Personal Data and Individual Access Control

Autonomous and Intelligent systems (A/IS) are developing faster than the supporting standards and regulation required for transparency and societal protections can keep pace. The impact of these systems on society is direct and considerable.

A/IS require data to fuel learning, and inform automatic decision-making. Increasingly this data is personal data, or personally identifiable information, known as PII. PII is defined as any data that can be reasonably linked to an individual based on their unique physical, digital, or virtual identity. As a result, through every digital transaction (explicit or observed) humans are generating a unique digital shadow of their physical self.

Ethical considerations regarding data are often focused largely on issues of privacy — what rights should a person have to keep certain information to themselves or have input into how it is shared? However, individuals currently lack clarity around how to access, organize, and share their data to ensure unintended consequences are not the Laws are generally enforceable result. Without clarity, these issues will continue to reflect negatively on the proliferation of the A/IS industry.

The aim of this Committee is to set out the ethical considerations in the collection and use of personal data when designing, developing, and/or deploying A/IS. Furthermore, to entreat all global (A/IS) technologists (academics, engineers, programmers, manufacturers, and policy makers) to proactively prioritize and include individuals in the data processes that directly relate to their identity.

There is a fundamental need for people to have the right to define access and provide informed consent with respect to the use of their personal data (as they do in the physical world). Individuals require mechanisms to help curate their unique identity and personal data in conjunction with policies and practices that make them explicitly aware of consequences resulting from the bundling or resale of their personal information and life experiences.

Enabling individuals to curate their identities and manage the ethical implications of their data use will remain essential to human culture everywhere in the world. While some may

Personal Data and Individual Access Control

choose only minimum compliance to legislation like the European General Data Protection Regulation (GDPR), forward-thinking organizations will shift their data strategy (marketing, product, and sales) to enable methods of harnessing volunteered intentions from customers (or in governmental contexts, citizens), versus only invisibly tracking their attention or actions.

For individuals to be at the center of their data, policy makers and society at large will need to rethink the nature of standards and human rights as they have been applied to the physical world and to re-contextualize their application in the digital world. While standards exist, or are in production relating to augmented and virtual reality, human rights law, privacy and data, it is still largely not understood how human agency, emotion, and the legal issues regarding identity will be affected on a large scale by society once A/IS technologies become ubiquitous.

The goal of the analysis of these ethical issues and considerations by this Committee regarding data usage and identity is to foster a positive and inclusive vision for our shared future. To accomplish this goal, this document is focused on the following themes:

1. Digital Personas
2. Regional Jurisdiction
3. Agency and Control
4. Transparency and Access
5. Symmetry and Consent

We have also created an Appendix document listing key resources referenced in the following section.

Personal Data and Individual Access Control

Addressing these issues and establishing safeguards prioritizing the protection and assets of individuals regarding privacy and personal data in the realms of A/IS is of paramount importance today. To that end, since the creation of the first draft of *Ethically Aligned Design* this Committee recommended ideas for the following IEEE Standards Working Groups which have been and approved and are free for all to join (click on links for details):

- IEEE P7002™, Data Privacy Process
- IEEE P7004™, Standard on Child and Student Data Governance
- IEEE P7005™, Standard on Employer Data Governance
- IEEE P7006™, Standard for Personal Data Artificial Intelligence (AI) Agent

The goal of this Committee is that our recommendations, in conjunction with the development and release of these Standards once adopted, will expedite the prioritization and inclusion of all global individuals in the data processes that directly relate to their identity.

Disclaimer: *While we have provided recommendations in this document, it should be understood these do not represent a position or the views of IEEE but the informed opinions of Committee members providing insights designed to provide expert directional guidance regarding A/IS. In no event shall IEEE or IEEE-SA Industry Connections Activity Members be liable for any errors or omissions, direct or otherwise, however caused, arising in any way out of the use of this work, regardless of whether such damage was foreseeable.*

Section 1 — Digital Personas

While many individuals may not currently have the ability to claim their identity (in the case of refugees, etc.), as a rule society understands how to apply the legal concepts of identity in real-life situations. In digital or virtual realms, however, our personas are fluid — individuals can be avatars in gaming situations or take on a different tone in various social networking settings. Behaviors regarding our personas considered normal in real-life are not directly applicable in the augmented, virtual and mixed reality worlds most individuals will soon be inhabiting on a regular basis in the near future. In regards to the algorithms powering AI, or the affective sensors becoming standard features in autonomous vehicles, or companion robots, etc., how A/IS affects our digital personas through use or misuse of our data is critical to understand, monitor, and control.

Issue:

Individuals do not understand that their digital personas and identity function differently than in real life. This is a concern when personal data is not accessible by an individual and the future iterations of their personas or identity cannot be controlled by them, but by the creators of the A/IS they use.

Background

A/IS created from personal experiences is different from AI created from farming or climate data. Society has had traditional safeguards on the use and application of personal information to encourage innovation and to protect minorities. Traditional systems for medicine and law limit secrecy and favor regulation of professionals at the edges over centralized hierarchical corporations. For example, almost 100% of intellectual property in the domains of medicine and law is open, peer-reviewable, and can be taught to anyone, anywhere.

