From Data Subject to Data Citizen

REALIZING THE PROMISE OF DIGITAL PRIVACY AND AUTONOMY
1970: A Mainframe view of the world

Fair Information Practices emerged in the 1970s and that architectural view of data
1970’s Fair Information Practices assumed that there are only a few data castles, and you can trust the guardians of your data.
Today’s Fair Information Practices

After years of negotiation, the General Data Protection Regulation passed in 2016 and went into effect in 2018.

This begs the question: 

Is a law based on a 1970 view of computers and networks fit for purpose in the 21st century?
2020: A Cloud of Servers

This is the reality behind the cloud. Racks of servers holding unprecedented amounts of data. The increase in global data storage is being measured in zettabytes.

That is $10^{21}$ or $1,000,000,000,000,000,000,000$ bytes.
2020: Every endpoint connected

Computers are always on and are making connections globally and constantly
Data Sharing

From a million people of MySpace in 2004 to more than 2 billion people on Facebook, it would seem we love to share.
Yes, I have read and understand the Terms and Conditions/Privacy Policy...

As of April 2019 there are 7,040 firms identified in this Marketing Technology Landscape.

Notice and Consent is broken

"The control we get from modern privacy regulations is like a distributed denial of service (DDoS) attack on our brains."

Hartzog, Woodrow. Privacy’s Blueprint (p. 65).
Harvard University Press.
The intent of privacy laws

GDPR: Rules to protect the processing of personal data and fundamental rights and freedoms

PIPEDA: An act to support and promote electronic commerce by protecting personal information
The results

Regulatory Burden
Tends to favour large companies
Reduces scope for innovation

Platform dominance
Builds large companies
Start-ups build to be acquired instead of building for competition

Power Asymmetry
Reduced effective autonomy
Social and Political impacts
Dark Patterns
But the Reports of the Death of Privacy are exaggerated

The history of technology being used to collect information about us is replete with news stories about the death of privacy.

But the very persistence of these stories suggests that there is something in the human condition that demands or requires privacy, whatever the context.
The road forward

It’s a bit foggy, but elements include:

- Replacing Platforms with Protocols
- Empowering Individuals
- A digital social contract
Instead of breaking up tech companies, when platform technologies emerge, they should be required to provide interoperability and accountability. The Internet was built on interoperable protocols.

Imagine, for example what would have happened if email had emerged as a ‘platform’ instead of a Simple Mail Transfer Protocol (SMTP)? That protocol enables us to choose between email vendors and companies, from Google Gmail or Microsoft Exchange/Outlook to Proton Mail or setting up our own servers. We have competition, innovation and a dearth of regulation over the specific technology.

We already have examples of user centered standards and protocols the provide choices, enable accountability and empower users.
User Centred Protocols

- User Managed Access
- Consent Receipts
- Information Sharing Agreements
User Managed Access Protocol

User-Managed Access (UMA) is an award-winning OAuth-based protocol designed to give an individual a unified control point for authorizing who and what can get access to their digital data, content, and services, no matter where all those things live.

- OAuth enables constrained delegation of access to apps
- OpenID Connect does modern-day federation
- To OAuth, UMA adds cross-party sharing in a wide ecosystem

Typical Use Cases

- Alice-to-Bob (person-to-person) delegated sharing of health data/devices, financial data, connected cars...
- Enterprise-initiated delegated sharing – enterprise API access management, access delegation between employees...
- Alice-to-Alice (person-to-self) delegated sharing – proactive policy-based sharing of OAuth-style app connections

A protocol that empowers the individual to decide and control what is done with the data that they have rights over.
Consent Receipt Standard

A Consent Receipt is record of authority granted by a Personally Identifiable Information (PII) Principal to a PII Controller for processing of the Principal’s PII. The record of consent is human-readable and can be represented as standard JSON. This specification defines the requirements for the creation of a consent record and the provision of a human-readable receipt. The standard includes requirements for links to existing privacy notices & policies as well as a description of what information has been or will be collected, the purposes for that collection as well as relevant information about how that information will be used or disclosed.

An accountability artefact and JSON for consent
An information sharing agreement protocol is a protocol for two parties to come to an agreement on the terms for data sharing and then to share the data. There is a new Kantara team to create the standard.

The JLINC protocol is an implementation of this notion that based on Decentralized identifiers and Standard Information Sharing Agreements. 

https://protocol.jjlinc.org
Privacy Engineering

NIST Privacy Framework
ISO Privacy 27701
IEEE Data Privacy Process
NIST Privacy Framework

The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders. It is adaptable to any organization’s role(s) in the data processing ecosystem. It can be used to help identify and prioritize actions for reducing privacy risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk.

