, to be placed within First Nations stewardship, or by contract with another entity that does not have the legal restrictions of ATIP… Changing stewardship of the data could take First Nations data out of the control of a federal institution. ” (FNIGC, 2013, p. 31)

- Addressing the lack of privacy literature in OCAP: “Concepts of personal privacy are not typically addressed in existing OCAP™ literature, or expressed as OCAP™ principles. However, personal privacy is a fundamental element in First Nations information governance and is consistently present in OCAP™ models.” (FNIGC, 2013, p. 34)
    - “OCAP™ is a way for First Nations to express principles of information governance and community privacy in an aggregate sense – a notion that seems quite foreign to many non-First Nations. Personal privacy, on the other hand, is a universal value that is reflected in western society, through laws, policies and ethics. It is not something that First Nations must fight for, or to vigilantly defend. Canadian laws protect personal privacy.” (FNIGC, 2013, p. 34)
    - “Suggestions that following OCAP™ principles will result in a breach of personal privacy are simply incorrect. All of the models presented above, under OCAP™ in Action, have examined and protected personal privacy to the same or better standards as found in applicable laws. In fact, respecting OCAP™ principles and concepts of community privacy add an additional layer of privacy protection for individuals; not only is an individual’s personal identity protected from disclosure and any resulting harm, but their group identity and status as a member of a community is also protected.” (FNIGC, 2013, p. 35)

Further Reading

- First Nations Information Governance Centre. (2014). Barriers and Levers for the Implementation of OCAP™. *The International Indigenous Policy Journal, 5*(2). Retrieved from http://ir.lib.uwo.ca/iipj/vol5/iss2/3

- First Nations Information Governance Centre. (2016). Pathways to First Nations' data and information sovereignty in Kukutai, T., & Taylor, J. (Eds.). Indigenous Data Sovereignty: Toward an agenda. Acton ACT, Australia: ANU Press. Retrieved from http://press-files.anu.edu.au/downloads/press/n2140/pdf/book.pdf?referer=2140

Data Trusts Using City Data

This section examines proposed projects working with city data in the context of data trusts. It first examines Sidewalk Lab's Civic data trust model, content from MarS, and the DECODE project in Barcelona.

Civic data trusts are trying to solve the issues of obtaining meaningful individual consent from the people whom city data is collected from. Much of the city data is collective or de-identified such as sensor data from stop lights or bike paths. However, there are questions raised about collective and group rights, and re-identification.

Sidewalk Labs: Civic Data Trust

Sidewalk Labs. (2018, October). Digital Governance Proposals for DSAP Consultation. *Sidewalk Labs.* Retrieved from https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES

Definitions

- **Civic Data Trust:** is a model for stewardship and management of data and digital infrastructure that approves and controls the collection and use of data for the benefit of society and individuals." (Slide 12)
    - "useful where data is being collected and used in an urban environment and there are challenges in obtaining meaningful consent." (Slide 12)

- **Urban Data:** Urban Data is data collected in a physical space in the city. SL argues that urban data is different from other data because it could be considered as a public asset, individual consent is hard to achieve, de-identified data like urban data is technically not protected, there are concerns of community surveillance, the data is tied to geography, and that citizens have rights to protection (Slide 13).
- Urban data includes the following (Slide 13):
    - Public spaces, such as streets, squares, plazas, parks, and open spaces
    - Private spaces accessible to the public, such as building lobbies, courtyards, ground-floor markets, and retail stores
    - Private spaces not controlled by those who occupy them (e.g. apartment tenants)

- **Responsible Data Impact Assessments:** "RDIA is an assessment of the prospective use of data involved in an activity, including an analysis of whether the benefits of the activity outweighs the risks involved. It is a vehicle for assessing alignment with principles, legal requirements, and stakeholder expectations." They are "conducted at the design phase, prior to data collection or use." (Slide 18)

Functions

- "It is an independent third party that ensures that value from data goes to the people, communities, government, industry, and society from which it was collected, and that data privacy and security are protected. A Data Review Board, assembled of diverse members of the community, would monitor and enforce data collection and use."(Slide 12)
- Trust would be a steward of urban data, and would "make de-identified Urban Data freely and publicly accessible—and not owned by any private entity" by default. (Slide 13)
    - "The Trust would consider applications to collect Urban Data that involves personal information (e.g. CCTV cameras) or proposals to collect Urban Data on a proprietary or commercial basis." (Slide 13)
- "Following Responsible Data Use Guidelines, the Trust would approve and control the collection and use of, manage access to, and, potentially, store Urban Data originating in Quayside. This would be on top of—not in the place of—existing law, regulation, and government enforcement." (Slide 13)

Responsible Data Impact Assessment Process (RDIA) (Slide 15):

1) **RDIA Filing** and approval by the Trust must happen before collection or use
2) **Approval** of the RDIA will be quick for the "collection of non-identifiable data that will be made freely and publicly available." They will advance quickly to the registration step. Substantive review required for identifiable data collection or proprietary data.
3) **Registry** of the placement collection devices, the RDIA will be accessible to the public to get information on what data is being collected, why, how, where, and by whom.
4) **Managing Access.** By default, non-personal and de-identified data will be freely accessible. Restricted data will be managed by the Trust. Trust could be an actual data repository.
5) **Enforcement.** The Trust "retains the duty to audit all uses and remove digital devices in the event it discovers a violation." Also the ability to shutdown access to bad actors
6) **Exemptions** and authority to exempt specific uses will be given to the Trust for uses that "do not have implications for personal privacy by virtue of their limited technical capabilities"

•• Privacy Impact Assessments (PIAs) will be required if personal information is collected

Data Typologies (Slide 16):

SL provides a framework to categorize the different types of urban data

1) **Urban Data Type 1 – Collected in the public realm:** Citizens have little control over what's collected (pedestrian counters). Will automatically be made publicly available because it's considered a public asset. The Trust will "Reliably and speedily—potentially, automatically—approves accurate, self-certified applications"
2) **Urban Data Type 2 – Collected in privately-owned but public spaces:** Citizens have little control over collection.
    a) **Class A:** (e.g. camera in a large building lobby): Applications to Data Trust go through same process as Urban Data Type 1. The Trust follows the same procedures as Urban Data Type 1.
    b) **Class B:** (e.g. small café camera): All applications to Data Trust can be self-certified. No substantive review needed, the Trust will register device placements and publish RDIA online but the data is not made publicly available by default.
3) **Urban Data Type 3 – Collected in fully private spaces:** May be necessary to achieve community goals (like temperature management). Trust would substantively review applications for devices installed by a landlord or builder. Trust would audit de-identification and storage.
4) **Traditionally Collected data – involving direct consent like websites:** SL argues that "local, geographically-bound governance regime unworkable given the lack of a relationship between this kind of data collection and geography." No RDIA necessary, unless voluntary.

<u>The Platform</u>

- **Standards and Open Architecture:** "Well-documented, standardized formats and interfaces. Any party will have the information required to build a replacement component for any urban system, or to create an entirely new application." (Slide 30)
- This will provide "Easy access to public-domain data" and allow for data portability (Slide 30).
- **No data localization:** Data localization "Is not necessary to ensure that data that originates in Canada is handled in accordance with Canadian law with regard to privacy protections, which can be achieved through contractual and technical mechanisms. Runs counter to the way information travels across the internet, without regard to geographic boundaries" (Slide 35)

Commentary on Sidewalk Labs' Civic Data Trust Proposal

McDonald, S. (2018, October 17). Toronto, Civic Data, and Trust. *Medium.* Retrieved from https://medium.com/@McDapper/toronto-civic-data-and-trust-ee7ab928fb68

- McDonald analyzes SL's Civic Data Trust, first commending the transparency of the conversation and then delving into the "bad" and the "ugly" of the data proposal.

