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

Data protection behind walls

1970'S FAIR INFORMATION PRACTICES ASSUMED THAT THERE ARE ONLY A FEW DATA CASTLES, AND YOU CAN TRUST THE GUARDIANS OF YOUR DATA.

Photo by Sandra Ahn Mode on Unsplash

Today’s Fair Information Practices

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

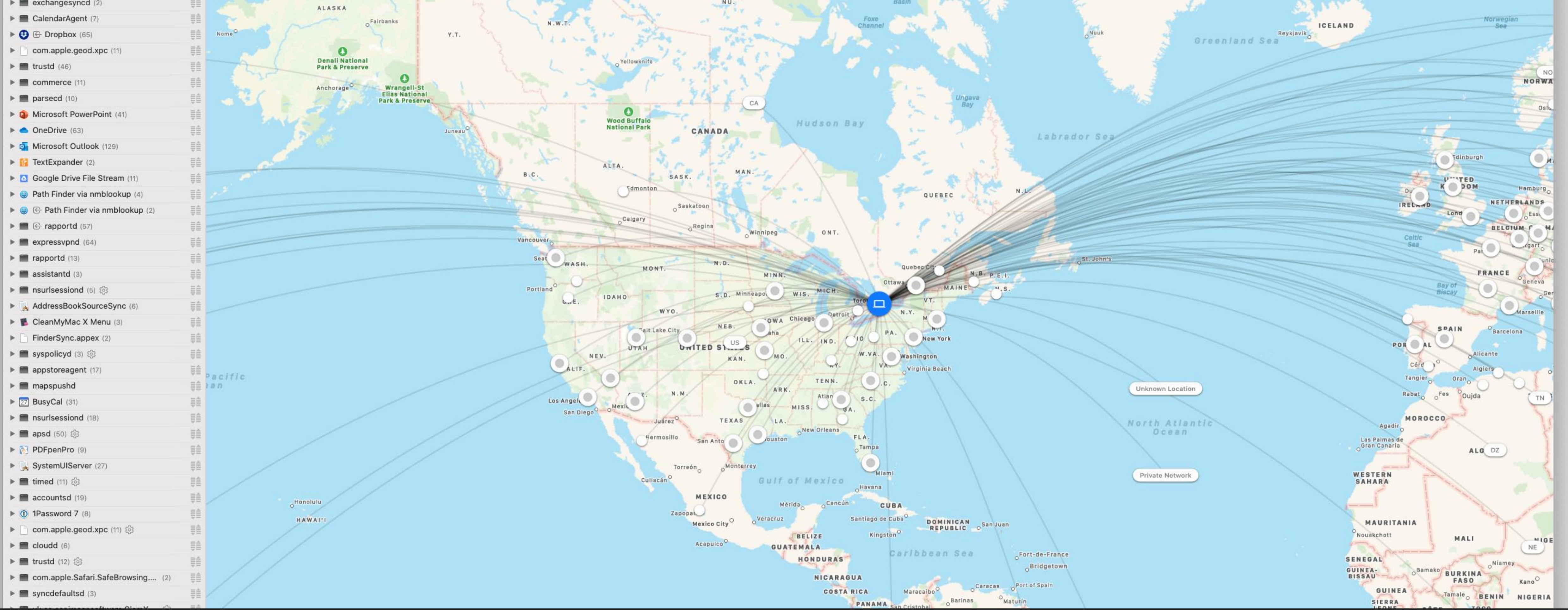
This begs the question:

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



exchangesyncd (2)
CalendarAgent (7)
Dropbox (65)
com.apple.geod.xpc (11)
trustd (46)
commerce (11)
parsecd (10)
Microsoft PowerPoint (41)
OneDrive (63)
Microsoft Outlook (129)
TextExpander (2)
Google Drive File Stream (11)
Path Finder via nmblookup (4)
Path Finder via nmblookup (2)
rapportd (57)
expressvpnd (64)
rapportd (13)
assistantd (3)
nsurlsessiond (5)
AddressBookSourceSync (6)
CleanMyMac X Menu (3)
FinderSync.appex (2)
syspolicyd (3)
appstoreagent (17)
mapspushd
BusyCal (31)
nsurlsessiond (18)
apsd (50)
PDFpenPro (9)
SystemUIServer (27)
timed (11)
accountsd (19)
1Password 7 (8)
com.apple.geod.xpc (11)
cloudd (6)
trustd (12)
com.apple.Safari.SafeBrowsing.... (2)
syncdefaultsd (3)

2020: Every endpoint connected

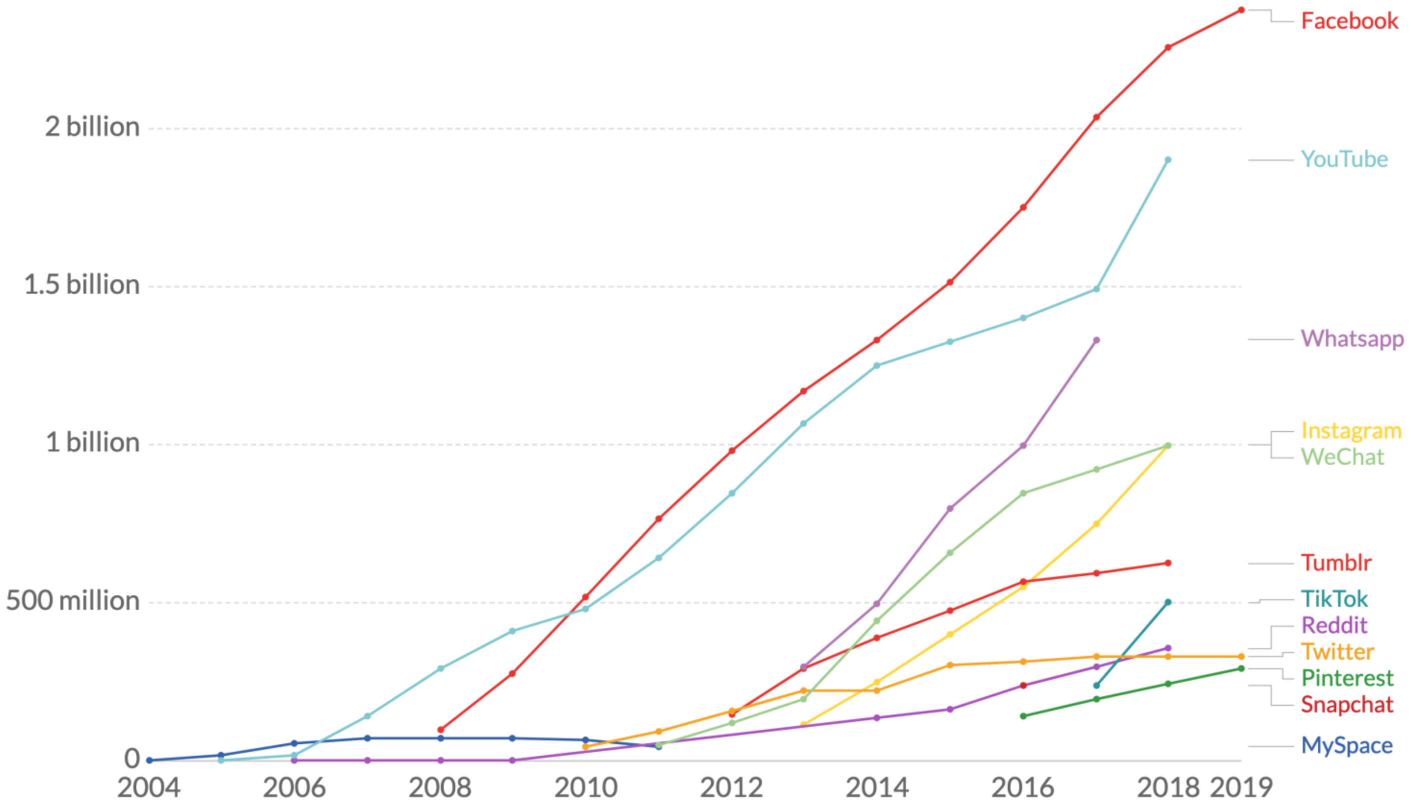
Computers are always on and are making connections globally and constantly