Personal Data and Individual Access Control

However, the emergence of the Internet of Things (IoT) and augmented reality/virtual reality (AR/VR) means personal information forms a foundation for every system being designed. This data acts as the digital representation and proxy for our identity. From birth, the different roles individuals take on in life provide specific contexts to the data they generate. Previously these contexts and roles enabled individuals to maintain some level of privacy due to the siloes of collection. Now, as the prospect of an omni-connected world approaches, those silos are being replaced by horizontal integrations that put the digital versions of personas and roles at risk. It is therefore important that citizens understand these roles and their related data to assess the downstream (further) consequences of its aggregation. Digital personas/roles include:

- Pre-birth to post-life digital records (health data)
- Birth and the right to claim citizenship (government data)
- Enrollment in school (education data)
- Travel and services (transport data)
- Cross-border access and visas (immigration data)
- Consumption of goods and services (consumer and loyalty data)
- Connected devices, IoT and wearables (telecommunications data)
- Social and news networks (media and content data)
- Professional training, internship, and work (tax and employment data)
- Societal participation (online forums, voting and party affiliation data)
- Contracts, assets, and accidents (insurance and legal data)
- Financial participation (banking and finance data)
- Death (digital inheritance data)

By the time individuals reach early adulthood, they are simultaneously acting across these roles, generating vast amounts of personal data that is highly contextual and easy to identify and link directly to an individual. If an individual's digital shadow is a proxy of their physical self, then technologists and policy makers must address the transparency, control, and asymmetry of how personal data is collected and used to enable A/IS. A/IS technologists need to recognize the coercive nature of many current identity schemes — such as hidden tracking by advertising brokers — and adopt privacy-preserving identity practices such as same-domain pseudonymous identifiers and self-sovereign identity.

Candidate Recommendation

The ethics of creating secret and proprietary A/IS from people's personally identifiable information (PII) need to be considered based on the potential impact to the human condition. To preserve human dignity, policies, protections, and practices must provide all individuals the same agency and control over their digital

Personal Data and Individual Access Control

personas and identity they exercise in their real-world iterations no matter what A/IS may be in place to monitor, assist, or interact with their data.

Further Resources

- Blockchain Identity (Rebooting Web-of-Trust).
- W3C Credentials Community Group.
- HIE of One.

Issue:

How can an individual define and organize his/her personal data and identity in the algorithmic era?

Background

Identity is emerging at the forefront of the risks and opportunities related to use of personal data for A/IS. Across the identity landscape there is increasing tension between the requirement for federated identities (all data linked to a natural and identified natural person) versus a range of identities (personas) that are context specific and determined by the use-case, for example opening a bank account, crossing a border, or ordering a product online. New movements, such as Self-Sovereign Identity — defined as the right of a person to determine his or her own identity — are emerging alongside legal identities (issued by governments, banks, and regulatory authorities) to help put individuals at the center of their data in the algorithmic age.

Personas (an identity that acts as a proxy) and pseudonymity are also critical requirements for privacy management since they help individuals select an identity that is appropriate for the context they are in or wish to join. In these settings, trust transactions can still be enabled without giving up the "root" identity of the user. For example, it is possible to validate a user is over 18 (for adult content) or eligible for a service (postcode confirmation). Attribute verification (comprising the use of empowered persona usage by an individual) will play a significant role in enabling individuals to select the identity that provides access without compromising agency. This type of access is especially important in dealing with the myriad algorithms interacting with data representing tiny representations of our identity where individuals typically are not aware of the context for how their data will be used.

Candidate Recommendation

Individuals should have access to trusted identity verification services to validate, prove, and support the context-specific use of their identity. Regulated industries and sectors such as banking, government, and telecommunications should provide data-verification services to citizens and consumers to provide greatest usage and control for individuals.

Personal Data and Individual Access Control

Further Resources

- The Inevitable Rise of Self-Sovereign Identity by The Sovrin Foundation.
- See Identity Examples in the Appendix Document for this section.
- IEEE P7006™, Standard for Personal Data Artificial Intelligence (AI) Agent Working Group. This Standards Working Group is free and open to anyone wishing to join and addresses issues relating to how an individual could have the ubiquitous and always-on services of a personalized AI agent to ensure their identity is protected and has symmetry with the A/IS their data comes into contact with at all times.

Section 2 — Regional Jurisdiction

Legislation regarding personal data varies widely around the world. Beyond issues of data operability issues when transferring between country jurisdictions, rights of individuals and their access and usage of data depends on the regions and laws where they live. Much of A/IS ethics involves the need to understand cultural aspects of the systems and services an organization wishes to create for specific users. This same attention must be given to how data related to A/IS are positioned from a regional perspective to best honor the use, or potential abuse of the global citizens' data. A/IS will also be subject to regional regulation, for example under the General Data Protection Regulation (GDPR), European citizens may have specific rights of redress where AI or AS has been used.

Issue:

Country-wide, regional, or local legislation may contradict an individual's values or access and control of their personal data.

Background

Ethical considerations regarding data are often focused largely on issues of privacy — what rights should a person have to keep certain information to themselves, or have input into how it is shared? While rhetoric in various circles stating, "privacy is dead" may be someone's personal opinion reflecting their values, privacy is nonetheless a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties.

However, this fundamental right is not universally recognized or supported. It is also culturally contextual and nuanced. It is therefore critical to understand the jurisdictional and specific legal requirements that govern the access and use of personal information when developing A/IS solutions. *These include, but are not limited to:*

- **Europe**; the introduction of the General Data Protection Regulation (GDPR), Personal Services Directive II (PSD2), and ePrivacy. These new regulations carry substantial fines for non-compliance. Depending on the nature and circumstances of the violation, these penalties may include:
  - A warning in writing in cases of first and non-intentional non-compliance
  - Regular periodic data protection audits

Personal Data and Individual Access Control

  - A fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4)
  - A fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 5 and 6)

- **United States**: The United States lacks a single "baseline" privacy regime; instead, policies and procedures affecting the collection and use of PII varies based on type of information and which entity possesses the data. Laws, for example, afford certain procedural requirements around financial data, certain protected health information, and children's data. Laws are generally enforceable by state and federal regulators (including the Federal Trade Commission and state attorney general), though individuals may have private rights of action under state law or certain federal laws such as the Video Privacy Protection Act, which governs disclosures of identifiable video rental records, and the Fair Credit Reporting Act, which provides access and rights to consumer reports used for eligibility determinations. See also: Jurisdiction Examples in the Appendix Document for this section.
- **Australia**: In addition to strict privacy regulation, the Australian Productivity Commission issued reports in 2016 and 2017 acknowledging that personal information is a personal asset and therefore recognized the need for Australians to have control with respect to its collection and use. At the time of publication, The Australian Federal Government is in the process of using these reports to inform the drafting of new personal data regulation.
- **Japan**: The Act on the Protection of Personal Information was amended in 2016. The act precisely defines the definition of personal information; however, the concept of privacy is not explicitly stated. In this sense, the act is deemed as a practice-oriented law. The new concept of *anonymously processed information* is introduced which is produced to make it impossible to identify a specific individual. In addition, it can be transferred to, and used by, the third parties without the data subject's consent. The method of producing anonymously processed information will be determined on a sector-by-sector basis because each sector has distinct constraints and purposes of personal information.