<u>"The Ugly" Concerns:</u>

McDonald Outlines four major concerns and unanswered questions with the proposal:

1) **Default to open publishing:**
    - "Sidewalk Labs does not need proprietary data access to monetize the Quayside project, and enforcing a "default to open" approach—especially if compelled—is likely to end up as a defensive advantage."
    - "could be read as an attempt to use government to quasi-nationalize competitor data through open publication requirements."
2) **Concept of 'urban' data:**
    - "attempts to reorient the country's data ownership laws based on characteristics—either of the data itself, or its means of collection."
    - "'urban' data would be declared a "public asset," and then published. There's nothing new about proposals for attenuating data's treatment to its characteristics, including Linnet Taylor's work on group harms and Nathaniel Raymond's work on demographically identifiable data."

3) **Resistance to Data Localization**
    - "(1) it's the only specifically articulated requirement for data architecture; (2) it suggests that 'urban' data should be owned and opened locally because of its relationship to the place of its collection, but not required to be stored there; and (3) it offers a combination of mechanisms to virtualize compliance with Canadian Law."
    - McDonald argues that making everything open by default "suggests there's a specific, unexplained interest in being able to store personally identifiable data about Quayside residents extra-nationally. This is particularly noticeable because of how the proposal otherwise grounds data ownership and openness, particularly of 'urban' data, in its relationship to public consent."

4) **Theory of law and authority**
    "implies, that Civic Data Trusts should have the relatively new authority to track data supply chains and licenses—and to punish violation with, at the least, mitigated access. All of that gives Civic Data Trusts the ability to substantially project their authority into the backbone of data collectors, which is a relatively rare amount of enforcement power for someone other than a government regulator."

<u>"The Bad" Concerns:</u>

- **Bundles collection with use:** "the proposal bundles licensing of data collection with data use—a Civic Trust should be able to control each independently." (McDonald, 2018)
    - "there's no inherent reason to bundle licenses to collect data with licenses to use data—and any governance body should have the freedom to be as granular with its licensing as it so chooses." (McDonald, 2018)
- **Limits scope of authority:** it "leav[es] the most sensitive data outside of trust protection." (McDonald, 2018)

    - “the proposed trust would grant licenses to collect and use data—and the more sensitive the data, the more proprietary it would be.” (McDonald, 2018)
- **Open Publication limits enforcement:** “the “openness” of the data often affects how effective “managing” that data can be. The primary goal of the “Registry,” “Managing Access,” “Enforcement,” and “Exemptions,” components appear to be preserving public access, selectively controlling public access, building a policy apparatus around access, and an enforcement mechanism of use-based license limitations. In most governance systems, those functions are at least separate, if not sometimes in direct conflict.” (McDonald, 2018)
- **Sweeping audit authority but lack of punitive tools:** SL’s proposal suggests that enforcement tool should mainly happen through access to openly published data. Legal and technical challenges with use-based licensing, and intellectual property. Needs more tools, resources, funding and investigatory powers beyond publicly available data. (McDonald, 2018).

MaRS: Civic Digital Trust

MaRS. (2018, December). A Primer on Civic Digital Trusts. *MaRS.* Retrieved from https://marsdd.gitbook.io/datatrust/
This primer aims to introduce civic digital trusts. It is a partnership between MaRS Solutions Laband Waterfront Toronto, with funding from Sidewalk Labs.

Definitions

- **Trust:** "An arrangement under which money or other property is held by one person, often a trust company, for the benefit of another person or persons. These assets are administered according to the terms of the trust agreement." (Irwin Law in MaRS, 2018).
    - “Trusts are set to provide stewardship over an asset. **Assets** held in trust are most often land or money, but can be established for anything of value, including intellectual property and data. There are three parties involved in a trust agreement. Each party can be a person, a group of people, an organization, or a community” (MaRS, 2018):
    - The **trustor** contributes property to the trust.
    - The **trustee** manages the trust.
    - The **beneficiary** receives the benefits of the trust agreement.
- **Fiduciary duty:** “trustees are legally obligated to act in the best interests of the beneficiaries, rather than serving their own interests. For example, attorneys have a fiduciary duty to their clients, and board members of a corporation have a fiduciary duty to shareholders.”(MaRS, 2018).
    - “The most important duties for trustees are loyalty and prudence. **Loyalty** means acting in good faith for the beneficiaries, avoiding conflicts of interest, and not acting for the benefit of themselves or a third party. **Prudence** means acting with due care, skill and diligence.” (MaRS, 2018).

- “Trusts provide beneficiaries with legal protection when they place their confidence in the trustee. If a trustee acts against the interest of the trust's beneficiaries or fails to declare a conflict of interest, a **breach** of fiduciary duty has occurred. If a breach has occurred and the beneficiaries have suffered damages, the beneficiaries are entitled to take action in civil court.” (MaRS, 2018).

Civic Digital Trusts

- **Digital Trust:** “ Following Andrew Clement, we have chosen to call it a *digital* trust to remind people that the digital layer includes many assets beyond data… focusing solely on data is insufficient, since data is not "owned" in the same way as other types of assets. What is being governed is the data flows and uses.” (MaRS, 2018).
- **Civic Trust:** “Following Sean McDonald, we have chosen to call it a *civic* trust to emphasize the requirement to build civic participation into the governance of the trust. Civic means relating to a city or a town” (MaRS, 2018).

Technical Architecture Options

MaRS lists the different kinds of systems that a civic digital trust could use to carry out duties:

1) **Centralized data system:** Database, standards, and platforms are held locally. Provides the greatest amount of control and enforcement because “the infrastructure in place was built by the organization, creating ownership of the assets.” Data stored in one place, heavy upfront costs. (MaRS, 2018).
2) **Semi-Centralized data system:** “hybrid between a centralized and distributed system. In practice, we have seen centralized platforms and infrastructure built by a governing body, with public and private institutions creating and maintaining their own sharable repositories of data which adhere to the governing body's principles and standards.” Central portal grants access to multiple repositories, interoperability and admin costs. (MaRS, 2018).
3) **Decentralized Architecture:** “nodes of information are held with the various participating entities, and are all interconnected to encourage the sharing of their repositories for approved uses. In this system, the governing body creates standards and policies for all partnering entities to follow to ensure ease of access to information and the ability to utilize them.
    a) Each entity creates and manages their own repositories, and may provide their own individual platforms for data access.” Access to each repository is different, “an index or catalogue is the only method to obtain data.” Costs are around building “common usage and ontology” (MaRS, 2018).
4) **Open Data:** “Common standards are created by an entity, collaboration, or group to create a repository of shared data. This method requires the exclusive use of non-personally identifiable information.” Access to data is through a “central repository with common usage, standards, access policy and single approval.” (MaRS, 2018).

5) **Data Marketplace:** “Neutral legal, tax entity, and platform that brings together buyers and sellers of data” with a “central database of repositories” with costs going towards building “a central platform and point of access” (MaRS, 2018).
6) **Data sharing agreements:** “ An agreement between multiple institutions to share data according to certain terms and conditions. Data sharing agreements identify the standards which govern the collection, storage, security, analysis, re-use, and destruction of data.” Access is “granted to repositories with dictated terms and conditions around the use.” (MaRS, 2018).