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.

Number of people using social media platforms

Estimates correspond to monthly active users (MAUs). Facebook, for example, measures MAUs as users that have logged in during the past 30 days. See source for more details.



Source: Statista and TNW (2019)

CC BY

Display & Programmatic Advertising
Search & Social Advertising
Native/Content Advertising
Video Advertising
PR
Video Marketing
Email Marketing
Content Marketing
Optimization, Personalization & Testing
DAM & MRM
SEO
Marketing Automation & Campaign/Lead Management
Events, Meetings & Webinars
Social Media Marketing & Monitoring
Advocacy, Loyalty & Referrals
Influencers
Community & Reviews
Conversational Marketing & Chat
Customer Experience, Service & Success
Channel, Partner & Local Marketing
Sales Automation, Enablement & Intelligence
Affiliate Marketing & Management
Ecommerce Marketing
Ecommerce Platforms & Carts
Marketing Analytics, Performance & Attribution
Mobile & Web Analytics
Dashboards & Data Visualization
Business/Customer Intelligence & Data Science
iPaaS, Cloud/Data Integration, RPA & Tag Mgmt
Product Mgmt
Budgeting & Finance
Collaboration
Projects & Workflow
Agile & Lean Mgmt

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.

https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/

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

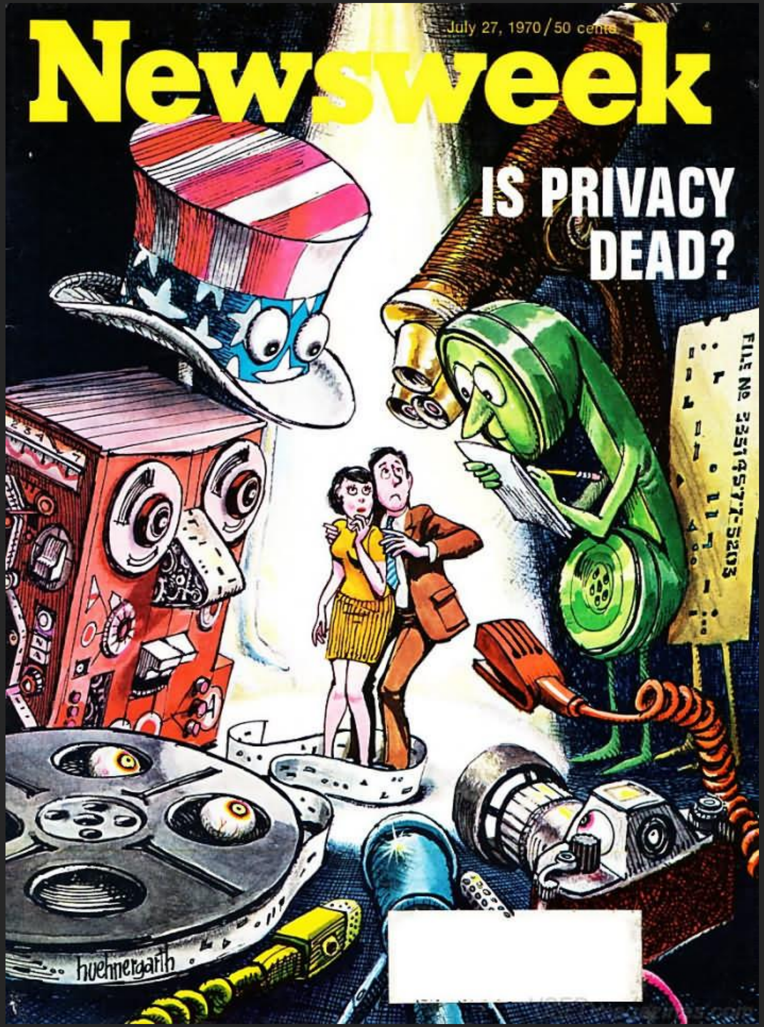
Social and Political impacts

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.