- Functions: Foundational Privacy Activities
- Categories are groups of privacy outcomes
- Subcategories are specific technical or management activities
ISO 27701 Standard

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d’ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

8 Additional ISO/IEC 27002 guidance for PII processors
   8.1 General
   8.2 Conditions for collection and processing
      8.2.1 Customer agreement
      8.2.2 Organization’s purposes
      8.2.3 Marketing and advertising use
      8.2.4 Infringing instruction
      8.2.5 Customer obligations
      8.2.6 Records related to processing PII
   8.3 Obligations to PII principals
      8.3.1 Obligations to PII principals
   8.4 Privacy by design and privacy by default
      8.4.1 Temporary files
      8.4.2 Return, transfer or disposal of PII
      8.4.3 PII transmission controls
   8.5 PII sharing, transfer, and disclosure
      8.5.1 Basis for PII transfer between jurisdictions
      8.5.2 Countries and international organizations to which PII can be transferred
      8.5.3 Records of PII disclosure to third parties
      8.5.4 Notification of PII disclosure requests
      8.5.5 Legally binding PII disclosures
      8.5.6 Disclosure of subcontractors used to process PII
      8.5.7 Engagement of a subcontractor to process PII
      8.5.8 Change of subcontractor to process PII

Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers)
Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors)
Annex C (informative) Mapping to ISO/IEC 29100
Annex D (informative) Mapping to the General Data Protection Regulation
Annex E (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

Bibliography
IEEE Data Privacy Process

This standard defines requirements for a systems/software engineering process for privacy oriented considerations regarding products, services, and systems utilizing employee, customer or other external user’s personal data. It extends across the life cycle from policy through development, quality assurance, and value realization. It includes a use case and data model (including metadata). It applies to organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information. By providing specific procedures, diagrams, and checklists, users of this standard will be able to perform a conformity assessment on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.
Empowering Individuals

MYDATA OPERATORS

INFORMATION FIDUCIARIES

BOTTOM UP DATA TRUSTS
MyData Operators

- A Nordic Model for human-centered personal data management and processing
Information Fiduciaries

Service Providers and Cloud companies that collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end users.

Because of their special power over others and their special relationships to others, information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute. These duties place them in a different position from other businesses and people who obtain and use digital information.
Currently a lack of legal mechanisms that may plausibly empower us.

Return the power that stems from aggregated should be returned to individuals through the legal mechanisms of trusts.

Trustees would have a fiduciary obligation of undivided loyalty.

There would be a plurality of trusts rather than a ‘one size fits all’ approach.
A digital social contract

MYDATA GLOBAL  ME2B ALLIANCE  CIVIL SOCIETY
MyData Global's mission is to empower individuals by improving their right to self-determination regarding their personal data. The human-centric paradigm is aimed at a fair, sustainable, and prosperous digital society, where the sharing of personal data is based on trust as well as balanced and fair relationship between

https://mydataglobal.slack.com/signup
https://mydata.org/join/
https://mydata.org/mydata-global-membership-application/organisations/
Me2B Alliance

A different kind of SDO

- Multi-stakeholder by design
  - Me-s & B-s
- More than technical criteria
  - Ethics
  - Usability
  - Legal
- Results/Change- Focused

https://www.me2balliance.org/join.html

**OUR VISION**

**Ensuring human dignity in connected products and services**

We live in a connected world. The technology products and services we buy and use everyday, like smart phones, ride shares, and social media, generate and consume data. Data can be integral to the product or service, used to improve the products, or used to tailor services to your needs. However, sometimes data is used in ways that do not benefit you, cause you real harm or manipulate you.

The Me2B Alliance helps you know that technology products and services are giving you a fair deal and real agency: with your data, with your purchases, with your online activities.

*In short, that they are treating you right.*

**OUR MISSION**

**Growing the availability of trustworthy technology choices**

Businesses work with the Me2B Alliance to make sure that they and their suppliers are helping, not harming, consumers. We connect them to other companies that are already certified and have met the rigorous Me2B standards. Or, we work with them to get the companies they are already working with certified by addressing the economic, social and privacy needs of consumers. If a product or service meets all of our criteria, they may display the Me2B Mark to let shoppers know that they are managing your data ethically and responsibly, and that you have an active role in setting up the fair deal.
Civil Society

Canada
- CIPPIC
- Citizen Lab
- Open Media

International
- Access Now
- CDT
- EDRI
- EPIC
- Privacy International
There are real alternatives available for policy makers and technologists who want to move forward with user centered options. They will not only meet current regulatory requirements but future proof your organization or technology.
Thank you

FOR QUESTIONS OR FOLLOW UP: JOHN@WUNDERLICH.CA

Photo by Javier Allegue Barros on Unsplash