Additionally, there is growing evidence that not providing clear consent (regarding personal data usage) decreases mental and emotional well-being. The rapid rise in ad blocking tools or lowering of consumer trust via reports of non-ethically driven online studies provides tangible evidence toward the failure of these clandestine efforts.

Personal Data and Individual Access Control

Candidate Recommendation

While specific uses of data must be taken in context of the regions where specific legislation applies, individuals should always be provided access to, and control of, their data to ensure their fundamental human rights are honored without fear of the risk of breaking applicable laws.

Further Resources

- Amended Act on the Protection of Personal Information in Japan.
- Outline of the Amended Personal Information Protection Act in Japan.

Section 3 — Agency and Control

Agency is the capacity of individuals to act independently and to exercise free choice, a quality fundamental to democratic ideals. Central to human agency is control. As society moves towards complete connectivity, humans will require tools and mechanisms to enable agency and control over how their personal data is collected and used. When people do not have agency over their identities political participation is impossible, and without political participation ethics will be decided by others. As the rise of algorithms accessing people's data relating to their identities continues, there is increased risk of loss of agency and well-being, adding the potential for depression and confusion along with the lack of clear ways to contribute ideas in an open and democratic fashion.

Issue:

To understand the role of agency and control within A/IS, it is critical to have a definition and scope of personally identifiable information (PII).

Background

Different laws and regulations around the globe define the scope of PII differently. The use of data analytics to derive new inferences and insights into both personal data and technical metadata raises new questions about what types of information should be considered PII. This is further complicated by machine learning and autonomous systems that access and process data faster than ever before.

Multiple global bodies believe PII is a sovereign asset belonging to an identified individual. PII, or personal data, is defined as any data that can be reasonably linked to an individual based on their unique physical, digital, or virtual identity. PII protections are often related to the U.S. Fourth Amendment, as the right of the people to be secure in their persons, houses, papers, and effects.

As further clarification, the European Union definition of personal data set forth in the Data Protection Directive 95/46/ECl vi, defines personal data as "any information relating to an identified or identifiable natural person." Identifiable when? The question asked today will have a very different answer tomorrow given that all A/IS person-level or device-level data is identifiable if the tech advances and the data is still available. Agency requires that the control be exercised by the subject at the time the data is used, not at the time the data is collected.

Personal Data and Individual Access Control

Overall, personal data reflects self-determination and the inalienable right for an individual to be able to access and control the attributes of their physical, digital, and virtual identity.

Candidate Recommendation

Individuals should have access to means that allow them to exercise control over use of personal data at the time the data is used. If that agency and control is not available, person-level data needs to either be aggregated into larger cohorts and the person-level data deleted. PII should be defined as the sovereign asset of the individual to be legally protected and prioritized universally in global, local, and digital implementations regardless of whether deemed to be de-identified in the way it is stored.

Further Resources

- Determining What Is Personal Data, U.K. Information Commissioner's Office.
- Electronic Communications Privacy Act.
- Open PDS.
- IEEE Digital Inclusion through Trust and Agency Industry Connection Program.
- HIE of One — a patient-owned and controlled standards-based, open source EHR, so patients can collect, aggregate, and share their own data.

Issue:

What is the definition of control regarding personal data, and how can it be meaningfully expressed?

Background

Most individuals believe controlling their personal data only happens on the sites or social networks to which they belong, and have no idea of the consequences of how that data may be used by others tomorrow. Providing individuals with tools, like a personal data cloud, can empower users to understand how their data is an asset as well as how much data they produce. Tools like personal data vaults or clouds also let individuals organize their data around various uses (medical, social, banking). Control enables individuals to also assert a version of their own terms and conditions.

In the current context of A/IS technologies, and in the complex and multi-level or secondary uses of data, it is important to be clear about the boundaries of control for use of personal data that can affect an individual directly compared to collection of data for aggregated or systematic work (and exceptions for approved research). For example, an individual subway user's travel card, tracking their individual movements, should be protected from uses that identify or profile that individual to make inferences about his/her likes or location generally, but could be included in the overall travel systems management to

Personal Data and Individual Access Control

aggregate user data into patterns for scheduling and maintenance as long as the individual-level data is deleted.

The MyData movement combines related initiatives, such as Self Data, Vendor Relationship Management, Internet of Me, and Personal Information Management Systems (PIMS) under a common cause to empower individuals with their personal data. The Declaration of MyData Principles highlights human-centric control of personal data as one of core principles, emphasizing that people should be provided with the practical means to understand and effectively control who has access to data about them and how it is used and shared. In detail, the MyData Declaration states: "We want privacy, data security and data minimization to become standard practice in the design of applications. We want organizations to enable individuals to understand privacy policies and how to activate them. We want individuals to be empowered to give, deny or revoke their consent to share data based on a clear understanding of why, how and for how long their data will be used. Ultimately, we want the terms and conditions for using personal data to become negotiable in a fair way between individuals and organizations."

Candidate Recommendation

Personal data access and consent should be managed by the individual using systems that provide notification and an opportunity for consent at the time the data is used, versus outside actors being able to access personal data outside of an individual's awareness or control.