DECODE Project

Bria, F. (2018, April 5) Our data is valuable. Here's how we can take that value back. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/apr/05/data-valuable-citizens-silicon-valley-barcelona?CMP=twt_gu

- “We badly need a new social pact on data that will make the most of our data while guaranteeing citizens’ rights to privacy and information self-determination.” (Bria, 2018)
- “Cities can’t, of course, solve all our digital problems: many of them need urgent attention at the national and global level. But cities can run smart, data-intensive, algorithmic public transportation, housing, health and education – all based on a logic of solidarity, social cooperation and collective rights.” (Bria, 2018)
- “By helping citizens regain control of their data, we aspire to generate public value rather than private profit. Our goal is to create “data commons” from data produced by people, sensors and devices.” (Bria, 2018)
- “A New Deal on data, based on a rights-based, people-centric framework, which does not exploit personal data to pay for critical infrastructure, is long overdue.” (Bria, 2018)

Decode Project. (n.d.a). Have more questions?. *Decode Project.* Retrieved from https://decodeproject.eu/have-more-questions

This project aims to promote a vision of data as a common asset and to empower the general public with an infrastructure that provides it with control over how the data is used, given that it is the main producer of that data. Pilot projects focus on citizen control on IoT devices, creating socially-driven common resources and away from centralized data platforms, and open democracy (Decode project, n.d.a).

- **Blockchain and attribute-based cryptography:** “DECODE is creating tools which will give people ownership of their data. These tools will combine blockchain technology with attribute-based cryptography to give the data owner control of how their data is accessed and used. This will help build a trustworthy and privacy-aware digital society.” (Decode project, n.d.a).
- **Trust and privacy:** “Entitlements attached to the private data would be searchable in the public domain but will grant access only to those parties that have the entitlement to access it. This novel concept of data rights and entitlements also applies to data being

sent to or used by connected Internet of Things (IoT) objects in order to perform actions in the real world, allowing citizens to manage and control their devices and the data they generate." (Decode project, n.d.a).

- **Data Commons:** "a shared resource – made accessible and intentionally open – rather than subject to restrictions through licensing. It enables everyone to contribute, access and use the data in the data commons." (Decode project, n.d.a).
    - **DECODE is an attempt to avoid personal data exploitation:** "There are other forms of digital commons licensing, such as that for software, which have been studied widely. However, a digital commons made of personal data continue to be the subject of exploitation by big service providers. DECODE will create and implement new rules that make alternatives possible." (Decode project, n.d.a).
        - "People will be able to decide which personal data they want to share into the commons, and on which basis. For instance, they can decide whether their data is anonymised." (Decode project, n.d.a).
- **Smart Rules:** "are the means by which people can decide how their data is used, by whom and on what basis. Using distributed ledger technologies such as blockchain, DECODE will create smart contracts that enable people to create rules about whether their personal data is kept private or shared." (Decode project, n.d.a).
    - "Smart rules allow people to define conditions for the access and use of data, and legal/contractual obligations and other constraints. Through the smart rules, one may provide or remove authorisation for access to personal data; their association with its identity; or change the legal status and the conditions of use and exploitation of the data" (Decode project, n.d.a).

Decode Project. (n.d.n). Pilots. *Decode Project.* Retrieved from https://www.decodeproject.eu/pilots

There are four pilot Projects using DECODE architecture:

Barcelona

1) **Digital Democracy and Data Commons:** Barcelona City Council's digital democracy software Decidim.org "will integrate a DECODE module which allows petitions to be signed anonymously but still in line with authentication requirements, such as place of residence." It "gives people more granular control over their data. It will enhance privacy (via the DECODE app), allow data sharing and visualization (via the BCNOW dashboard) and transparency (via the DECODE distributed ledger)." (Decode Project, n.d.b)
2) **Citizen Science Data Governance:** "residents will use environmental sensors which record factors such as noise levels and pollution. The sensors will be located inside their homes and in their neighbourhood." (Decode Project, n.d.b)

Amsterdam

3) **Amsterdam Digital Register - age check with municipal census data:** "This pilot aims to give citizens access to personal data that is stored in the municipal database, and allows them to share these data in a different context, on- or offline. In the

pilot, participants will use DECODE technology to prove their age, as it certifies that they are over 16 or 18 years of age, without having to share their full identity or social security number. This pilot uses Attribute Based Credentials, a data minimising authentication mechanism." (Decode Project, n.d.b)

4) **Gebiedonline (Neighbourhood Online)**
   "GebiedOnline is a local neighbourhood social network in Amsterdam. Access to GebiedOnline is currently managed by email/password or Facebook login. This creates unwanted dependencies and security issues. This pilot will test a more privacy-preserving local social network… using attribute based credentials" (Decode Project, n.d.b)

DECODE Architecture Documents

Relevant documents for further study into specific aspects of the DECODE architecture if interested for further reading:

Bonelli, F., van Dijk, T., Samuel, G. (2019). Design & implementation interface for smart rules. *DECODE.* Retrieved from https://www.decodeproject.eu/publications/design-and-implementation-interface-smart-rules-0
"It aims to explain through the Smart Rules interface, the possibility to clearly perceive who is doing what with our data and take clear decisions when it matters, looking at privacy in context and the implementation of the DECODE platform through user testing."

Sonnino, A., Bano, S., Danezis, G., Barritt, J. (2019). Intermediate Version of DECODE Architecture. *DECODE.* Retrieved from https://www.decodeproject.eu/publications/intermediate-version-decode-architecture
"It aims at offering a more comprehensive system overview, description of the distributed ledger and smart contract applications."

Meessen, P., Venema, M., Sonnino, A., Bano, S. (2019). Decentralised models for data and identity management: Blockchain and ABC MVPs. *DECODE.* Retrieved from https://www.decodeproject.eu/publications/decentralised-models-data-and-identity-management-blockchain-and-abc-mvps
"It aims at explaining decentralised identity management and access control."

Cuartielles, D., López, E., Therner, S. (2018). Hardware prototype and reference platform running the DECODE OS. *DECODE.* Retrieved from https://www.decodeproject.eu/publications/hardware-prototype-and-reference-platform-running-decode-os
"This document is part of the work done by Arduino in collaboration with the other technical partners in the DECODE project in the search for an optimal hardware platform ready to perform well enough to run the software created by the other partners in the consortium. While previous

studies, made in D4.5, focused in a pure performance analysis of the boards chosen by the different partners, D4.8 builds on top of those results, includes the observations made by partners, makes a further analysis of other boards, and makes a final suggestion of an architecture that should be ready to fulfil the needs of the project."

Overview of Other Data Trust Projects

This is a list of the other data trust projects mentioned by MarS or Sidewalk Labs in their proposals:

Copenhagen-Hitachi City Data Exchange

"The City Data Exchange is a private/public collaboration to examine the possibilities of private/public data exchange. The project will examine purchasing, selling and sharing a broad range of data types between all kinds of users in a city – citizens, public institutions and private companies. The project is a collaboration between Copenhagen Municipality, the Capital Region, CLEAN (a Danish clean-tech cluster) and Hitachi." (Copenhagen Solutions Lab, n.d.)

- **Report on two years of the City Data Exchange**
  "The City Data Exchange (CDE) has closed a gap in regional data infrastructure. Both public-and private sector organizations have used the CDE to gain insights into data use cases, new external data sources, GDPR issues, and to explore the value of their data. Before the CDE was launched, there were only a few options available to purchase or sell data." (Sylverstersen and Johanson, n.d.)