July 1970

Gauging the allure of designer drugs p. 469
Blown-up brains for a better inside view pp. 474 & 543
Single-crystal perovskite solar cells pp. 519 & 522
Science
$10
30 JANUARY 2015
sciencemag.org
AAAS
SPECIAL ISSUE
The End of
PRIVACY

January 2015

The road forward

It’s a bit foggy, but elements include:

Replacing Platforms with Protocols

Empowering Individuals

A digital social contract

Protocols not Platforms

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

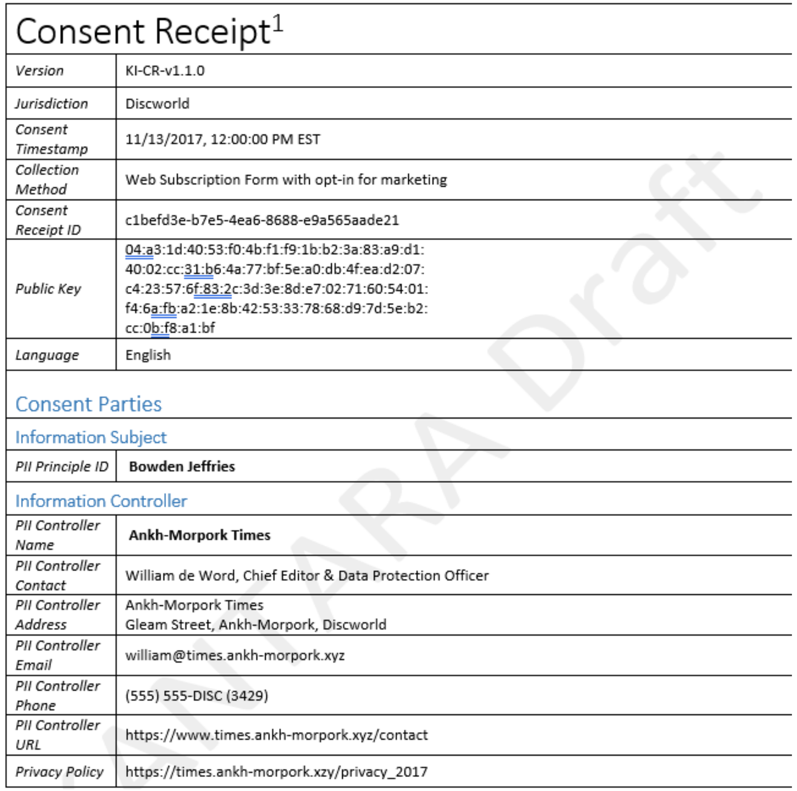
Typical Use Cases

- ○ 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 the 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.



Consent Receipt[1]

Version	KI-CR-v1.1.0
Jurisdiction	Discworld
Consent Timestamp	11/13/2017, 12:00:00 PM EST
Collection Method	Web Subscription Form with opt-in for marketing
Consent Receipt ID	c1befd3e-b7e5-4ea6-8688-e9a565aade21
Public Key	04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1: 40:02:cc:31:b6:4a:77:bf:5e:a0:db:4f:ea:d2:07: c4:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01: f4:6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2: cc:0b:f8:a1:bf
Language	English

Consent Parties

Information Subject

PII Principle ID	**Bowden Jeffries**

Information Controller

PII Controller Name	**Ankh-Morpork Times**
PII Controller Contact	William de Word, Chief Editor & Data Protection Officer
PII Controller Address	Ankh-Morpork Times Gleam Street, Ankh-Morpork, Discworld
PII Controller Email	william@times.ankh-morpork.xyz
PII Controller Phone	(555) 555-DISC (3429)
PII Controller URL	https://www.times.ankh-morpork.xyz/contact
Privacy Policy	https://times.ankh-morpork.xzy/privacy_2017

An accountability artefact and JSON for consent

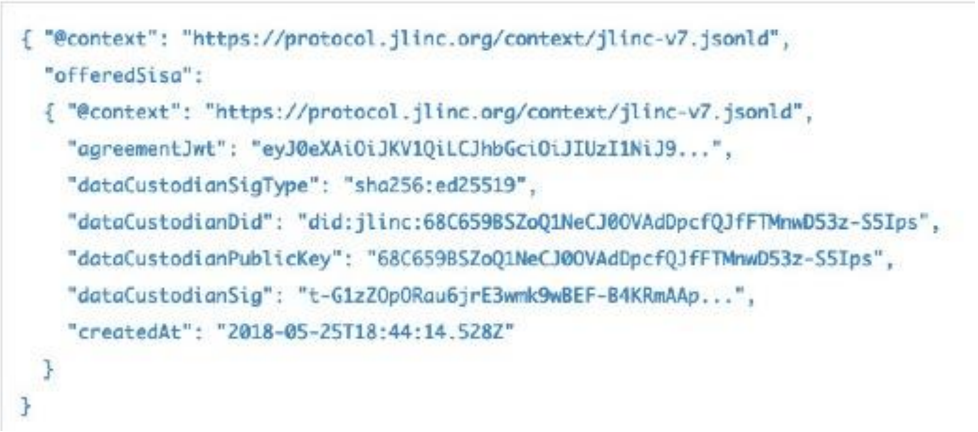
Information Sharing Agreement Protocol

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

Standard JSON-LD



```
{ "@context": "https://protocol.jlinc.org/context/jlinc-v7.jsonld",
  "offeredSisa":
  { "@context": "https://protocol.jlinc.org/context/jlinc-v7.jsonld",
    "agreementJwt": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9...",
    "dataCustodianSigType": "sha256:ed25519",
    "dataCustodianDid": "did:jlinc:68C659BSZoQ1NeCJ0OVAdDpcfQJfFTMnwD53z-S5Ips",
    "dataCustodianPublicKey": "68C659BSZoQ1NeCJ0OVAdDpcfQJfFTMnwD53z-S5Ips",
    "dataCustodianSig": "t-G1zZOpORau6jrE3wmk9wBEF-B4KRmAAp...",
    "createdAt": "2018-05-25T18:44:14.528Z"
  }
}
```

