



THE DOMAINS OF IDENTITY

A FRAMEWORK FOR UNDERSTANDING
IDENTITY SYSTEMS IN CONTEMPORARY
SOCIETY

KALIYA "IDENTITY WOMAN" YOUNG



The Domains of Identity

Series Introduction to Kaliya Young's *The Domains of Identity*

As Lead Editors, we are excited to write this Introduction to the Anthem Press Ethics of Personal Data Collection Series. We are grateful to Acquisitions Editor Megan Greiving whose initial communication with Colette Mazzucelli inspired our cooperation after speaking with Publisher Tej P. S. Sood.

The series builds on an initial special issue of *Genocide Studies and Prevention* that Colette organized at the invitation of Professor Douglas S. Irvin-Erickson, School for Conflict Analysis and Resolution, George Mason University; and Yasemin Irwin-Erickson, with funding for a series of workshops at New York University provided by a grant from the Robert Bosch Foundation in Stuttgart, Germany. We are most grateful to Anda Ruf and Carolin Wattenberg at the Bosch Foundation for their helpful and timely assistance in Germany and to Executive Director Richelle Ash and Professor Elisabeth King, NYU Steinhardt, as well as Miss Yvonne (Ye) Wang, PRIISM New York University, for Steinhardt's gracious hosting during one of the contributors' workshops. Tina Lam and Nicolette Teta, MA in International Relations (MAIR) Program at New York University, were instrumental in providing the introduction to the NYU DC site for the closing Bosch Workshop, including this volume's author Kaliya Young.

Likewise, the dedicated participation of NYU graduate candidates is sincerely appreciated, notably Laura Salter, Danielle Marie Lucksted, Annika Squires, Nicole Scartozzi, and Jakub Wojciech Kibitlewski. Jakub is joining the series team as a graduate exchange student in the MAIR Conflict Resolution seminar taught by Colette from the John F. Kennedy Institute for North American Studies, *Freie Universität Berlin*. We eagerly anticipate developing a partnership with Berlin institutions as the research in this series evolves and express our gratitude particularly to Senta Hoefler, Global Diplomacy Lab (GDL) and German Federal Foreign Office, for the forward-looking GDL initiatives related to our areas of interest.

This first volume in the series underlines an integral aspiration on the part of the editors and publisher alike: to advance the public discourse on the ethics of personal data, particularly its collection and dissemination. The omnipresent influence of big data, the rapid advances in technology, and the need to access personal data in increasingly remote locations to hold perpetrators of heinous crimes against humanity, including sexual violence in conflict, accountable, before local as well as international courts, resonate in the field experiences and academic research of different contributors to forthcoming volumes in the Series.

The rising concerns and incessant questions pertaining to the ethics of personal data speak to its evolution as a "meta-rhino," which is defined by Michele Wucker as "a structural issue that creates/worsens other challenges," for example, inequality, as expressed in her 2016 volume *The Gray Rhino*. Since the Cambridge Analytica scandal, it is abundantly clear, as Alexandra Samuel writes in a 2018 article for *The Verge*, that "[s]ocial networks and other advertising platforms may set up various processes that

nationally screen out data aggregators or manipulative advertisers, but as long as these companies run on advertising revenue, they have little incentive to promote transparency among data brokers and advertisers. And those industries, in turn, have little motivation to place ethics ahead of profit.”

The need for a revolutionary approach to the ways in which citizens worldwide should be compensated for the use of their personal data by myriad institutions and multinationals is a cardinal rule in the public conversations this series aims to instigate.

Moreover, of fundamental ethical concern as this series evolves is “surveillance capitalism,” which Shoshana Zuboff analyzes in the context of an emerging system of domination by technology firms. The transformation of power by these firms and their experts, and the corresponding behavior modification that occurs in this context operating “outside individual awareness and public accountability,” as discussed by Princeton Professor Paul Starr in the November/December 2019 issue of *Foreign Affairs*, necessitates action and reflection to nurture personal and community engagement to uphold democracy.

By launching a partnership with the Bled Strategic Forum, participating in the Paris Peace Forum, and developing projects with colleagues within the BMW Foundation Herbert Quandt Responsible Leaders Network, the contributors to this series intend purposefully to exchange ideas and propose initiatives that speak to various themes introduced by Kaliya Young in her timely analysis.

More than 20 years in the making, *The Domains of Identity* is pioneering research to expand enterprising thought leadership in our Anthem Press series. Kaliya is a trailblazer in the codification of the industry that we term “personal data,” specifically, the understanding of identity across every fragment of our diversity. The longstanding dedication by James Felton Keith in his career to asking questions such as “What is data?” and the industrial space of personal data, in particular, make this book as much a historical reference as a seminal touchstone of what we consider to be evidence of the existence of our personhood.