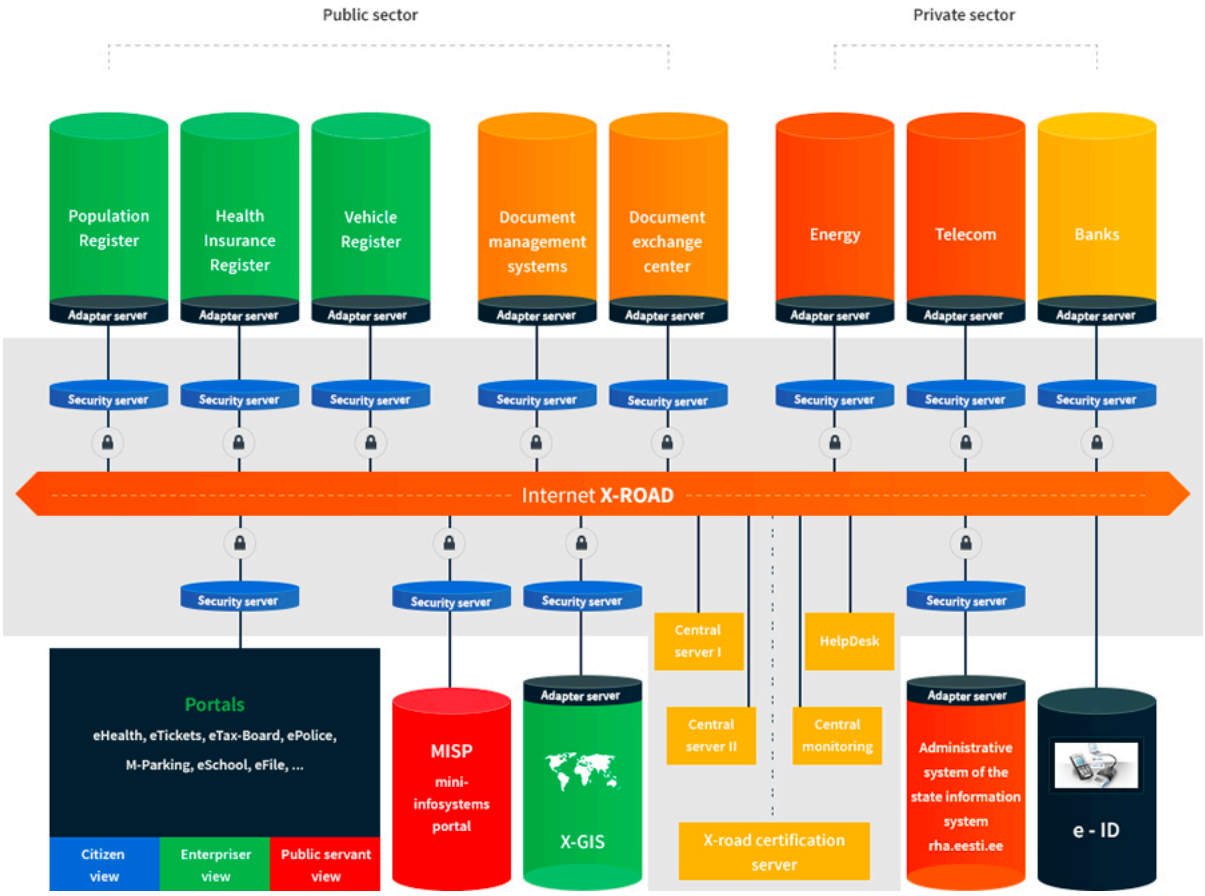
Estonia Model: API Framework Management

- **What is X-Road:** "Estonia's X-Road data exchange platform is based on an approach where each collector of data stores its own data, which are standardized and accessed through APIs that are managed by the Trust. It is a repeatable framework of terms and conditions with APIs that allow developers and others to access data for testing, product development, and data analytics." (Sidewalk Labs, 2018)

- Each data owner determines what information is available and who has access to it. Couple this with some enforced data and messaging standards, et voila; you have joined up government. It's basically how you would architect software, but on a macro level." (Herlihy, 2013)
  - "some parts of the private sector can also utilise the X-Road - allowing the principle of not duplicating data in different locations to flow out from government." (Herlihy, 2013)
- **Transparency and Accountability:** "There's an open register showing the profile information that is held in each government system, what reason it is held for, and who it can be accessed by" (Herlihy, 2013)

- “This register also shows the formats and data standards that each system is using.” (Herlihy, 2013)
- “People in Estonia can also see which officials have viewed their data. It’s against the law to view someone’s data without appropriate reasons (you could go to prison), and all access is logged. I looked at some of these logs and they show you clearly who has been looking at your information” (Herlihy, 2013)

Architecture of X-Road (Herlihy, 2013):



Estonian Potential in Framework Programmes: Analysis and Policy Options.
• University of Tartu Kadri Ukrainski, Hanna Kanep, Tanel Hirv, Youjun Shin
• Tallinn University of Technology Margit Kirs, Erkki Karo
https://www.etag.ee/wp-content/uploads/2018/03/Estonian-Potential-in-Framework-Programmes_Analysis-and-Policy-Options-1.pdf

E-Estonia. (2019, March). Estonia to share its e-governance know-how. *E-Estonia.* Retrieved from https://e-estonia.com/global-digital-society-fund/

Guernsey Island Trust

What is Guernsey

- "Guernsey is a leading jurisdiction for the establishment and management of trusts. The Island has a large and well qualified professional trust sector, modern trusts legislation and an effective judicial system. It is also recognised as being in the top division of international finance centres in the regulation and supervision of its financial services industry." (Olsen, 2017)
- "Generally in Guernsey, trusts are administered by professional corporate trustees regulated by the Guernsey Financial Services Commission ("GFSC")." (Olsen, 2017)
- "Guernsey's principal trusts legislation is the Trusts Law which is supported by a body of case law from the Island's courts." (Olsen, 2017)

Guernsey Island Trusts

- "A Guernsey trust can be used to hold any types of assets, and any share, right or interest in the assets, including tangible and intangible property, and other rights and interests. In relation to data, examples of rights could include intellectual property rights in the data as well as licences to access, process and store the data." (Ozanne, 2017)
- "For over a decade, Guernsey has been one of only 11 non-EU jurisdictions whose data protection regimes benefit from an adequacy decision of the EU Commission." (Ozanne, 2017)
- "In relation to data trusts containing personal data, the trustee would be a data controller of the data for data protection purposes and must hold the data in compliance with Guernsey's data protection requirements. This should enable the easy flow of personal data to and from EU and EEA countries and the trustee." (Ozanne, 2017)

Different Kinds of Trusts in Guernsey

- **Discretionary trusts:** "gives the trustees wide powers to administer the assets of the trust and to distribute them at their discretion." (Olsen, 2017)
    - "flexibility to adapt to the changing needs of beneficiaries over time." (Olsen, 2017)
- **Fixed interest trust:** "Trustees have little discretion as to how trust property is distributed in a fixed-interest trust." (Olsen, 2017)
- **Purpose trusts:** "it is possible for Guernsey law trusts to be established partly or wholly for noncharitable purposes. Purpose trusts may be used in corporate transactions to create orphan structures or to hold assets which are otherwise difficult or undesirable for a company to hold." (Olsen, 2017)
- **Settlor reserved:** "Settlors may retain certain powers over the trust or trust property when they create a trust, such as the power to give binding directions to the trustees in relation to the investment of the trust fund, the power to vary or amend the terms of the trust, the power to remove a trustee and the power to change the proper law of the trust. Reserved power trusts are often used where a settlor is a successful business person

and would like to remain actively involved in the management of a company following its settlement on trust." (Olsen, 2017)

Further Reading:

- Full text of *The Trusts (Guernsey) Law, 2007.* http://www.guernseylegalresources.gg/article/97619/Trusts-Guernsey-Law-2007

The Silicon Valley Regional School Board

- "The Silicon Valley Regional School Board is working to tear down the silos between partners and other public agencies to create more value through safe sharing of personal data. Sharing these data sets among previously siloed institutions, such as public school districts, public health, child and family services, mental health, juvenile justice and Education Technology companies, is allowing for a more robust understanding of contributing factors of student success and failure within the school system in Silicon Valley." (MaRS, 2018).

- Founded in 2015, "SVRDT is a regionally-based, nationally-grounded collaborative research organization dedicated to building a well-managed regional data trust that overcomes the limitations of siloed data systems and resolves privacy and trust issues, combining data from numerous public agencies that service children and families, to provide a comprehensive understanding of factors contributing to student failure and success." (SVRDT, n.d.)