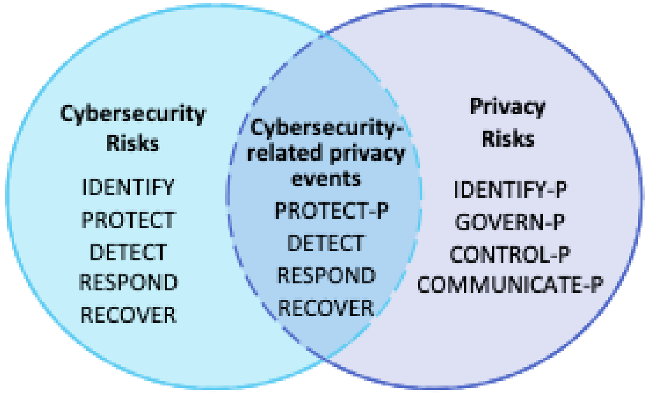
Privacy Engineering

NIST Privacy Framework

ISO Privacy 27701

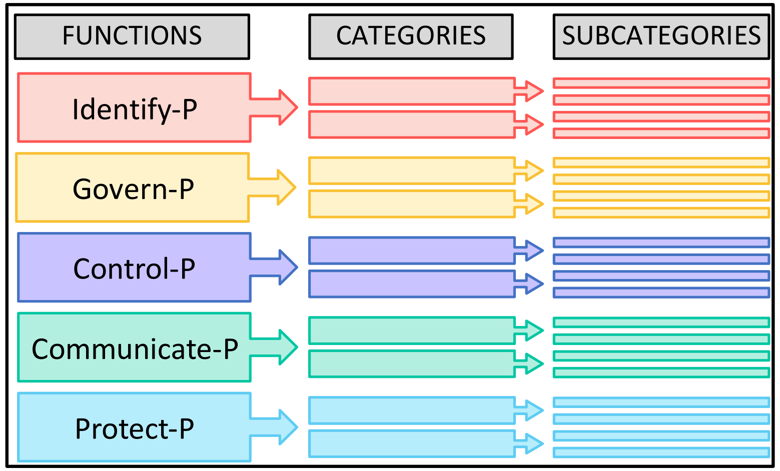
IEEE Data Privacy Process

NIST Privacy Framework

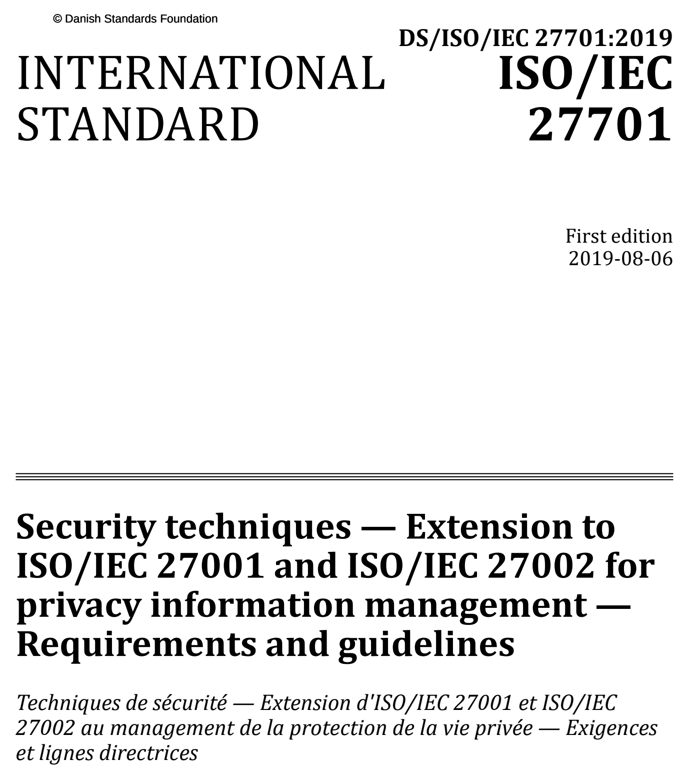


The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders. It is adaptable to any organization’s role(s) in the data processing ecosystem. It can be used to help identify and prioritize actions for reducing privacy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



DS/ISO/IEC 27701:2019

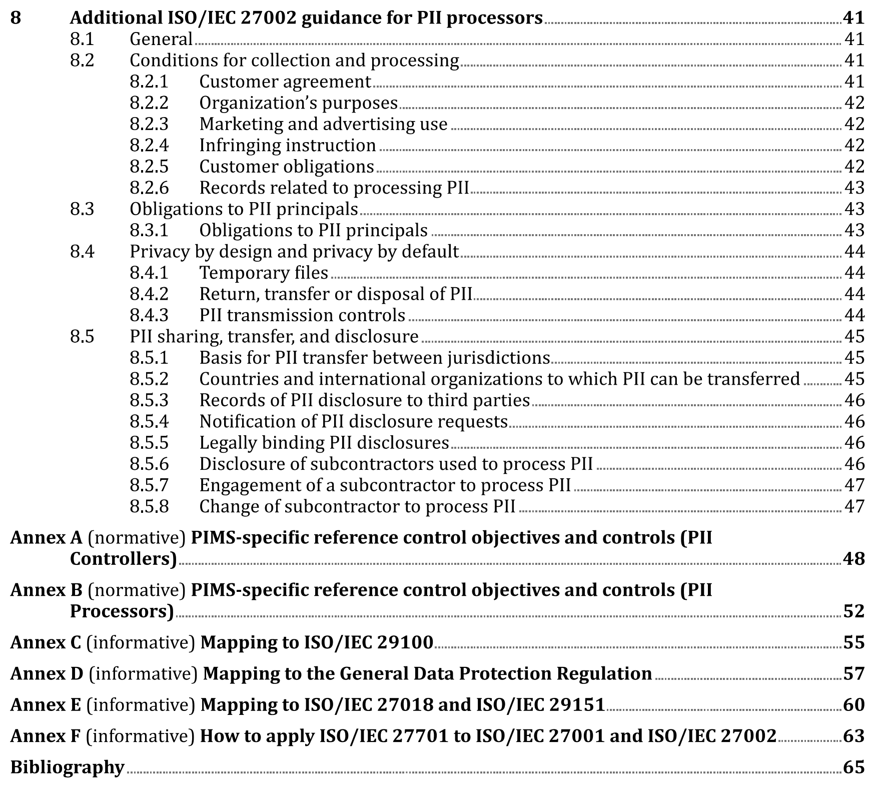
INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08-06