The groundbreaking history of this book is embodied equally by its contents and creator. It is a pleasure to shed light on the influence that Kaliya Young has on transforming a genre of thought about the Internet, cyberspace, personhood, privacy, protection, capitalism, corporatization, publicization (a new word introduced into the vocabulary of the genre), and privatization of the evidence of our lives and the communities in which they exist.

The journey leading James to the space of data sovereignty and data value that started via The Data Union was preceded by the oldest digital asset trade association, the Personal Data Ecosystem Consortium, which was preceded by the Internet Identity Workshop. Born out of the dot-com era and propelled into the twenty-first century, these orgs were all mothered by Kaliya. In 2005, Kaliya was asked to build an online

presence by Doc Searls when he founded Project VRM at the Harvard Berkman Klein Center for Internet & Society. She began her blog named "Identity Woman" and has become *The Identity Woman*, here a widely used Internet handle, to differentiate her from the others writing on topics of digital and non-digital data.

The Domains of Identity are as important to this time as our early laws of physics: how we understand our ability to move forward with the codification of our existence must be designed with the human's autonomy and choice first. Or man and womankind run the risk of automating everything that makes people human. This text's election is deliberate and hopeful: we did not know if Kaliya would agree to participate. James "Jim" Pasquale, a member of the series editorial board, deserves a special thank-you for making this work our lead volume citing Kaliya's lectures in 2010. His participation in a Bosch Fellowship Alumni–New York University–The Data Union transnational dialogue organized during fall 2018 at Cultural Vistas in New York City's historic Woolworth Building, including Zoom video communications with BMW Foundation Responsible Leader and Global Diplomacy Lab Alumna Elizabeth Maloba in Nairobi, allow us to reflect on the nature of this series and its evolution. In this context, our appreciation is expressed to Cultural Vistas President and Chief Executive Officer Jennifer Clinton, PhD, for her gracious assistance hosting our thought leadership events as a fellow member of the series editorial board.

Jim is an original cowboy of the data ecosystems and subject-matter expert at interoperability of data, leading with

"interoperability is more than just the ability of individuals to take their data along with them, and more about freedom of choice for individuals seamlessly moving data in and out of other ecosystems and platforms, including those based on Blockchains. This approach has an intrinsic value to both sides of the B2C (business-to-customer) and C2B (customer-to-business) equation. Some refer to this as hyper-relevance. Yet, it is more about putting customers first by starting with trust around data."

As we consume *The Domains of Identity*, it is necessary to consider data itself as a tangible, dynamic, non-rivalrous good that is only valuable in caucus with communities, yet with special regard for the individual to be able to exist holistically within a community with rigidity and agency. Without adding to the obfuscation of a relatively new topic, it is necessary to suggest that we all stick to the cultural basics when applying this text: "Do unto others as you would have them do unto you."

Colette Mazzucelli and James Felton Keith

New York University, The Data Union

The Domains of Identity

A Framework for Understanding Identity
Systems in Contemporary Society

Kaliya "Identity Woman" Young



ANTHEM PRESS

Anthem Press
An imprint of Wimbledon Publishing Company
www.anthempress.com

This edition first published in UK and USA 2020
by ANTHEM PRESS
75–76 Blackfriars Road, London SE1 8HA, UK
or PO Box 9779, London SW19 7ZG, UK
and
244 Madison Ave #116, New York, NY 10016, USA

Core definitions of the domains of identity (pp. 5–8) are licensed under
Creative Commons Attribution 4.0 International Public License

Copyright © Kaliya Young 2020

The author asserts the moral right to be identified as the author of this work.

All rights reserved. Without limiting the rights under copyright reserved above,
no part of this publication may be reproduced, stored or introduced into
a retrieval system, or transmitted, in any form or by any means
(electronic, mechanical, photocopying, recording or otherwise),
without the prior written permission of both the copyright
owner and the above publisher of this book.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN-13: 978-1-78527-369-8 (Hbk)

ISBN-10: 1-78527-369-8 (Hbk)

ISBN-13: 978-1-78527-491-6 (Pbk)

ISBN-10: 1-78527-491-0 (Pbk)

This title is also available as an e-book.

To my late parents David and Evangeline Young who made me and raised me,
AND

To the founders of Planetnetwork, Jim Fournier and Elizabeth Thompson,
without whose efforts I may never have found user-centric
identity and become the *Identity Woman*.