- **It's a partnership between** county education offices in Santa Clara, San Mateo, and Santa Cruz; University of California; and health and human services agencies in the tri-county region of the Silicon Valley. (SCCOE, 2017)
- **"The "DataZone" data warehouse,** administered by the Santa Clara County Office of Education (SCCOE), is the education data repository for the initiative and is the hub for the SVRDT." (SCCOE, 2017)
- **Software is called "FosterVision application** that provides critical information to social workers, probation officers and student services personnel who serve some of our most at-risk youth." (SCCOE, 2017)
- Backed by the Chan Zuckerberg Initiative (SCCOE, 2017)

Note: haven't found much else about it

Trūata

Mentioned by Sidewalk Labs and the MaRs primer as an example of a data trust

- Announced March 16, 2018, "Truata will be set up as a data trust in Dublin under Irish law. Mastercard will be one of the first clients to use Truata, and, the report states, three

other companies will help get the data trust off the ground once the GDPR goes into effect." (IAPP, 2018)

- "Mastercard and IBM have founded Truata, an independent trust to allow companies to conduct analytics while complying with the upcoming General Data Protection Regulation (GDPR)." (Andreasyan, 2018)
- **Services:** "It will offer a service to fully anonymise data and provides analytic services to assist customers with tools, data insights, algorithms and reports that customers can use in their own products and solutions." (Andreasyan, 2018)
    - "It will be assisting firms in finance, insurance, airlines and automotive to safely anonymise their data and extract useful insights in compliance with GDPR." (Keane, 2018)
- **Process:** "A customer removes the name, address, whatever that personal identifier might be and then sends (the data) to us," Marx said on how the process will work." (Keane, 2018)
    - "Before the information can be analysed, Truata strips away any remaining details in the data that could link it to anyone or anything. The data is put through a "differential privacy test" to prove it has no links left to an identifiable person." (Keane, 2018)
    - "After it's passed this differential test, it's ready for analytics," Marx said. (Keane, 2018)
- **Why Ireland?:** "Irish law allows us to set up as a trust," Marx said. "Many other countries don't. Secondly, we wanted to be audited and governed by the best-resourced data privacy agency in Europe, and that is currently the Irish one." (Keane, 2018)
    - "Ireland's Data Protection Commissioner, Helen Dixon, is about to become Europe's busiest data authority as she polices the European headquarters of Facebook, Twitter, Google and many others… the commissioner's office has faced criticism for being under-funded and ill-equipped to take on an EU-wide data policing role." (Keane, 2018)
- **Won the 2018 International Privacy Innovation Award** (Truata, 2018)

Solid (Tim Berners-Lee Project)

- Work to reverse the control of corporate giants is underway at the Decentralized Information Group at MIT's Laboratory for Computer Science and Artificial Intelligence (CSAIL), co-lead by Tim Berners-Lee (Finley, 2017)
    - "start-up, Inrupt, Inc, will be putting its own effort into the Solid open source technology and the Solid movement." (Solid, n.d.)
- **About:** "Solid (derived from "social linked data") is a proposed set of conventions and tools for building decentralized social applications based on Linked Data principles. Solid is modular and extensible and it relies as much as possible on existing W3C standards and protocols." (Solid, n.d.)

- **A model of user-control:** “users control where their data is stored and how it's accessed. For example, social networks would still run in the cloud. But you could store your data locally. Alternately, you could choose a different cloud server run by a company or community you trust. You might have different servers for different types of information—for health and fitness data, say—that is completely separate from the one you use for financial records.” (Finley, 2017)
    - "It's kind of like when you had floppy disks and you had one disk for the application and another the storage, [says Berners-Lee]” (Finley, 2017)
- **Solid, an open-source project:** “He hopes to create an open technology standard that different applications can use to share data, regardless of what that data is or what type of application needs to read it.” (Finley, 2017)
    - “Such a standard would enable applications—your hospital’s record-keeping software or a social network—to read and write data from the servers you choose and control, rather than the servers that belong to an individual company.” (Finley, 2017)

- **True Data Ownership:** “Because applications are decoupled from the data they produce, users will be able to avoid vendor lock-in, seamlessly switching between apps and personal data storage servers, without losing any data or social connections.” (Solid, n.d.)
- **Reusing existing data: “**Developers will be able to easily innovate by creating new apps or improving current apps, all while reusing existing data that was created by other apps.” (Solid, n.d.)

List of Further Readings for Solid:

- Mansour, E., Sambra, A.V, Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., Aboulnaga, A., and Berners-Lee, T. A Demonstration of the Solid Platform for Social Web Applications. *WWW '16 Companion Proceedings of the 25th International Conference Companion on World Wide Web.* Retrieved from https://doi.org/10.1145/2872518.2890529
- Sambra, A.V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., Berners-Lee, T. (2016). Solid: A platform for decentralized social applications based on linked data. Retrieved from http://emansour.com/research/meccano/solid_protocols.pdf

Section Sources

Andreasyan, T. (2018, March 19). Mastercard and IBM join forces for new “data trust”, Truata. *Baking Tech.* Retrieved from https://www.bankingtech.com/2018/03/mastercard-and-ibm-join-forces-for-new-data-trust-truata/

Carey Olsen. (2017, March 23). An overview of the types and uses of Guernsey law trusts. *Carey Olsen.* Retrieved from https://www.careyolsen.com/briefings/overview-types-and-uses-guernsey-law-trusts

Copenhagen Solutions Lab. (n.d.). City Data Exchange. *Copenhagen Solutions Lab.* Retrieved from https://cphsolutionslab.dk/en/news/city-data-exchange

Finley, K. (2017, April 4). Tim berners-lee, inventor of the web, plots a radical overhaul of his creation. *Wired.* Retrieved from https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/

Herlihy, P. (2013, October 31). 'Government as a data model' : what I learned in Estonia. *Gov.uk.* Retrieved from https://gds.blog.gov.uk/2013/10/31/government-as-a-data-model-what-i-learned-in-estonia/

IAPP. (2018, March 16). Mastercard, IBM launching 'data trust' to help with GDPR compliance. *IAPP.* Retrieved from https://iapp.org/news/a/mastercard-ibm-launching-data-trust-to-help-with-gdpr-compliance/

Keane, J. (2018, May 28). Why Mastercard and IBM chose Dublin as the base for their new data protection trust. *FORA.* Retrieved from https://fora.ie/truata-gdpr-4029849-May2018/

Ozanne, S. (2017, November 23). Guernsey Data Trusts: Three Important Reasons Why You Should Use Them. *We Are Guernsey.* Retrieved from https://www.weareguernsey.com/literature/2017/guernsey-data-trusts-three-important-reasons-why-you-should-use-them/

Santa Clara County Office of Education. (2017, January 18). Silicon Valley Regional Data Trust: Investing in the Future of Children, Families, and Communities. *SCCOE.* Retrieved from https://www.sccoe.org/news/NR/Pages/011817-Investing-in-children-families-communities.aspx
Silicon Valley Regional Data Trust. (n.d.). About Us. *SVRDT.* Retrieved from http://www.svrdt.org/about-svrdt/

Sidewalk Labs. (2018, October). Digital Governance Proposals for DSAP Consultation. *Sidewalk Labs.* Retrieved from https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES

Solid. (n.d.). Homepage. *Solid.* Retrieved from https://solid.mit.edu/

Truata. (2018, November 28). Trūata Wins Prestigious International Privacy Innovation Award. *Truata.* Retrieved from

https://www.truata.com/2018/11/28/truata-wins-prestigious-international-privacy-innovation-award/

Wray, S. (2018, May 29). Copenhagen shares takeaways from its City Data Exchange. *Smart Cities World.* Retrieved from https://www.smartcitiesworld.net/news/news/copenhagen-shares-takeaways-from-its-city-data-exchange-2961

Open Data Institute

What is the Open Data Institute

- https://theodi.org/article/what-is-a-data-trust/
- https://theodi.org/article/defining-a-data-trust/

- Data trust pilots:
https://theodi.org/article/uks-first-data-trust-pilots-to-be-led-by-the-odi-in-partnership-with-central-and-local-government/

Academic Literature, Journal Articles, White Papers

O'hara, K. (2019). Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship. *University of Southampton [White Paper].* Retrieved from https://eprints.soton.ac.uk/428276/

White paper aims to explore what existing structures can data trusts exploit, and what relationships data trusts have with formal understandings of trusts in law. It heavily focuses on ODI literature and Wendy Hall and Jérôme Pesenti's understandings of a "data trust" in the context of AI. The paper defends this thesis: "A data trust works within the law to provide ethical, architectural and governance support for trustworthy data processing" (O'hara, 2019, p. 6). It also mentions Delacroix and Lawrence's paper that argue how data trusts have little in common with the traditional legal definition of a "trust." O'Hara also proposes a possible data trust architecture that would enhance "trustworthiness."