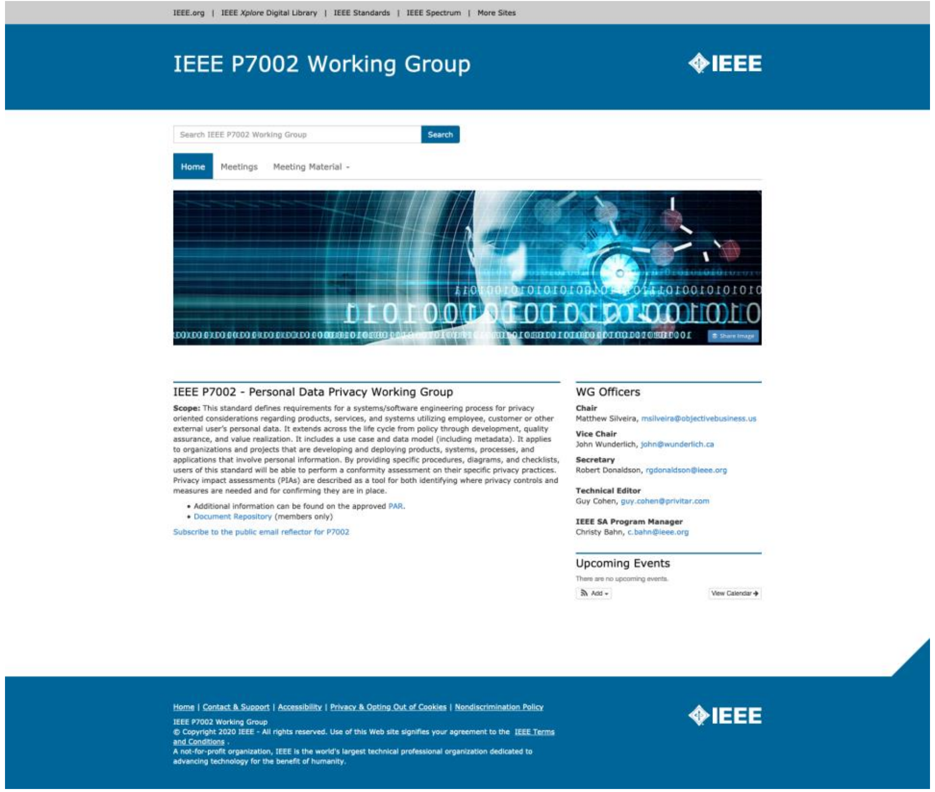
Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

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



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.


IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites
IEEE
Search IEEE P7002 Working Group
Search
Home
Meetings
Meeting Material
Share Image
Add
View Calendar
IEEE

IEEE P7002 Working Group

IEEE P7002 - Personal Data Privacy Working Group

Scope: 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.

- Additional information can be found on the approved PAR.
- Document Repository (members only)

Subscribe to the public email reflector for P7002

WG Officers

Chair
Matthew Silveira, msilveira@objectivebusiness.us

Vice Chair
John Wunderlich, john@wunderlich.ca

Secretary
Robert Donaldson, rgdonaldson@ieee.org

Technical Editor
Guy Cohen, guy.cohen@privitar.com

IEEE SA Program Manager
Christy Bahn, c.bahn@ieee.org

Upcoming Events

There are no upcoming events.

Home | Contact & Support | Accessibility | Privacy & Opting Out of Cookies | Nondiscrimination Policy

IEEE P7002 Working Group

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

Empowering Individuals

MYDATA OPERATORS

INFORMATION FIDUCIARIES

BOTTOM UP DATA TRUSTS

MyData Operators

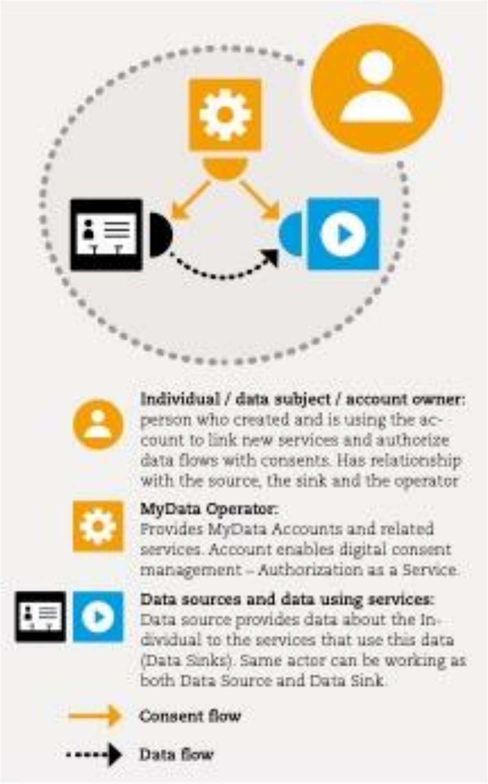
MyData

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

Ministry of Transport and Communications

Antti Poikola
Kai Kuikkaniemi
Harri Honko

This white paper presents a framework, principles, and a model for a human-centric approach to the managing and processing of personal information. The approach – defined as MyData – is based on the right of individuals to access the data collected about them. The core idea is that individuals should be in control of their own data. The MyData approach aims at strengthening digital human rights while opening new opportunities for businesses to develop innovative personal data based services built on mutual trust.



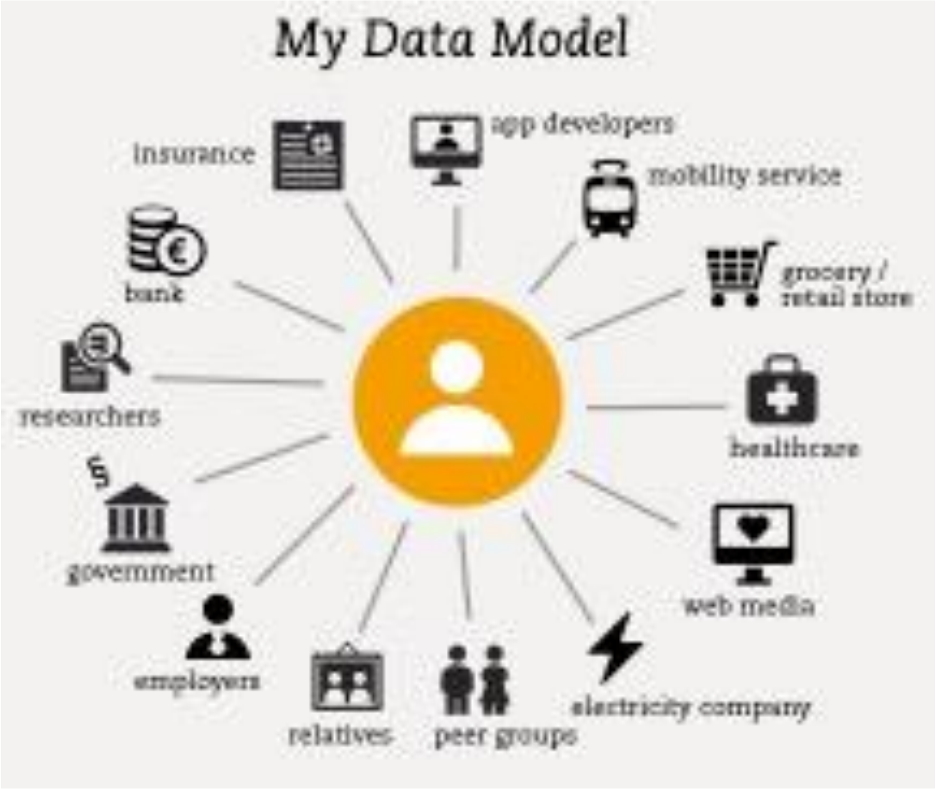
Individual / data subject / account owner: person who created and is using the account to link new services and authorize data flows with consents. Has relationship with the source, the sink and the operator

MyData Operator: Provides MyData Accounts and related services. Account enables digital consent management – Authorization as a Service.