Contents

Acknowledgments	xi
Introduction.	1
1. Me and My Identity	9
2. You and My Identity (Delegated Relationships).	17
3. Government Registration	25
History to See the Future	37
4. Government Transactions	43
5. Civil Society Registration	49
6. Civil Society Transactions	53
7. Commercial Registration.	57
8. Commercial Transactions	63
9. Government Surveillance	67
10. Civil Society Surveillance	73
11. Commercial Surveillance.	77
12. Employment Registration	83
13. Employment Transactions	87
14. Employment Surveillance	91
15. Data Broker Industry	95
16. Illicit Market.	103
Conclusion.	107
Bibliography	109
Index.	125

Acknowledgments

I need to thank the Master of Science in Identity Management and Security program faculty whose teaching inspired me to come up with these domains of identity.

I would like to thank Phil Windley and Doc Searls with whom I co-founded The Internet Identity Workshop in 2005. The work of our community is instrumental in informing this book.

I would like to thank Dan McNeece, Bill Cope, Daren Hansen, and Phil Windley who were at the session I held during the personal API (un)Conference in Utah where I first workshopped the original set of six domains of identity.

The second person I workshopped the 12 domains of identity with was Bob Blakley, and I am grateful for his encouragement to develop them out and his willingness to become a co-supervisor of this report.

I would like to thank Dawna Ballard for her teaching in the MSIMS program and for her willingness to be a supervisor of this report.

A final thank you goes to Rich Gibson and John Kelly for doing strong copy edits of this book.

Comments, Questions, or Collaboration

I welcome your feedback on this book. Please write to us with your comments or questions to DomainsofID@identitywoman.net.

INTRODUCTION

The Domains of Identity outlines 16 key domains where individual's personally identifiable information ends up in databases. The book enumerates the 16 domains of identity, describing each in detail along with the types of data collected in the domain, the source and key actors among whom information moves.

I wrote this book for several reasons:

- 1) to give journalists and the general public clear simple terms to understand the mechanics of and issues surrounding identity management across a range of societal contexts;
- 2) to support professionals in the fields of identity management and privacy having a common language to understand where and how different types of identity interactions are happening, and from there being more able to solve the challenges that different domains present;
- 3) to support those working in academia and the private sector having a common language to understand the landscape of issues so that academic research actually serves industry and industry work can be better understood by those researching the field; and
- 4) to support government officials and those engaged with public policy issues being able to understand the challenges that exist in different domains and be able to craft better policies to address challenges within those domains.

Everyone in our society participates in identity management on a daily basis. It is so common that we do not really think about it. As a result, the discourse about identity often conflates radically different issues. The illicit market in which personal data are bought and sold is very different from the contemporary data broker industry, but it is not uncommon for people with fears about personal data use to lump these two contexts together—forgetting that one is a legal business market and the other is a result of criminal activity. Likewise, the data from a data breach via an HVAC vendor, such as the Target breach, that end up in an illicit market is different from data from a compromised enterprise identity management system protected by weak authentication (just a password) resulting in employee's authentication credentials being stolen in a spear phishing attack.

There are a few very obvious and much-discussed archetypical identity management scenarios:

Employee to employer
Citizen to government
Consumer to merchant

Each one of these has very different power relationships and characteristics. Through conversations arising out of the University of Texas (UT) at Austin Master of Science in Identity Management and Security program, it became clear that these three simple scenarios were not comprehensive enough to hold the whole range of activities that lead to individuals' personally identifiable information (PII) being collected, ending up in databases, and being used and misused.

I worked to define a simple comprehensive set of domains, each with different processes and contexts, where individuals' data (PII) end up in databases. The result is the 16 domains of identity. Once the domains had been defined, I dove into all the academic research relative to identity management, finding more than 900 articles in the UT Library, and then sifted through them to identify papers that specifically explained and defined the domains. For my master's report, I wrote out detailed descriptions of each domain based on the literature. The domains articulated in this book are not new; all of them existed 100 years ago. However, computer technologies have changed how all of them operate.