Definitions

- **Hall and Pesenti's definition of Data Trusts (in context of AI):** "data trusts should be "proven and trusted frameworks and agreements" that supply the trust that will "ensure exchanges [of data] are secure and mutually beneficial" (O'hara, 2019, p. 6)
    - Assumes that data sharing is inherently risky: personal data sharing may put people at risk, exposing organizations to reputational damage, or to lose trade secrets by sharing. (O'hara, 2019, p. 6)
- **ODI Data Trust Definition:** "a legal structure that provides independent third- party stewardship of data" (O'hara, 2019, p. 6)
- **"Trust" definition [law]:** "A trust is a legal relationship in which an asset is run by a trustee for the benefit of a beneficiary. Even though the trustee owns the asset in law, she is not allowed to run it for her own benefit, but has a fiduciary duty to ensure that the benefits fall to the beneficiary" (O'hara, 2019, p. 6)
    - Leans on US and UK common law

Data Trust Functions

- **Needs to fulfill two functions:**
    - Must be an area where "data processing and data science can take place transparently, allowing data controllers to be held accountable… it should also allow data scientists to interact and debate what constitutes trustworthy behaviour in their profession." (O'hara, 2019, p. 6)
    - "needs to be an interface between data scientists, data subjects and other stakeholders. This should allow stakeholders both to hold data scientists to account themselves, and also to inject their own views about what constitutes trustworthy behaviour by data scientists" (O'hara, 2019, p. 6)
- **Data trusts should have multiple models:** There is "no 'one size fits all' data trust, but a range of models should be available, as argued, for different reasons" (Delacroix and Lawrence, 2018 in O'hara, 2019, p. 7)

- **All kinds of data (personal, non-personal) can have trust issues:** “The trust issues that arise in data sharing are not restricted to the sharing of personal data; non-personal data can be sensitive too” (O’hara, 2019, p. 7)
- **Trust deficit even in GDPR regime:** “trust is a relative term – X trusts Y to do something in a particular context (O’Hara 2012)... [In the GDPR] The focus on personal data is already too weak to protect us from all the inappropriate interventions that data processing can afford.” (O’hara, 2019, p. 8)
- **Trust concerns the entire data assemblage:** “many of the trust problems… go beyond the problems of the data subject, covering the doubts of data providers, data consumers and other stakeholders. Data protection does little for the concerns of these stakeholders.” (O’hara, 2019, p. 8)

<u>Theoretical Approaches of Trust and Data Trusts</u>

- **Data protection as a rights-based, neoliberal function:** In the GDPR, “the data subject is seen as the defender of her own interests in a complex marketplace. This neoliberal view of the data protection regime sits alongside other mechanisms where the onus is on the individual to understand and express her own preferences, and to ensure they are met, where possible, through her own efforts” (O’hara, 2019, p. 9)
    - **Rights-based approach problems:** “In the rights arena, the individual is warned that the world is full of potential threats to her well-being, and by bad actors who will not treat her with the dignity proper to a human being, and that she therefore needs conventions and courts to protect her.” (O’hara, 2019, p. 9)
    - **Neoliberal-based approach problems:** “Under neoliberalism, which aims to expand freedom by shrinking public space and growing the powers of private actors under market conditions, the individual is told that she must pursue her own interests, because no-one else will do it for her.” (O’hara, 2019, p. 9)
    - <u>In both the rights-based and neo-liberal approaches, the data subject is on their own.</u> (O’hara, 2019, p. 11)
    - **Social licenses:** Trust is built in various professions through codes of conducts, licenses, etc. before they can operate in a community. Following sociologist Everett Hughes’ notions of license and mandate, O’Hara argues that trust is a negotiation – ”the delicate and informal nature of the licence provides no guarantee that trust will be preserved if the professional goes too far” (O’hara, 2019, p. 10)
        - Communication is key to gain trust (O’hara, 2019, p. 10)

<u>Data Trusts diverge from a rights-based or neoliberal-based approach to data:</u>

1) **Compromise between parties is essential to trust:** “its starting point would be the compromise between trustor and trustee that is essential for creating trust in the first place.” (O’hara, 2019, p. 11)
2) **Data scientists must have expertise:** “the expertise of the data scientist is a central part of the picture.” (O’hara, 2019, p. 11)

- "With a data trust, data scientists can (and should) engage with data subjects and other stakeholders to determine what kind of treatment of data is acceptable"
- **Must have meaningful avenues of engagement:** "The data scientists should absolutely not assume, ab initio, that they have a monopoly of rationality" (O'hara, 2019, p. 11)
- **People don't have time or expertise to control their data:** Sending notifications about data flows, third parties, etc. "is well- meant transparency, but hardly useful to the data subject (O'Neill 2009), who not only has better things to do but who also may struggle to understand a highly complex document containing several names of companies of which he has probably not heard, performing actions, such as auctioning adverts, whose significance is unclear to him, and which may not do him any tangible harm" (O'hara, 2019, p. 11)

3) **Data trust as an accountability mechanism:** "the data trust would be a centre for data processing that could be used to hold data scientists accountable, auditing how they treat the data and who is allowed access." (O'hara, 2019, p. 11)
4) "the data trust would aid transparency by being inspectable and scrutable." (O'hara, 2019, p. 11)
    - This would allow individuals and representative groups to intervene (O'hara, 2019, p. 11)
    - "the real advantage of a data trust is that it would allow data scientists to be transparent and accountable to their peers." (O'hara, 2019, p. 11)
5) **Data trust as an exercise in examining consent, and legal processing** "a data trust might even help with determining which processing is legal. GDPR provides for a number of grounds for data processing, of which one of the most important is consent. If a data trust were well- enough known and trusted, then it might become the focus of consent" (O'hara, 2019, p. 11)
    - Data subjects would be asked at the time of collection whether they consented "to the use of their data within a (specified?) data trust, for purposes consistent with the principles underlying the trust." (O'hara, 2019, p. 11)
    - Data trust could serve as a "convenient point of contact for a data subject who wished to withdraw consent at a later date." (O'hara, 2019, p. 11-12)

Considerations:

- **Data trusts should be voluntary:** "The point of the data trust is to signal and to demonstrate the trustworthiness of the data processing… legislation and regulation constrain data processing, but not sufficiently to promote widespread trust" (O'hara, 2019, p. 12)
- **"Trust and trustworthiness are two sides of the same coin:** trustworthiness is the virtue of reliably meeting one's commitments, while trust is the belief of another that the trustee is trustworthy (O'Hara 2012). Trust without trustworthiness is a severe vulnerability. Hence what is needed is a means for (a) establishing the parameters of trustworthy data science, and (b) demonstrating to would-be trustors that the data

science is indeed trustworthy, so that they could be confident that their trust is warranted." (O'hara, 2019, p. 12)