Data sources and data using services: Data source provides data about the Individual to the services that use this data (Data Sinks). Same actor can be working as both Data Source and Data Sink.

Consent flow

Data flow

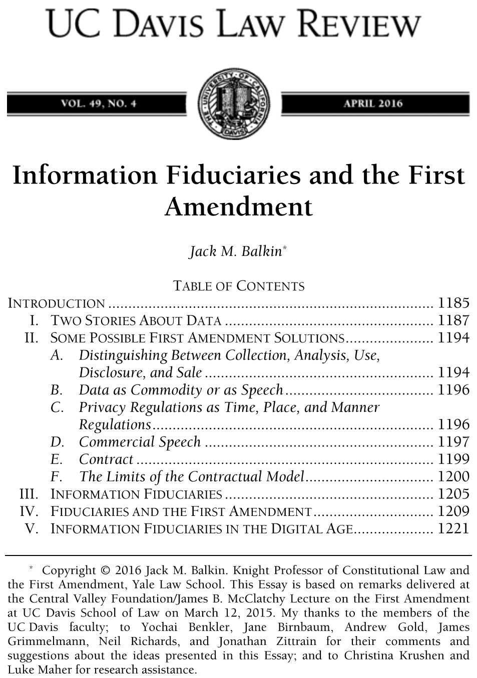


My Data Model

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.



UC DAVIS LAW REVIEW

VOL. 49, NO. 4 APRIL 2016

Information Fiduciaries and the First Amendment

Jack M. Balkin[*]

TABLE OF CONTENTS

[*] Copyright © 2016 Jack M. Balkin. Knight Professor of Constitutional Law and the First Amendment, Yale Law School. This Essay is based on remarks delivered at the Central Valley Foundation/James B. McClatchy Lecture on the First Amendment at UC Davis School of Law on March 12, 2015. My thanks to the members of the UC Davis faculty; to Yochai Benkler, Jane Birnbaum, Andrew Gold, James Grimmelmann, Neil Richards, and Jonathan Zittrain for their comments and suggestions about the ideas presented in this Essay; and to Christina Krushen and Luke Maher for research assistance.

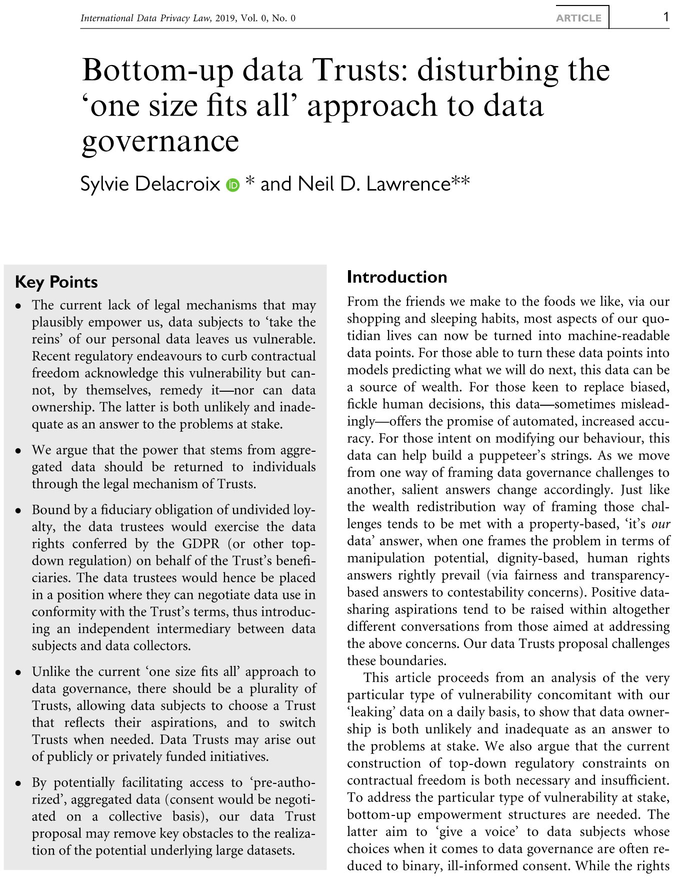
Bottom-Up Data Trusts

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.



International Data Privacy Law, 2019, Vol. 0, No. 0 ARTICLE 1

Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance

Sylvie Delacroix * and Neil D. Lawrence**

Key Points

- The current lack of legal mechanisms that may plausibly empower us, data subjects to ‘take the reins’ of our personal data leaves us vulnerable. Recent regulatory endeavours to curb contractual freedom acknowledge this vulnerability but cannot, by themselves, remedy it—nor can data ownership. The latter is both unlikely and inadequate as an answer to the problems at stake.
- We argue that the power that stems from aggregated data should be returned to individuals through the legal mechanism of Trusts.
- Bound by a fiduciary obligation of undivided loyalty, the data trustees would exercise the data rights conferred by the GDPR (or other top-down regulation) on behalf of the Trust’s beneficiaries. The data trustees would hence be placed in a position where they can negotiate data use in conformity with the Trust’s terms, thus introducing an independent intermediary between data subjects and data collectors.
- Unlike the current ‘one size fits all’ approach to data governance, there should be a plurality of Trusts, allowing data subjects to choose a Trust that reflects their aspirations, and to switch Trusts when needed. Data Trusts may arise out of publicly or privately funded initiatives.
- By potentially facilitating access to ‘pre-authorized’, aggregated data (consent would be negotiated on a collective basis), our data Trust proposal may remove key obstacles to the realization of the potential underlying large datasets.

Introduction

From the friends we make to the foods we like, via our shopping and sleeping habits, most aspects of our quotidian lives can now be turned into machine-readable data points. For those able to turn these data points into models predicting what we will do next, this data can be a source of wealth. For those keen to replace biased, fickle human decisions, this data—sometimes misleadingly—offers the promise of automated, increased accuracy. For those intent on modifying our behaviour, this data can help build a puppeteer’s strings. As we move from one way of framing data governance challenges to another, salient answers change accordingly. Just like the wealth redistribution way of framing those challenges tends to be met with a property-based, ‘it’s *our* data’ answer, when one frames the problem in terms of manipulation potential, dignity-based, human rights answers rightly prevail (via fairness and transparency-based answers to contestability concerns). Positive data-sharing aspirations tend to be raised within altogether different conversations from those aimed at addressing the above concerns. Our data Trusts proposal challenges these boundaries.