The domains are the following:

- Me and My Identity
- You and My Identity (Delegated Relationships)
- Government Registration
- Government Transactions
- Government Surveillance
- Civil Society Registration
- Civil Society Transactions
- Civil Society Surveillance
- Commercial Registration
- Commercial Transactions
- Commercial Surveillance
- Employment Registration
- Employment Transactions
- Employment Surveillance
- Data Broker Industry
- Illicit Market

Figure I.1 gives a visual flow of how the domains relate to one another. The identity information about individuals flows from the individual or their delegated representatives into their interactions with governments, civil society organizations, commercial entities, and when they themselves are employed. Within all these contexts, individuals register, transact, and are surveilled. With all of those interactions, databases are created with PII about people. The data broker industry collects data from almost

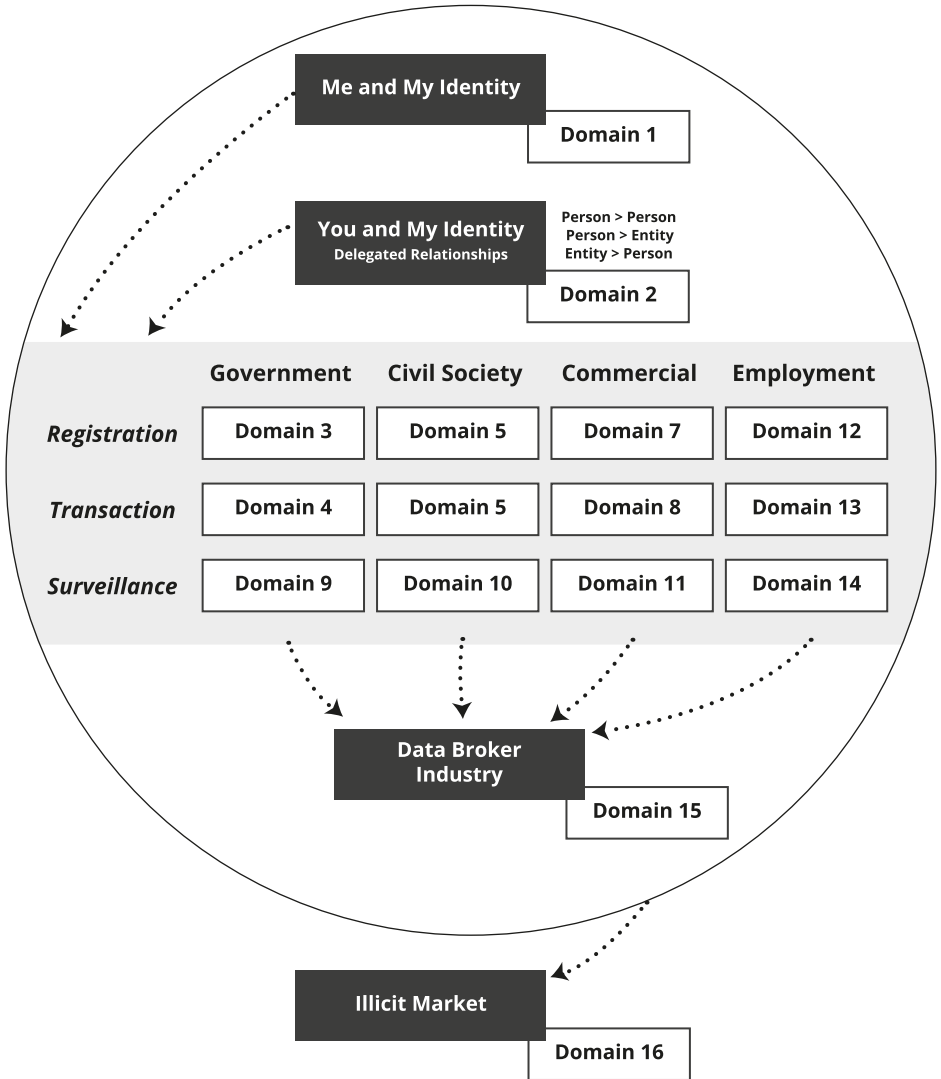



Figure I.1. The domains of identity and their relationship to each other mapped.

Created by the author Kaliya Young.



all of these domains and uses the information to create detailed dossiers about millions of individuals and sells the data. All of the places where individuals' data are in databases are vulnerable to data theft by criminals operating in the illicit market. To simplify navigating this book, each domain has the chapter it can be found in listed. Together, these domains present a holistic framework to understand all of the places where people's PII ends up in databases.

There is extensive formal academic research about some of the domains in this article such as government registration, government surveillance and commercial surveillance, employment in all areas, and the data broker industry. However, there is not sufficient formal academic research outlining the basic business processes involved in the civil society in all contexts, commercial registration, commercial transactions, and the illicit market. The lack of clear systematic research into understanding these domains is evidence of a need to provide a coherent framework for understanding identity domains.

The Identity Domains

This section provides a brief overview of the identity domains to introduce the detailed treatment of each domain in its own chapter later in the book.