Further Resources

- Project VRM — vendor relationship management (VRM) tools and frameworks.
    - Kuan Hon, W. K., C. Millard, and I. Walden. "The Problem of 'Personal Data' in Cloud Computing — What Information Is Regulated? Cloud of Unknowing, Part 1." *Queen Mary School of Law Legal Studies Research Paper No. 75/2011; International Data Privacy Law* 1, no. 4 (2011): 211–228.
    - Boyd, E. B. "Personal.com Creates an Online Vault to Manage All Your Data." *Fast Company*, May 7, 2012._
- Meeco Life Management Platform. Personal cloud, attribute wallet and personal data management tools, consent engine and dual sided permission APIs.
    - MyData2017. Declaration of MyData Principles.
- Poikola, A. K. Kuikkaniemi, and H. Honko (Ministry of Transport and Communications). MyData — A Nordic Model for Human-Centered Personal Data Management and Processing. Finland: Prime Minister's Office, 2014.
- Hasselbalch, G., and P. Tranberg. "Personal Data Stores" (chapter 12), in Data Ethics: *The New Competitive Advantage*. Publishare, 2016.
- GDPR Article 20, Right to Data Portability, Article 29 Working Party, Brussels, 2016.

Personal Data and Individual Access Control

- Thurston, B. "A Radical Proposal for Putting People in Charge of Their Data." *Fast Company*, May 11, 2015.
- de Montjoye, Y.-A., Wang, S. S., and Pentland, A. S. "openPDS: Protecting the Privacy of Metadata through SafeAnswers." *PLoS ONE* 9, no. 7 (2014): e98790.
- Definition of the *right* to be forgotten.
- IEEE Digital Inclusion through Trust and Agency. The Industry Connection Program develops comprehensive roadmaps, industry action reports, and educational platforms working to address issues around cyber-identity, digital personas, distributed ledger technology, and inclusion of underserved and vulnerable.
- See "The Attribute Economy 2.0," a multi-authored paper published by Meeco.
- The Path to Self-Sovereign Identity.
- uPort is an open source software project to establish a global, unified, sovereign identity system for people, businesses, organizations, devices, and bots. The Ethereum based self-sovereign identity system now in alpha testing.
- Sovrin—identity for all. The Sovrin Foundation describes self-sovereign identity (SSI) as "...an identity that is 100% owned and controlled by an individual or organization. No one else can read it, use it, turn it off, or take it away without its owner's explicit consent."
- Nichol, P. B. "A Look at India's Biometric ID System: Digital APIs for a Connected World." *CIO Perspectives*, February 23, 2017.
- See also Appendix 3: Digital Divide and Pay for Privacy.
- See also Appendix 4: Examples of Agency and Transparency.
- See also Appendix 5: Can Personal Data Remain Anonymous?

Section 4 — Transparency and Access

Much of the contention associated with the concept of "privacy" actually relates to access. Challenges often arise around transparency and providing an explicit understanding of the consequences of agreeing to the use of people's personal data. This is complicated by the data-handling processes behind true "consent." Privacy rights are often not respected in the design and business model of services using said data. They obscure disclosure of the ways the data is used and make it hard to know what data was used. This can be especially evident via the invisible algorithms representing multiple services that access people's data long after they've provided original access to a service or their partners.

If individuals cannot access their personal data and account for how it is used, they cannot benefit from the insights that the data could provide. Barriers to access would also mean that individuals would not be able to correct erroneous information or provide the most relevant information regarding their lives to trusted actors. Transparency is also about notification. It is important that an individual is notified when their data is collected, and what usage is intended. In accordance with the GDPR, consent must be informed, explicit, and unambiguous.

Issue:

It is often difficult for users to determine what information a service provider or A/IS application collects about them at the time of such aggregation/collection (at the time of installation, during usage, even when not in use, after deletion). It is difficult for users to correct, amend, or manage this information.

Candidate Recommendation

Service providers should ensure that personal data management tools are easy to find and use within their service interface. *Specifically:*

- The data management tools should make it clear who has access to a user's data and for what purpose, and (where relevant) allow the user to manage access permissions.
- There should be legal, reputational, and financial consequences for failing to adhere to consent terms.
- It should be easy for users to remove their

Personal Data and Individual Access Control

data from the service. (Note: This is a GDPR requirement. It may not be mandated in the United States or for other services in countries outside of the EU, but represents a best-in-class practice to follow.) Organizations should create open APIs to their data services so that customers can access their data and governments should share the data they collect about their users directly with individuals and encourage them to ensure its accuracy for mutual value to combat the rising issue of dirty data.

Further Resources

- The User Managed Access Standard, proposed by The Kantara Initiative, provides a useful model to address these types of use cases.
- Surveys about how adults feel about health IT in 2005 and 2016 show that distrust of health technology has grown from 13% that withheld data from providers due to mistrust to 89%.

Issue:

How do we create privacy impact assessments related to A/IS?

Background

Because the ethical implications of intelligent systems are so difficult to discern, interested parties would benefit from analytical tools to implement standards and guidelines related to A/IS and privacy impacts. Like an environmental impact study or the GDPR privacy impact assessments, A/IS impact assessments would provide organizations with tools to certify their products and services are safe and consistent for the general public.

Candidate Recommendation

A system to assess privacy impacts related to A/IS needs to be developed, along with best practice recommendations, especially as automated decision systems spread into industries that are not traditionally data-rich.

Further Resources

In the GDPR in the EU, there is a requirement for a privacy impact assessment. The full report created by PIAF, The Privacy Impact Assessment Framework can be found here. In the report, of interest is Section 10.3, "Best Elements" whose specific recommendations provide insights into what could be emulated to create an AI impact assessment, including:

- PIA guidance documents should be aimed at not only government agencies but also companies or any organization initiating or intending to change a project, product, service, program, policy, or other initiative that could have impacts on privacy.