This article proceeds from an analysis of the very particular type of vulnerability concomitant with our ‘leaking’ data on a daily basis, to show that data ownership is both unlikely and inadequate as an answer to the problems at stake. We also argue that the current construction of top-down regulatory constraints on contractual freedom is both necessary and insufficient. To address the particular type of vulnerability at stake, bottom-up empowerment structures are needed. The latter aim to ‘give a voice’ to data subjects whose choices when it comes to data governance are often reduced to binary, ill-informed consent. While the rights

A digital social contract

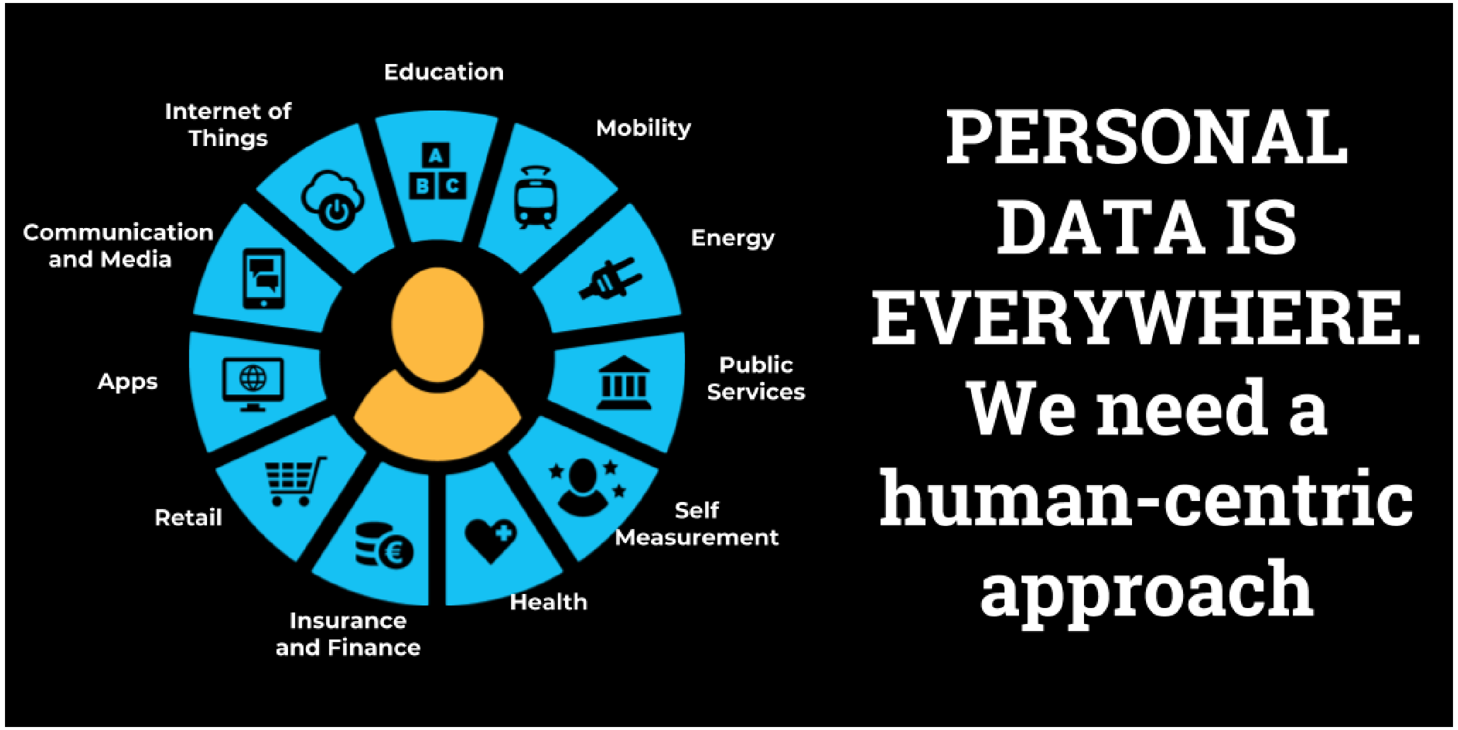
MYDATA GLOBAL

ME2B ALLIANCE

CIVIL SOCIETY

MyData Global

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



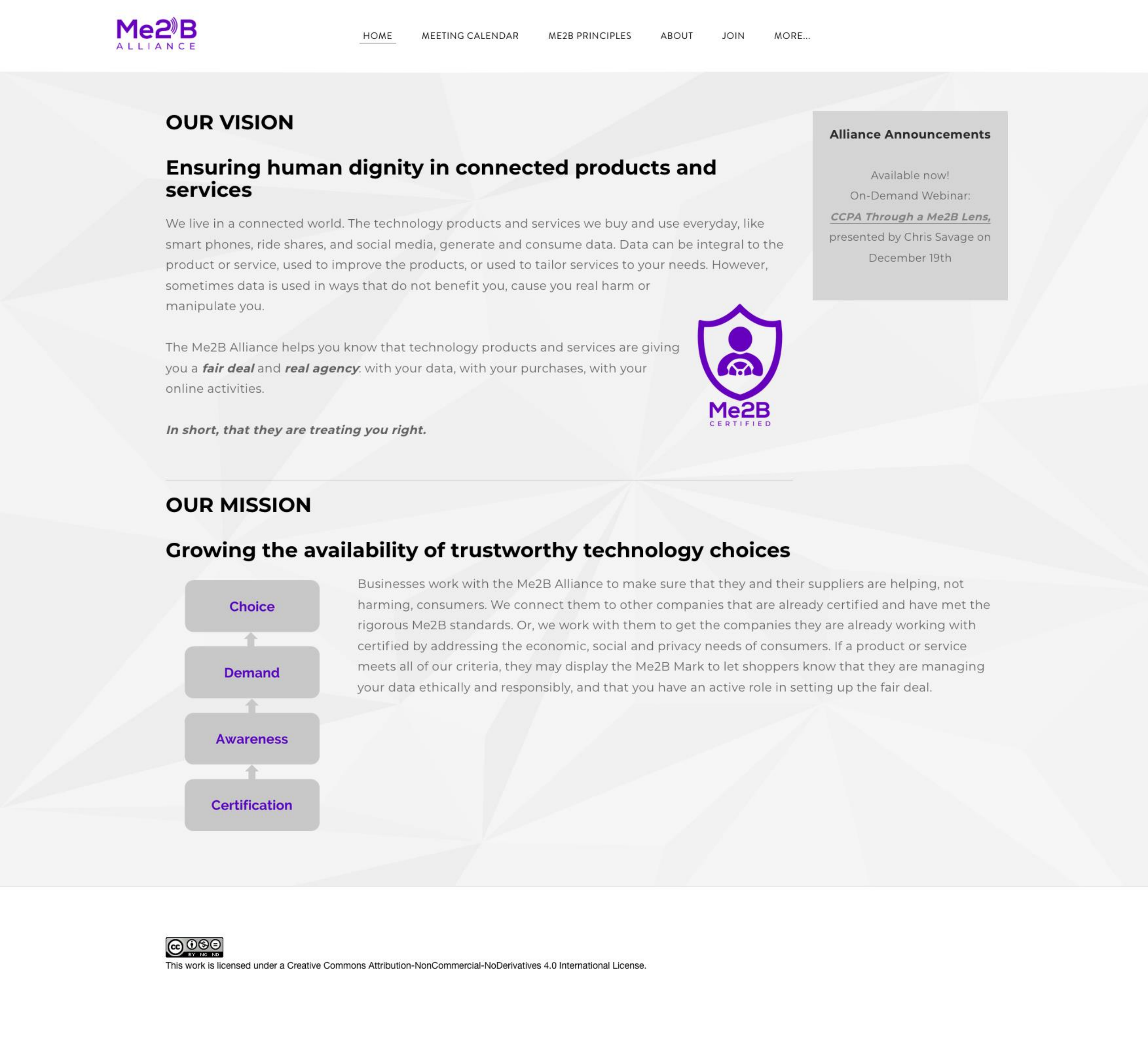
https://mydataglobal.slack.com/signup
https://mydata.org/join/
https://mydata.org/mydata-global-membership-application/organisations/