1 Me and My Identity

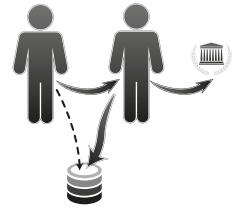
Me and my identity is the identity of the self, and how each individual is the starting point for interacting with digital systems. The community of professionals focused on user-centric identity has this focus at the center of their work. It is in this domain that the individual might have control of their own applications and cloud services and collect their own data.



2 You and My Identity (Delegated Relationships)

There are three main types of delegation:

1. **Person-to-person delegation.** The primary example of this is a parent's relationship with their children or adult children's custody of their elder parents. Another case is an individual delegating a particular portion of their affairs to another, for example, delegating interacting with the tax authority to a professional accountant. In a will, one can establish who becomes the executor of one's estate after one dies. There is also the new phenomena of intimate surveillance by household members.
2. **Person-to-entity delegation.** An individual delegates something to a corporate entity (legal person). For example, an individual wanting to aggregate all their financial information. They pull it together using a service like Mint.com that logs into all their bank accounts, pulls the information, and centralizes it.
3. **Entity-to-person delegation.** Corporations delegate the responsibility to act on their behalf to particular natural persons.



3 Government Registration

Most individuals' first identity-related event with an institution occurs when parents register their child's birth (on behalf of the child) in a **government registration** process. Individuals also register with the government at other times in their life. These secondary government registrations include marriage and death, obtaining a license to drive, getting a passport, professional licensing, and registering to pay taxes or registering to vote. The first step is filling out registration forms once the government has accepted those and created a record in their systems they issue identification numbers and/or documents to the individual.



4 Transactions with Government

Once an individual has been formally registered with the government and an identifier has been issued (a number in a government database that points at a particular person), the individual can use this number to do a **transaction with government**. For example, a transaction is the payment of taxes using the identifier issued (in the United States this is a Social Security number (SSN)). These two types of interactions (registration and transactions) with government are often thought of as the same, but they are quite different. For the most part, one needs to be registered with the government before transacting with it. Individuals present identification to their government and are able to transact with or receive services from the government.



5 Civil Society Registration

Civil society registration happens when individuals begin relationships with any number of institutions: professional associations, nonprofit membership groups, religious congregations, sports leagues, and so forth. We also include educational and health care contexts in which people are patients and students. While some of these institutions are “for profit,” the nature of the transactional relationships suggests that it makes more sense to include these types of transactions in this domain. The first step is for the individual to go through a registration process possibly filling out forms. Once the organization has accepted those and created a record in their systems the organization issues a credential to the individual.



6 Civil Society Transactions

Civil society transactions are all the interactions with civil society institutions after registration: the classes you attend and the resulting transcripts that document those transactions, the visits to the doctor, hospital and labs, the accumulation of continuing education credits (CEC) as a professional, or the participation in any regular meetings/activities and voting as a member. Individuals present their credentials to the organization and are able to transact with or receive services from the organization.



7 Commercial Registration

Commercial registration happens when one creates an account with a merchant or service provider. The first step is for the individual to go through a registration process possibly filling out forms. Once the company has accepted those and created a record in their systems the company issues a credential and/or number to the individual.



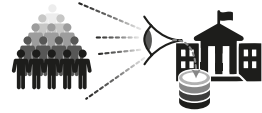
8 Commercial Transactions

Commercial transactions happen when a customer transacts for goods and services with a merchant or service provider. Individuals present their credentials to the company and are able to buy goods or services and have those transactions linked to their customer record.



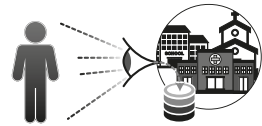
9 Government Surveillance

Lawful **government surveillance** can include surveillance of the whole society by a census, labor department surveys of employment trends, surveillance as part of lawful Internet tracking, or law-enforcement surveillance via warrant access. Examples of unlawful surveillance include warrantless mass surveillance of communications, revealed by Edward Snowden.



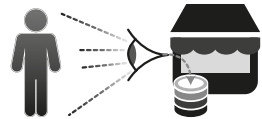
10 Civil Society Surveillance

Civil society surveillance is not yet widespread. However, there is more and more tracking of health care and educational activities. Professional associations may also be surveilling their members. Civil society groups may organize to perform collective citizen surveillance of corporations or governments.



11 Commercial Surveillance

Commercial surveillance is vast as the push is to get more information about consumers and use it to shape their purchasing activity. It happens in person in stores with CCTV and sensor networks. It also happens with digital tools and services via cookies and beacons from advertising networks in web content.