Personal Data and Individual Access Control

- PIAs should be undertaken about any project, product, service, program, or other initiative, including legislation and policy, which are explicitly referenced in the Victoria Guide and the UK Information Commissioner's Office (ICO) Handbook.

Information privacy is only one type of privacy. A PIA should also address other types of privacy, e.g., of the person, of personal behavior, of personal communications, and of location.

- PIAF Consortium. "PIAF: A Privacy Impact Assessment Framework for Data Protection and Privacy Rights," 2011. Section 10.3.
- See the Personalized Privacy Assistant for a project applying these principles.
- While not explicitly focused on PIAs or AI, IEEE P7002™ Data Privacy Process is a Standards Working Group still open to join focused on these larger issues of data protection required by the enterprise for individuals' data usage.
- Usable Privacy Policy project for examples of how difficult privacy policies can be to maneuver.
- See also Appendix 4: Examples of Agency and Transparency.

Issue:

How can AI interact with government authorities to facilitate law enforcement and intelligence collection while respecting rule of law and transparency for users?

Background

Government mass surveillance has been a major issue since allegations of collaboration between technology firms and signals intelligence agencies such as the U.S. National Security Agency and the U.K. Government Communications Headquarters were revealed. Further attempts to acquire personal data by law enforcement agencies, such as the U.S. Federal Bureau of Investigation, have disturbed settled legal principles regarding search and seizure. A major source of the problem concerns the current framework of data collection and storage, which puts corporate organizations in custody of personal data and detached from the generators of that information. Further complicating this concern is the legitimate interest that security services have in trying to deter and defeat criminal and national security threats.

Candidate Recommendations

Personal privacy A/IS tools such as IEEE P7006™ have the potential to change the data paradigm and put the generators of personal information

Personal Data and Individual Access Control

at the center of collection. This would re-define the security services' investigative methods to pre-Internet approaches wherein individuals would be able to control their information while providing custody to corporate entities under defined and transparent policies.

Such a construct would mirror pre-Internet methods of information management in which individuals would deposit information in narrow circumstances such as banking, healthcare, or in transactions. This personal data AI agent would include root-level settings that would automatically provide data to authorities after they have satisfied sufficiently specific warrants, subpoenas, or other court-issued orders, unless authority has been vested in other agencies by local or national law. Further, since corporately held information would be used under the negotiated terms that the A/IS agent facilitates, authorities would not have access unless legal exceptions were satisfied. This would force authorities to avoid mass collection in favor of particularized efforts:

- The roots of the personal privacy A/IS should be devoid of backdoors that allow intrusion under methods outside of transparent legal authority. Otherwise, a personal A/IS could feed information to a government authority without proper privacy protection.
- Nuanced technical and legal techniques to extract warranted information while segregating and avoiding other information will be crucial to prevent overreach.
- Each request for data acquisition must come on a case-by-case basis versus an ongoing access form of access, unless the ongoing access has become law.
- Data-acquisition practices need to factor in the potential status of purely virtual representations of a citizen's identity, whether they do not have formal country of origin (physical) status, or their virtual identity represents a legal form of identity.
- Phasing in personal privacy AIs will mitigate risks while pre-empting reactive and disruptive legislation.
- Legal jurisdiction over personal privacy A/IS access will need to be clarified.

Further Resources

- UNECE. "Evaluating the Potential of Differential Privacy Mechanisms for Census Data." *Work Session on Statistical Data Confidentiality 2013*. Ottawa, October 28, 2013.
- CASD — Le Centre D'Accès Sécurisé Aux Données (The Secure Data Access Centre) is equipment that allows users, researchers, data scientists, and consultants to access and work with individual and highly detailed microdata, which are therefore subject to confidentiality measures, in the most secure conditions.
- Initiatives such as OPAL (for Open Algorithms), a collaborative project being developed by a group of partners committed

Personal Data and Individual Access Control

to leveraging the power of platforms, big data, and advanced analytics for the public good in a privacy-preserving, commercially sensible, stable, scalable, and sustainable manner.

- Ohm, P. "Sensitive Information." *Southern California Law Review* 88 (2015): 1125–1196.
- Y.-A. de Montjoye, L. Radaelli, V. K. Singh, A. S. Pentland. "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata." *Science* 347 (2015): 536–539.
- Sanchez, D., S. Martinez., and J. Domingo-Ferrer. "Comment on 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata'." Science 351, no. 6279 (2016): 1274–1274.
- Polonetsky, J., and O. Tene. "Shades of Gray: Seeing the Full Spectrum of Practical De-Identification." *Santa Clara Law Review* 56, no. 3 (2016): 593–629.
- Narayanan, A., and V. Shmatikov, "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)." February 5, 2008.
- de Montjoye, Y.-A., C. A. Hidalgo, M. Verleysen, and V. D. Blondel. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* 3, no. 1376 (2013). doi: 10.1038/srep01376
- Coyne, A. "Government Pulls Dataset That Jeopardised 96,000 Employees." *iTnews*, October 6, 2016.
- Cowan, P. "Health Pulls Medicare Dataset After Breach of Doctor Details." *iTnews*, September 29, 2016.

Section 5 — Symmetry and Consent

Widespread data collection followed by the emergence of A/IS and other automated/autonomous data processing has placed tremendous strain on existing conceptions of "informed consent." This has created a vast asymmetry between the volume of organizations tracking individuals versus the tools allowing those individuals to fully understand and respond to all these tracking signals.

Legal frameworks such as the GDPR rely on the notion that data subjects must provide "freely given, specific, informed, and unambiguous" consent to certain data processing. Heavy reliance on a system of "notice and choice" has shifted the burden of data protection away from data processors and onto individual data subjects. A/IS can exacerbate this trend by complicating risk assessments of data sharing. When A/IS data transfer is done incorrectly it may alter or eliminate user interfaces, limiting choice and consent.