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.

Alliance Announcements

Available now!
On-Demand Webinar:
CCPA Through a Me2B Lens,
presented by Chris Savage on
December 19th

OUR MISSION

Growing the availability of trustworthy technology choices

Choice ↑ Demand ↑ Awareness ↑ Certification

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

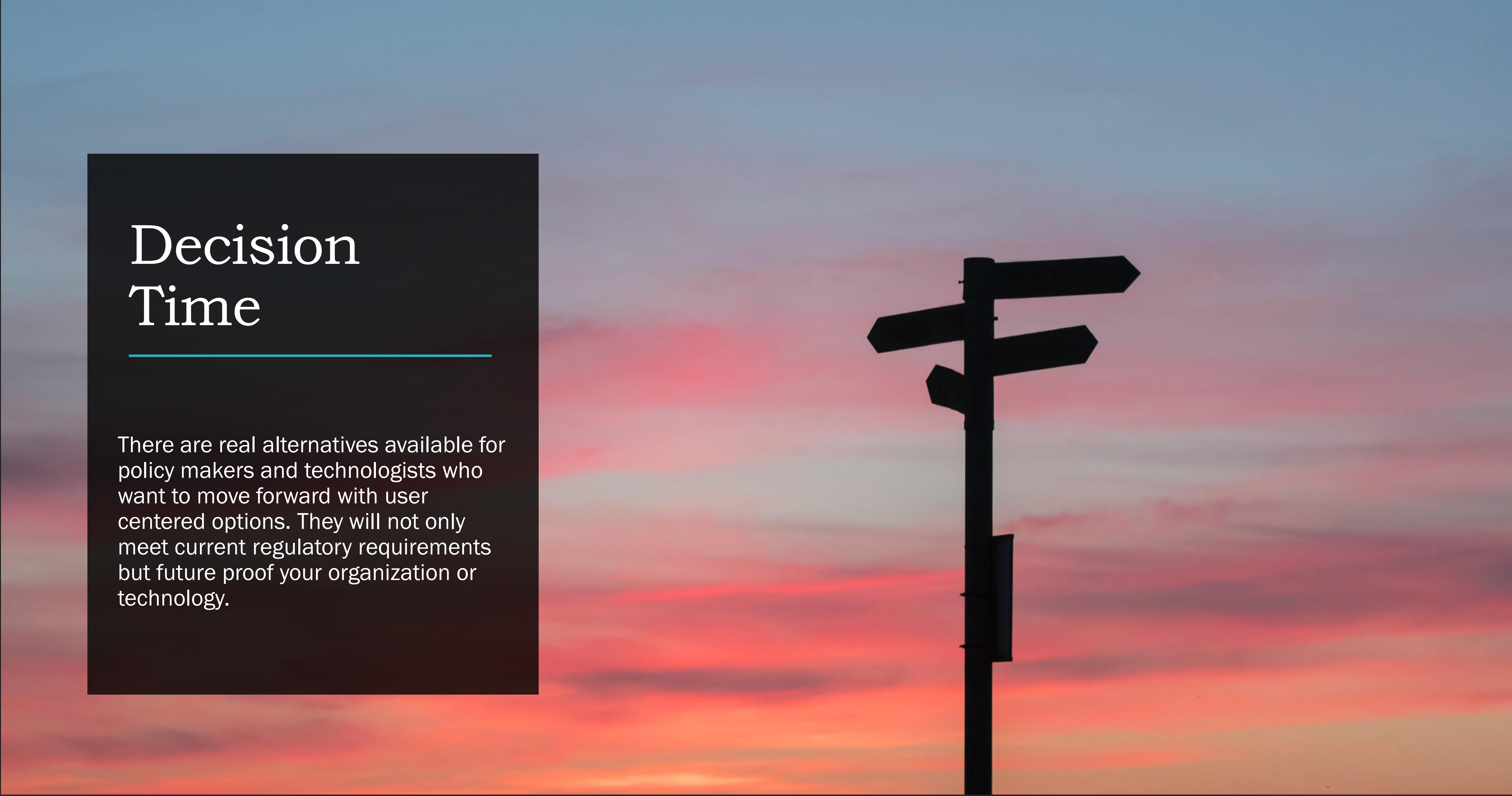
Access Now

CDT

EDRI

EPIC

Privacy International



Decision Time

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.

Photo by Javier Allegue Barros on Unsplash

Thank you

FOR QUESTIONS OR FOLLOW UP: JOHN@WUNDERLICH.CA

Photo by Javier Allegue Barros on Unsplash