The Anonymisation Decision-Making Framework (Data stewardship framework)

- **Notes:** O'Hara uses the ADF as an example to show how it could help inform ethical principles in the data stewardship model of a data trust.
    - Though it's about anonymization, "the use of this example, of an anonymisation methodology, does not mean that all data in a data trust should be anonymised (although some of it may be). It is rather that the ADF contains principles for responsible data stewardship that may be applicable outside its intended sphere." (O'Hara, 2019, p. 14)

- **Framework context:** "developed to support the complex task of anonymising data, under the legal regime of the Data Protection Directive in the EU. It was developed by the UKAN organisation, a joint venture of the Universities of Manchester and Southampton, the ODI, and the Office for National Statistics. It was adapted for the Australian data protection regime as the De-Identification Decision-Making Framework (DDF – O'Keeffe et al 2017), and is currently under further development to bring it into line with GDPR." (O'Hara, 2019, p. 12-13)

- **ADF component 1: Data situation audit**
    - "Ethical data stewardship must involve understanding the flow of data and its ramifications." (O'Hara, 2019), p. 14)
    - Two components in this:
        - 1) "understanding stakeholders' trust in the system. This is not simply whether this is high or low, but also what the stakeholders understand the data controller to be committed to, and for whom" (O'Hara, 2019), p. 14)
        - 2) "idea of a data environment. The insight of the ADF is that whether data is anonymous is not a function of the data alone. Much depends on the context in which data is held… As the context changes, so will the risk." (O'Hara, 2019, p. 14)

- **ADF Component 2: Impact management**
    - "This area of data management is often overlooked, so responses to emergencies are often ad hoc, opaque and improvised. The immediate instinct of an organisation is to minimise liability, which can result in slow responses and even dissembling, while messaging is cleared with lawyers. The result is an apparent shiftiness, which is easily taken as a signal of untrustworthiness." (O'Hara, 2019, p. 15)

    - Three components to impact management in the ADF:
        - 1) Standardized governance and architecture: "there needs to be a plan about how data sharing will be managed. Within a data trust, much of this

will be standardised within the trust's governance and architecture." (O'Hara, 2019, p. 15)

- 2) Communications plans ahead of time: "plan how to communicate with stakeholders, particularly in the event that something goes wrong. This involves each organisation in the data trust maintaining a line of communication with stakeholders in the data it holds" (O'Hara, 2019, p. 15)
- 3) Plan for when things go wrong: "If there is a data breach, how can it be closed down quickly? Who needs to be informed, by whom, and with what messaging? If an organisation within the data trust is held accountable, how will it be disciplined? Will it be expelled? If so, how will this be managed, for instance if it has shared valuable data with other organisations in the trust." (O'Hara, 2019, p. 16)

O'Hara's Recommendation for a Data Trust Architecture for Trustworthiness

O'Hara identifies eight desirable properties in a data trust architecture (O'Hara, 2019, p. 17):

1) **Discovery:** Users need to be able to know about the properties and quality of the data.
2) **Provenance:** Users need to be able to assess data quality by accessing metadata, etc.
3) **Access controls:** "Data controllers need to be able to retain control over who gets access. Users need to engage with data controllers to discuss the terms and conditions for sharing. The liability for data protection breaches, therefore, remains with the data controllers where the data is personal."
4) **Access:** "Users need a mechanism to get access to the data. Access need not be unconditional, and could be mediated, or be to a limited quantity of the data, or to a redacted, anonymised or pseudonymised version."
5) **Identity management:** "Data controllers need to be able to identify those attempting to get access through time."
6) **Auditing of use:** "A record of uses of data needs to be generated and stored. This needs to be transparent, so that it can be checked for compliance with the law, and compliance with the ethical principles agreed by trust members."
7) **Accountability:** "data controllers are accountable for the use of the data under their control, and the audit must enable them to be held accountable for misuse. Similarly, those receiving data and misusing it must also be held accountable."
8) **Impact:** "The value, use and misuse of data also ought to be assessed via the records kept in the data trust."

Possible architecture for a data portal:

** Inspired by the The Web Observatory

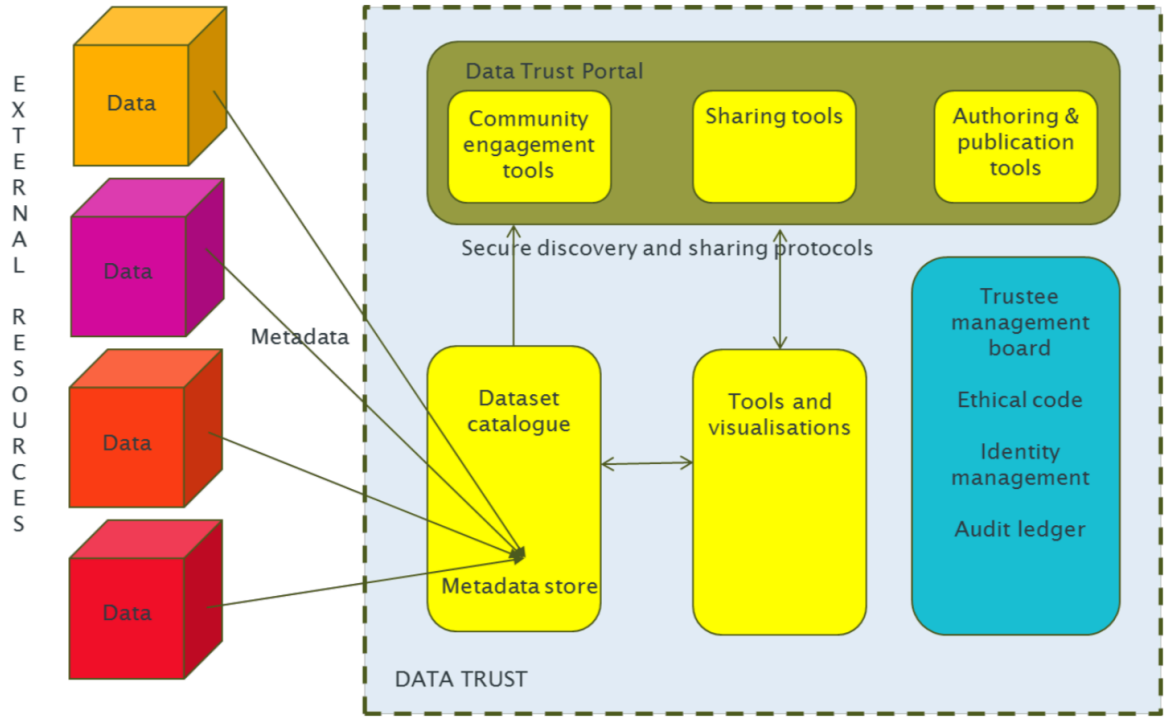


Figure 1: Architecture for a Data Trust portal

- "data does not get into the DTP at all; the DTP is not a data store, nor a distributed database. The data is held by the original data controllers, in their own controlled environments, and they retain their data protection responsibilities if the data is personal data. They do not transfer the data (unless they wish to), and remain in ultimate control of access. Different datasets can be treated differently." (O'Hara, 2019, p. 18)

- **Benefits of O'Hara's Data Trust Portal:** Data sharing arrangements could be automated or applied to some datasets; access can be tiered ($$ wise), data controllers are in control because they only share when they want to; individuals with wearable device data can contribute if they want to if they abide by ethics; data will have metadata and provenance summaries that could become a dataset catalogue (O'Hara, 2019, p. 18-19)

<u>Legal status of a "Data Trust"</u>

- **O'Hara argues that data trusts are too complex to make a "literal trust":** "the proposed arrangement in the data trust differs from the property arrangements typical of a trust, and partly because a trust is a development of common law, and is not always found in civil law jurisdictions (Penner 2016, 52ff.)" (O'Hara, 2019, p. 20)
- **But can take components of a trust:** where "property is owned and managed by a trustee for the benefit of a beneficiary." (O'Hara, 2019, p. 20)