A/IS presents a new opportunity to offer individuals/end users a "real choice" with respect to how information concerning them is collected, used, and shared. Researchers are working to solve this issue in some contexts, but design standards and business incentives have yet to emerge.

Issue:

Could a person have a personalized privacy AI or algorithmic agent or guardian?

Background

For individuals to achieve and retain parity regarding their personal information in the algorithmic age, it will be necessary to include a proactive algorithmic tool that acts as their agent or guardian in the digital, and "real" world. ("Real" meaning a physical or public space where the user is not aware of being under surveillance by facial recognition, biometric, or other tools that could track, store, and utilize their data without pre-established consent or permission). The creation of personalized privacy A/IS would provide a massive opportunity for innovation in A/IS and corporate communities. There is natural concern that the rights of the individual are protected in the face of such opportunities.

The sophistication of data-sharing methodologies has evolved so these scenarios could evolve from an "either/or" relationship: "We get all of your data for this project, or you provide nothing and hinder this work") to a "Yes and" relationship — by allowing individuals to set their preferences for sharing and storing their data. An additional

Personal Data and Individual Access Control

benefit of finer-grained control of consent is that individuals are more likely to trust the organizations conducting research and provide more access to their data.

The guardian could serve as an educator and negotiator on behalf of its user by suggesting how requested data could be combined with other data that has already been provided, inform the user if data is being used in a way that was not authorized, or make recommendations to the user based on a personal profile. As a negotiator, the guardian could negotiate conditions for sharing data and could include payment to the user as a term, or even retract consent for the use of data previously authorized, for instance if a breach of conditions was detected.

Nonetheless, the dominant paradigm for personal data models needs to shift away from system and service-based models not under the control of the individual/human, and toward a model focused on the individual. Personal data cannot be controlled or understood when fragmented and controlled by a myriad of entities in legal jurisdictions across the world. The object model for personal data should be associated with that person, and under the control of that person utilizing a personalized privacy A/IS or algorithmic guardian.

During the handshake/negotiation between the personal agent and the system or service, the personal agent would decide what data to make available and under what terms, and the system would decide whether to make the service available, and at what level. If the required data set contains elements the personal agent will not provide, the service may be unavailable. If the recommended data set will not be provided, the service may be degraded. A user should be able to override his/her personal agents should he/she decide that the service offered is worth the conditions imposed.

Vulnerable parts of the population will need protection in the process of granting access, especially given the asymmetry of power between an individual and entities.

Candidate Recommendations

Algorithmic guardian platforms should be developed for individuals to curate and share their personal data. Specifically:

1. Such guardians could provide personal information control to users by helping them track what they have agreed to share and what that means to them, while also scanning each user's environment to set personal privacy settings accordingly.

2. For purposes of privacy, a person must be able to set up complex permissions that reflect a variety of wishes.

3. Default profiles, to protect naive or uninformed users, should provide little or no personal information without explicit action by the personal agent's owner.

4. The agent should help a person foresee and mitigate potential ethical implications of specific machine learning data exchanges.

Personal Data and Individual Access Control

5. Control of the data from the agent should vest with the user, as otherwise users could lose access to his/her own ethical choices, and see those shared with third parties without permission.

6. A guardian should enable machine-to-machine processing of information to compare, recommend, and assess offers and services.

7. Institutional systems should ensure support and respect the ability for individuals to bring their own guardian to the relationship without any constraints that would make some guardians inherently incompatible or subject to censorship.

Further Resources

- The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Personal Data and Individual Access Control Section, in *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Artificial Intelligence and Autonomous Systems*, Version 1. IEEE, 2016.
- IEEE P7006™, Standard for Personal Data Artificial Intelligence (AI) Agent was launched in the summer of 2017 and is currently in development. Readers of this section are encouraged to join the Working Group if they are focused on these issues.
- We wish to acknowledge Jarno M. Koponen's articles on Algorithmic Angels that provided inspiration for portions of these ideas.
- Companies are already providing solutions for early or partial versions of algorithmic guardians. Anonyome Labs recently announced their SudoApp that leverages strong anonymity and avatar identities to allow users to call, message, email, shop, and pay — safely, securely, and privately.
- Tools allowing an individual to create a form of an algorithmic guardian are often labeled as PIMS, or personal information management services. Nesta in the United Kingdom was one of the funders of early research about PIMS conducted by CtrlShift.
- Privacy Assistant from MIT.

Issue:

Consent is vital to information exchange and innovation in the algorithmic age. How can we redefine consent regarding personal data so it respects individual autonomy and dignity?

Background

Researchers have long identified some key problems with notice and consent in the digital world. First, individuals cannot and will not read all of the privacy policies and data use statements to which they are exposed, and even if they could, these policies are not easy to understand.

Personal Data and Individual Access Control

Individual consent is rarely exercised as a meaningful choice due to poorly provisioned user-appropriate design.

A/IS place further strain on the notice and consent regime as further personalization of services and products should not be used as an excuse to minimize organizational transparency and choice for individuals to meet ethical and regulatory demand. If individuals opt not to provide personal information, they may find themselves losing access to services or receiving services based on stereotypes derived from the lower quality of data that they do provide.

When consent is not feasible or appropriate, organizations should engage in a robust audit process to account for processing of personal data against the interests of individuals. For instance, the GDPR permits processing on the grounds of an entity's legitimate interests, so long as those interests do not outweigh the fundamental rights and interests of data subjects. Organizations must develop internal procedures for conducting such an analysis, and external actors and regulators should provide further guidance and oversight where possible.

The needs of local communities, greater society, and public good should factor into this process. For example, a doctor may need medical data to be identified in order to treat a patient. However, a researcher may require it simply for statistical analysis, and therefore does not require the data to be identifiable. This is particularly important where the primary reason for data collection may mask important secondary uses post-collection. In time, however, new mechanisms for facilitating dynamic consent rules and core structure as use-cases change. As data moves from the original collection context to a change of context, agile ethics rules should be deployed.