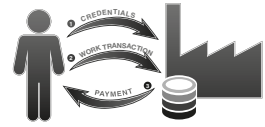
12 Employment Registration

Employment registration is the process that a new hire goes through to begin work with an employer. It starts with the application process where PII is shared from a prospective employee with an employer, there is an evaluation process where more PII might be shared and finally after a job offer is made to an employee they are enrolled in to the enterprise identity and access management system and then issued credentials.



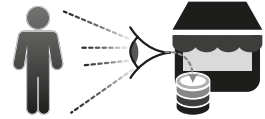
13 Employment Transactions

Employment transactions are all the logins and authorizations that happen when employees do their job while physically present on site, for example, entering a building for work. It also may happen when they log on to digital systems. Individuals present the credentials issued to them by the enterprise, do their work within the context of their employment and in turn are paid.



14 Employment Surveillance

Employment surveillance is something that happens in the workplace and isn't new. Taylorism was created in the early part of the twentieth century to track and shape how workers work in order to reduce employer costs and increase employee productivity. With the rise of computerized technology, its form is changing. When individuals work, they are surveilled by their employers.



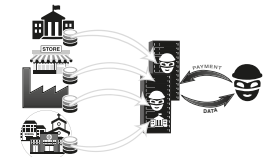
15 The Data Broker Industry

The **data broker industry** collects and links together data about millions of people in massive databases. There is no direct relationship between the companies that do this and the individuals they gather or buy information about. While there is no direct relationship in the collection of the data, brokers who are subject to the Fair Credit Reporting Act are required to provide consumers access to the information they have about them and the ability to correct it. This industry gets the data they use to compile these databases from the government, civil society, and commercial and employment contexts. They package the data about people into digital dossiers and sell them raw or in the form of scores on which they rate the subjects in their database on dimensions important to their clients.



16 The Illicit Market

The **illicit market** is where the information about individuals ends up after it is stolen or hacked by criminals from any of the above domains, including data brokers and even the individuals themselves. There are two primary types of illicit market activity: criminal networks and state-sponsored data theft and collection. Criminal networks are more likely managing the stolen data in spreadsheets rather than "organizational databases." Data from state-sponsored theft are ending up in large databases and being correlated with other data sets from other sources, including publicly available data. There is another illicit market context: individuals make a personal choice to transact in illicit or black markets, like buying drugs with bitcoin, but that is not included in the set of issues we are focused on.



1. Me and My Identity

Me and my identity is the identity of the self, and each individual is the starting point for interacting with digital systems. The community of professionals focused on user-centric identity, at the Internet Identity Workshop,¹ has this focus at the center of their work. It is in this domain that the individual might have control of their own identifiers, their own servers, and collect their own data (Figure 1.1).

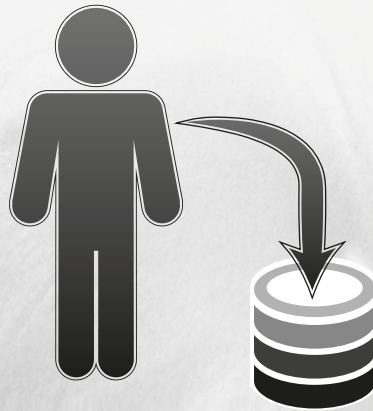


Figure 1.1. Me and my identity. This represents the individual and a database they have control over and store their identity information and data in.

Roles

- The individual
- Devices the individual uses to store and manage identity information and personal data
- Services that store individual's personal data

Sources of PII

- The individual
- The individual's identity documents
- Devices the individual uses
- Services the individual interacts with

Types of Transactions

- Setting up tools to store and save personal data and information
- Saving data generated in transactions with a personal data store
- Managing the software that works on behalf of the individual and setting up preferences

Types of PII

- Name
- Preferred name
- Relations

¹ The Internet Identity Workshop was co-founded by Doc Searls, Phil Windley, and myself in 2005: <http://www.internetidentityworkshop.com>.

What Is Identity?

Discussions about identity can get very philosophical quickly. There is an enormous body of work that covers this terrain stretching back to the origins of humanity. This description will touch on a very brief overview that is rooted in Western philosophical thought. An avenue for future research is exploring how different philosophical traditions (Indigenous, Africa, Asian, Feminist, etc.) can inform the development of digital identity systems.

Who is “me” and what does “my identity” mean?

“Me” is a “self,” that is, an individual referring to the same individual.

The word “identity” comes from the Latin word from “sameness.” This is the underlying frame of identity in the Western tradition. Locke’s theory of mind² articulates this modern notion of the self that is a persistent consciousness through time.