- **Trusts established by law (top-down):** An example are TABOLs – Trusts Arising By Operation of Law. O'Hara argues that it can be seen as "a top-down type of trust, where law mandates the creation of a certain type of structure." (O'Hara, 2019, p. 20)
    - " top-down approach would require some legislation in a world where the full effects of GDPR are not yet known, which would be not only unlikely but positively unwise." (O'Hara, 2019, p. 20)
- **Voluntary trusts (bottom-up):** "data subjects would compel their data to be managed by trustees, and would set the terms of its management (Delacroix & Lawrence 2018)" (O'Hara, 2019, p. 20)
    - "requires a somewhat proactive attitude from data subjects; it is not impossible to imagine, but would undoubtedly place a burden on data subjects however willing a cohort of trustees can be mustered" (O'Hara, 2019, p. 20)
- **Hall and Pesenti's "Middle-out trust":** "data controllers are prime movers, wanting to maintain warranted trust without losing control… The middle-out approach has not been explored in detail, and has many pragmatic points to commend it as a 'good enough' solution to a social problem that does not concern everyone." (O'Hara, 2019, p. 20)
- **Data trusts can't please all beneficiaries, and will look different based upon who they are;** "one would hope that trustworthy data stewardship would raise the level of trust all round." (O'Hara, 2019, p. 20)

<u>The end goal of data trusts:</u>

- **O'Hara argues that data trusts support <u>warranted trust:</u>** "To conclude, the purpose of a data trust is to define trustworthy and ethical data stewardship, and disseminate best practice. The aim is not to increase trust, which many have claimed as an imperative. The aim, rather, is to align trust and trustworthiness, so that we trust trustworthy agents and do not trust untrustworthy ones, and conversely make it so that trustworthy agents are more likely to be trusted, and untrustworthy agents less likely to be trusted. In other words, the aim is to support warranted trust."

Sylvie Delacroix & Neil D. Lawrence (2018). *Disturbing the 'One Size Fits All', Feudal Approach to Data Governance: Bottom-Up Data Trusts*,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265315

Balkin, J. (2016). Information Fiduciaries and the First Amendment. *UC Davis Law Review.* Retrieved from https://isp.yale.edu/sites/default/files/930am_49-4_balkin.pdf

Data Trusts in the Media

Build and annotate popular literature geared towards the public about data trusts (news sources, blogs)

McDonald, S. (2015, June 17). Toward (a) Civic Trust: No Experimentation Without Representation. *Medium.* Retrieved from https://medium.com/@McDapper/toward-a-civic-trust-e3265768dfe6

Balkin, J. and Zittrain, J. (2016, October 3). A Grand Bargain to Make Tech Companies Trustworthy. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/

- "To protect individual privacy rights, we've developed the idea of "information fiduciaries. In the law, a fiduciary is a person or business with an obligation to act in a trustworthy manner in the interest of another."
- **Definition:** "An information fiduciary is a person or business that deals not in money but in information."
- "To deal with the new problems that digital businesses create, we need to adapt old legal ideas to create a new kind of law—one that clearly states the kinds of duties that online firms owe their end users and customers."
    - "The most basic obligation is a duty to look out for the interests of the people whose data businesses regularly harvest and profit from."
    - **Things to do:** Need fairness and accountability for both parties; need to determine fiduciary duties; and persuade companies that information fiduciaries make sense
- Discusses the transformation of copyright law where "online intermediaries willingly took on new responsibilities in order to create a predictable business environment."
    - DMCA safe habour: "If an online business received notice from a copyright owner that content was infringing, it could avoid copyright liability by promptly removing the content; and if the original uploader responded by identifying him- or herself and claiming fair use, the content would be restored."
- **Balkin and Zittrain's data trust model is like a safe harbour (a sort of Digital Millennium Privacy Act)**: "Companies could take on the responsibilities of information fiduciaries: They would agree to a set of fair information practices, including security and privacy guarantees, and disclosure of breaches. They would promise not to leverage personal data to unfairly discriminate against or abuse the trust of end users. And they would not sell or distribute consumer information except to those who agreed to similar rules. In return, the federal government would preempt a wide range of state and local laws."
    - **The "Digital Millennium Privacy Act" would be less burdensome than figuring out regional rules:** "Even without the public giving up on any

hard-fought privacy rights recognized by a single state, a company could find that becoming an information fiduciary could be far less burdensome than having to respond to multiple and conflicting state and local obligations."

Lawrence, N. (2016, June 3). Data trusts could allay our privacy fears. *The Guardian.* Retrieved from https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy

- **Discusses NHS-Google DeepMind data sharing deal and problems:**
    - Company claims use is purposeful: "Royal Free and DeepMind contentiously claim that they are using the records for "direct care" of patients, meaning the hospital trust is able to oversee the implementation of the data sharing partnership."
        - Balances patient ownership of data with the "wider patient interest" "It aims to derive the mutual benefit, just like in a land society, but members of a land society were voluntary participants." (these people are not)
    - Patients have no voice: "The patients themselves have no direct voice in the regulatory framework. The hospital uses the principle of implicit consent and is under no obligation to even make the individual patients aware of the deal. This seems unacceptable."
        - "Legally the patient is referred to as a data subject. This term has unfortunate, but perhaps not inaccurate, connotations of royal prerogative."

- **Enter the data trust:** a "mutual organisation formed to manage data on its members' behalf. Data subjects would pool their data forming a trust, stipulating conditions under which data could be shared. The trust would retain a duty of care without conflicting goals such as making a profit or furthering a research career."
    - "By collating data, the trusts would become powerbrokers themselves, data-brokers."
    - "Like the land societies of old, data would be used for our mutual benefit governed by our mutually determined conditions and with our mutual consent."

- **Sharly Note for comparison:** Kind of like prescribed entity in PHIPA because subjects have no consent but problem is that the UK has no proper oversight or transparency mechanisms of reporting to the public, and the data goes to private companies. In prescribed entities, data goes to non-profits or academic/medical research.

Thornhill, J. (2017, October 30). Would you donate your data for the collective good? *Financial Times.* Retried from https://www.ft.com/content/00390a76-bd4a-11e7-9836-b25f8adaa111

Heller, N. (2018, April 12). We may own our data, but Facebook has a duty to protect it. *The New Yorker.* Retrieved from

https://www.newyorker.com/tech/elements/we-may-own-our-data-but-facebook-has-a-duty-to-protect-it

Verhulst, S., Sangokoya, D., and the GovLab. (2015, April 22). Data Collaboratives: Exchanging Data to Improve People's Lives. *Medium.* Retrieved from https://medium.com/@sverhulst/data-collaboratives-exchanging-data-to-improve-people-s-lives-d0fcfc1bdd9a

Summary and Areas for Future Research

- Short Summary of Key points and areas for future research

Summaries

Canadian Case Studies
The key point in these Canadian case studies is that these entities can manage data without individual consent because of pre-approved privacy practices. In the case of prescribed entities under Ontario's PHIPA, these practices are approved by the Information Privacy Commissioner of Ontario (IPC) every three years.

City Data Trusts
Civic data trusts are trying to solve the issues of obtaining meaningful individual consent from the people whom city data is collected from. Much of the city data is collective or de-identified such as sensor data from stop lights or bike paths. However, there are questions raised about collective and group rights, and re-identification.

Future Research

Collective and group rights

- The First Nations Information Governance's work heavily focuses on collective rights to information collection and management with its OCAP principles.

Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017). *Group Privacy.* New York, NY: Springer International Publishing. Retrieved from https://www.springer.com/gp/book/9783319466064

- Full pdf in Literature Materials folder here