Candidate Recommendations

The asymmetric power of institutions (including public interest) over individuals should not force use of personal data when alternatives such as personal guardians, personal agents, law-enforcement-restricted registries, and other designs that are not dependent on loss of agency are available. When loss of agency is required by technical expedience, transparency needs to be stressed in order to mitigate these asymmetric power relationships.

Further Resources

- Office of the Privacy Commissioner of Canada. "Consultation on Consent Under the 'Personal Information Protection and Electronic Documents Act'." September 21, 2017. U.K. Information Commissioner's Office. "Consultation: GDPR Consent Guidance." March 2017.
- United Nations. "United Nations Declaration on the Rights of Indigenous Peoples." 107th plenary meeting, September 13, 2007.

Personal Data and Individual Access Control

Issue:

Data that is shared easily or haphazardly via A/IS can be used to make inferences that an individual may not wish to share.

Background

It is common for a consumer to consent to the sharing of discrete, apparently meaningless data points like credit card transaction data, answers to test questions, or how many steps they walk. However, once aggregated these data and their associated insights may lead to complex and sensitive conclusions being drawn about individuals that consumers would not have consented to sharing. As analysis becomes more obfuscated via A/IS, not even data controllers will necessarily know what or how conclusions are being drawn through the processing of personal data, or how those data are used in the whole process.

Opting out has some consequences. Users need to understand alternatives to consent to data collection before they give or withhold it, as meaningful consent. Without understanding the choices, consent cannot be valid. This places further strain on existing notions of informed consent. It raises the need for additional user controls and information access requirements. As computational power advances and algorithms compound existing data, information that was thought to be private or benign can be linked to individuals at a later time. Furthermore, this linked data may then be used to train algorithms, without transparency or consent, setting in motion unintended consequences. Auditing data use and collection for potential ethics risks will become increasingly more complex with A/IS in relation to these issues in the future.

Candidate Recommendation

The same A/IS that parses and analyzes data should also help individuals understand how personal information can be used. A/IS can prove granular-level consent in real time. Specific information must be provided at or near the point (or time) of initial data collection to provide individuals with the knowledge to gauge potential privacy risks in the long-term. Data controllers, platform operators, and system designers must monitor for consequences when the user has direct contact with an A/IS system. Positive, negative, and unpredictable impacts of accessing and collecting data should be made explicitly known to an individual to provide meaningful consent ahead of collection. Specifically:

- Terms should be presented in a way that allows the user to easily read, interpret, understand, and choose to engage with the system. To guard against these types of complexities, consent should be both conditional and dynamic. The downstream consequences (positive and negative) must be explicitly called out, such that the individual can make an informed choice, and/or assess the balance of value in context.

Personal Data and Individual Access Control

- If a system impacts the ability of consumers to manage their own data via A/IS, accountability program management (PM) could be deployed to share consent solutions. A PM could span a diversity of tools and software applications to collect and transfer personal data. A PM can be assigned to evaluate consent metrics by ethics leadership to provide accountability reports. An actionable consent framework for personal data would not need to "reinvent the wheel." Existing privacy and personal data metrics and frameworks can be integrated into consent program management, as it becomes relevant. Likewise, resources, user controls, and policies should be put in place to afford individuals the opportunity to retract or erase their data if they feel it is being used in ways they do not understand or desire. Use limitations are also important and may be more feasible than collection limitations. At a minimum, organizations should commit to not use data to make sensitive inferences or to make important eligibility determinations absent consent. Because consent is so challenging in A/IS, it is vital that user participation, including data access, erasure, and portability, are also incorporated into ethical designs.
- Moving all computational values to the periphery (on the person) seems to be the only way to combat all the risks articulated. Systems should be designed to enable personalization and meta system learning concurrently without the permanent collection and storage of personal data for retargeting. This is a key architectural design challenge that A/IS designers must achieve if AI is going to be of service to society.

Further Resources

- Duhigg, C. "How Companies Learn Your Secrets." *The New York Times Magazine*, February 19, 2012.
- Meyer, R. "When You Fall in Love, This Is What Facebook Sees." The Atlantic, February 15, 2014.
- Cormode, G. "The Confounding Problem of Private Data Release." 18th International Conference on Database Theory (2015): 1–12.
- Felbo, B., P. Sundsøy, A. Pentland, S. Lehmann, and Y. de Montjoye. "Using Deep Learning to Predict Demographics from Mobile Phone Metadata." Cornell University Library, arXiv: 1511.06660, February 13, 2016.
- OECD Standard of Data Minimization — Minimum data required for maximum service.

Personal Data and Individual Access Control

Issue:

Many A/IS will collect data from individuals they do not have a direct relationship with, or the systems are not interacting directly with the individuals. How can meaningful consent be provided in these situations?

Background

Individuals can be better informed of uses, processing, and risks of data collection when they interact with a system. IoT presents evolving challenges to notice and consent. Data subjects may not have an appropriate interface to investigate data controller uses and processes. They may not be able to object to collection of identifiable information, known or unknown to them by wireless devices, driven by A/IS.

When individuals do not have a relationship with the data collecting system, they will have no way of participating in their data under the notice and consent regime. This challenge is frequently referenced as the "Internet of Other People's Things." A/IS embodied in IoT devices and value-chains will need better interfaces and functionality to help subjects understand and participate in the collection and use of their data.

Candidate Recommendations

Where the subject does not have a direct relationship with the system, consent should be dynamic and must not rely entirely on initial terms of service or other instruction provided by the data collector to someone other than the subject. A/IS should be designed to interpret the data preferences, verbal or otherwise, of all users signaling limitations on collection and use, discussed further below.