Some challenges arise applying this to digital identity because while persistent identifiers are viewable, third parties can’t see into individual’s persistent consciousness through time. The modern industrial states have had to invent a notion of identity that can be assigned and be based on observations by third parties over time where the observations get recorded in databases.

Individuals have identities composed of a whole range of characteristics. We interact with a wider world and project “a self” to a wider world with various actions. This dramaturgical model of human life in society was developed by Erving Goffman³ in his book *The Presentation of Self in Everyday Life*.

There are two theories that prevail in the literature about the interplay of the self in the social world. Identity Theory sees the meaning derived from roles one plays in social contexts and Social Identity Theory sees the meaning derived from belonging to groups.⁴

Identity Theory and Social Identity Theory have been extended. In the digital world, it is understood that we project different selves into different contexts. S. J. Tracy and A. Trethewey⁵ put forward the idea of a crystalized self that looks different from different angles or takes on different shapes.

Network theorist Manuel Castells discusses the interplay between the meaning that individuals create with their actions and the *symbolic identification* by a social actor of the purpose of their action: “For most social actors meaning is organized around primary identity (that is an identity that frames the others), which is self-sustaining across time and space.”⁶ He also points out that the social construction of identity always takes place in a context subject to power relationships.

² OECD (Organisation for Economic Cooperation and Development), “At a Crossroads: Personhood and Digital Identity in the Information Society,” 2007, Directorate for Science, Technology and Industry, STI Working Paper 2007/7, February 29, 2008.

³ Erving Goffman, *Presentation of Self in Everyday Life* (Garden City, NY: Doubleday, 1959).

⁴ W. B. Swann Jr. and J. K. Bosson, “Self and identity,” In *Handbook of Social Psychology*, ed. S. T. Fiske, D.T. Gilbert, and G. Lindzey (Hoboken, NJ: Wiley, 2010), 589–628.

⁵ S. J. Tracy and A. Trethewey, “Fracturing the Real-Self↔Fake-Self Dichotomy: Moving toward ‘Crystallized’ Organizational Discourses and Identities,” *Communication Theory* 15 (2005): 168–95. doi: 10.1111/j.1468-2885.2005.tb00331.x.

⁶ Manuel Castells, *The Power of Identity: The Information Age: Economy, Society, and Culture Volume II* (Malden, MA: Wiley-Blackwell, 2003).

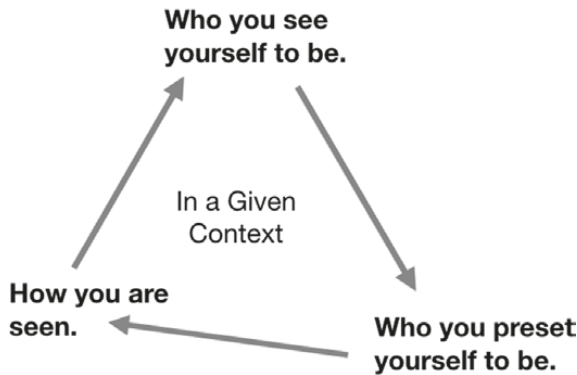


Figure 1.2. Identity of the individual in contexts.

Created by the author Kaliya Young

To make sense of these different theories, Figure 1.2 highlights the relationship between the internal self, the projected self that others see, and how the way one is seen in turn affects how one thinks about one's self.

What Is My Digital Identity?

Much of this book is about domains of identity where individuals' information is recorded in digital databases as they register with institutions, have transactions with institutions, or are surveilled by institutions. In this particular domain of me and my identity, we are concerned with tools to support the individual collecting and managing their own identity and data.

It is not new for people to log information about themselves in diaries using the technology of pen and paper. We now have digital tools at the individuals' disposal to collect information about themselves. Personal computers have been available for almost 40 years, smartphones for about 10, and now we have a whole range of small sensor devices. Some of the scholarship around these emerging self-tracking practices is reviewed below.

To understand the emergence of the systems for enabling people to manage their own identity, it is important to look at the terminology developed to describe the self or individual represented in the digital realm. The term "digital persona" was coined by Roger Clarke in 1992, inspired by Jungian psychology:

The *anima* is the inner personality, turned towards the unconscious, and the *persona* is the public personality that is presented to the world. The *persona* that Jung knew was that based on physical appearance and behavior. With the increased data-intensity of the second half of the twentieth century, Jung's *persona* has been supplemented, and to extent even replaced, by the summation of the data available about an individual.⁷

⁷ Roger Clarke, "The Digital Persona and its Application to Data Surveillance." *The Information Society* 10, no. 2 (1994a): 77-92, <http://www.rogerclarke.com/DV/DigPersona.html>.