Further Resources

- Kaminski, M. "Robots in the Home: What Will We Have Agreed To?" Idaho Law Review 51, no. 661 (2015): 551–677.
- Jones, M. L. "Privacy Without Screens and the Internet of Other People's Things," Idaho Law Review 51, no. 639 (2015): 639–660.
- Cranor, L. F. "Personal Privacy Assistants in the Age of the Internet of Things," presented at the World Economic Forum Annual Meeting, 2016.

Personal Data and Individual Access Control

Issue:

How do we make better user experience and consent education available to consumers as standard to express meaningful consent?

Background

Individuals are often not given agency or personal tools to express, invoke, or revoke consent to the terms of service or privacy and/or data use policies in their contracts. In many cases, individual data subjects were not notified at all of the transfer of their data in the course of business or government exchanges.

Industry data uses have led to individual exposure to intangible and tangible privacy harms, for example, mistaken identity. Inability to manage or control information has also led to barriers to employment, healthcare, and housing. This dynamic has resulted in some consumer resignation over the loss of control over personal information, despite a stated desire for additional control.

Candidate Recommendations

Tools, settings, or consumer education are increasingly available and should be utilized to develop, apply, and enforce consumer consent. *Specifically:*

- **Design the terms of service (ToS) as negotiable to consumers** — Combine user interface design to control the rate and method of data exchange, and provide a corporate terms ombudsman staffed as human agency to consumers facing a terms of service contract. Software developers would produce contract management platforms appropriate for consumer negotiation. This would support features to negotiate terms of consent contracts fairly for meaningful consumer consent. An example metric would be a consumer agreement held to 85% of a terms of service agreement content, as grounds to move forward with the contract. Companies conclude what the "deal breakers" or non-negotiables are ahead of time.
- **Provide "privacy offsets" as a business alternative to the personal data exchange** — Provide a pay alternative to the freemium data exchange model, to limit or cap third party vendor access to personal data or limit transactional data to internal business use only. Business developers would have to cost count individual data based on a general market profile, or offer a flat rate for advertising-free service. If they know immediately how much money they will lose if a new user would not consent to an external data exchange, they have grounds to pass the cost to new consumers as a privacy offset product.

Personal Data and Individual Access Control

- **Apply "consent" to further certify artificial intelligence legal and as ethics doctrine** — Legal consent principles could be applied to a larger self-regulatory or co-regulatory artificial intelligence ethics certification framework for businesses and governments. This would be similar to medical certifications in ethics as a professional requirement, supportive of the Hippocratic Oath. Artificial intelligence ethics certification for responsible institutions (medical, government, education, corporations) should include education in applied legal consent principles, situation training regarding forms of consent, ethics certification testing, and perhaps a notarized public declaration to uphold ethical principles of consent. As an ethics board is formed it might: evaluate complaints, resolve ethical conflicts related to artificial intelligence and consent issues, improve upon current ethics procedures for consent, request independent investigations, review licensure or certification determinations, recommend professional penalties or discipline to organizations, and/or file legal claims based on findings.

- **Aggregate and provide visualization options for terms of service and privacy statements** — One way to provide better education and improved user experience, with respect to legal terms of use, is to offer visual analytics tools as a consumer control point of reference. Potential examples of this sort of effort include the Terms of Service Didn't Read Project and the Clarip. Both tools simplify the content of these policies and may provide users with clarity into how services are collecting, making use of, and potentially sharing personal and other information.

Further Resources

- Cavoukian, A. "Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices." Internet Architecture Board, 2010.
- "From Consent to Data Control by Design." *Data Ethics*, March 20, 2017.
- Hintze, M. *Privacy Statements: Purposes, Requirements, and Best Practices.* Cambridge, U.K.: Cambridge University Press, 2017.

Personal Data and Individual Access Control

Issue:

In most corporate settings, employees do not have clear consent on how their personal information (including health and other data) is used by employers. Given the power differential between employees and employers, this is an area in need of clear best practices.

Background

In the beginning stages of onboarding, many employees sign hiring agreements that license or assign the usage of their data in very non-specific ways. This practice needs to be updated, so that it is clear to the employee what data is collected, and for what purpose. The employee must also have the ability/possibility to request privacy for certain data as well as have the right to remove the data if/when leaving the employment.

Candidate Recommendation

In the same way that companies are doing privacy impact assessments for how individual data is used, companies need to create *employee data impact assessments* to deal with the specific nuances of corporate specific situations. It should be clear that no data is collected without the consent of the employee.

Furthermore, it is critical that the data:

- Is gathered only for specific, explicitly stated, and legitimate purposes
- Is correct and up to date
- Is only processed if it is lawful
- Is processed in a proper manner, and in accordance with good practice
- Is not processed for any purpose that is incompatible with that for which the data was gathered
- Is rectified, blocked, or erased if it is incorrect or incomplete having regard for the purpose of the processing
- Is not kept for a longer period than is necessary

Further Resources

- The Swedish Personal Data Protection Act is taking a generic approach to data protection and data privacy, but it is well applicable for the specific case of employee data.
- IEEE P7005™, Standard for Transparent Employer Data Governance. *This Working Group is open and free for anyone to join.*

Personal Data and Individual Access Control

Issue:

People may be losing their ability to understand what kinds of processing is done by A/IS on their private data, and thus may be becoming unable to meaningfully consent to online terms. The elderly and mentally impaired adults are vulnerable in terms of consent, presenting consequence to data privacy.

Background

The poor computer literacy of the elderly has been well known from the beginning of the information and Internet age. Among various problems related to this situation, is the financial damage caused by the misuse of their private information, possibly by malicious third parties. This situation is extremely severe for elderly people suffering from dementia.

Candidate Recommendations

- Researchers or developers of A/IS have to take into account the issue of vulnerable people, and try to work out an A/IS that alleviates their helpless situation to prevent possible damage caused by misuse of their personal data.
- Build an AI advisory commission, composed of elder advocacy and mental health self-advocacy groups, to help developers produce a level of tools and comprehension metrics to manifest meaningful and pragmatic consent applications.