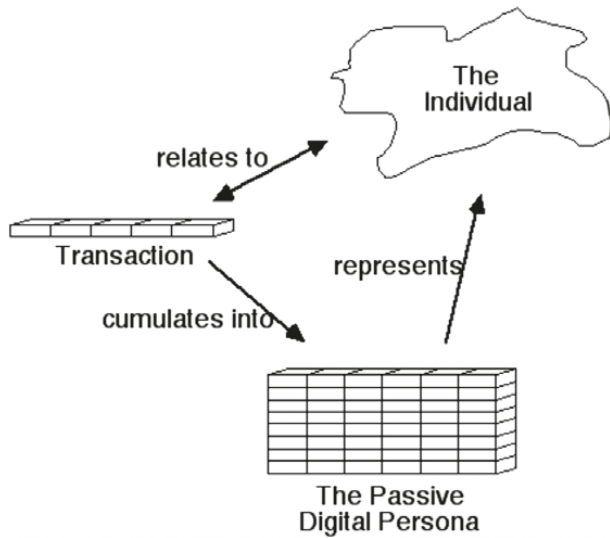


Figure 1.3. The passive digital persona.

This summation of the data might be called a “simulacrum,” Latin for “likeness” or “similarity,” and is a representation or imitation of a person or thing.

His definition of the digital persona is “a model of an individual’s public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.” During the time he wrote this, many people were interacting online in Usenet mailing lists, and the impression one had of them was based on those interactions.

In Figure 1.3,⁸ there is no conception that the individual has a digital identity of their own. This figure does model the aggregation of transactions over time that an organization collects and has access to. There also isn’t a conception of the individual having their own computing device to manage interactions with various institutions or to have their own record of such transactions.

Who Owns My Digital Identity? Is Ownership Even a Relevant Concept Here?

We own our physical selves. We have autonomy over choices we make as we navigate the physical world. In the digital world, we share information with various organizations and in various contexts. This information is collected and stored. Under US law, the entity that collects the information in fact owns it. In European legal doctrine, the person whom the information is about is not so much the owner but has rights over how the information can be used and dispersed.

There are challenges with using the frame of ownership to talk about data, because data is different from physical things. One can have more than one copy of data whereas there is only one of a physical thing and someone can own it or not. To

⁸ From *ibid.*

address the challenges of data sharing and systems, one needs protocols to support the tracking and flow of data from the individual to entities and to empower the individual to periodically update and change the information.

Who Controls My Digital Identity (or Pieces of It?)

Different efforts have been made to support the individuals owning their digital identity and having control over key aspects of it.

User-Centric Identity

A community of technologists met at Digital Identity World in 2003–4 and began to work together to create “user-centric digital identity” tools and technology. They aimed to put the user at the center of their own interactions online. These efforts were in response to two types of identity transactions that were common: (1) enterprise identity management of an employee identity relative to the enterprise and (2) the records of customers an enterprise keeps.

The Augmented Social Network White Paper⁹ defined it this way:

Every individual ought to have the right to control his or her own online identity. You should be able to decide what information about yourself is collected as part of your digital profile, and of that information, who has access to different aspects of it. Certainly, you should be able to read the complete contents of your own digital profile at any time. An online identity should be maintained as a capability that gives the user many forms of control. Without flexible access and control, trust in the system of federated network identity will be minimal. A digital profile is not treated [by corporations who host them] as the formal extension of the person it represents. But if this crucial data about you is not owned by you, what right do you have to manage its use?

A civil society approach to persistent identity is a cornerstone of the Augmented Social Network project.

Figure 1.4 is a diagram by Johannes Earnst drawn in 2006¹⁰ to articulate the core idea of an individual being able to manage their digital identity rather than companies pointing at them because they stored their identity and transaction data.

The Internet Identity Workshop,¹¹ which has gathered every six months since 2005, has been working to develop tools and protocols that empower the individual relative to how their identity information and data are managed by institutions they interact with.

⁹ Ken Jordan, Jan Hauser, and Steven Foster, “The Augmented Social Network: Building Identity and Trust into the Next Generation Internet,” *First Monday* 8, no. 8, <https://journals.uic.edu/ojs/index.php/fm/article/view/1068/988>.

¹⁰ Johannes Earnst, image clipped from presentation by Johannes on use-centric digital identity (2006).

¹¹ Internet Identity Workshop (IIW) (2005–18): <http://www.internetidentityworkshop.com>.

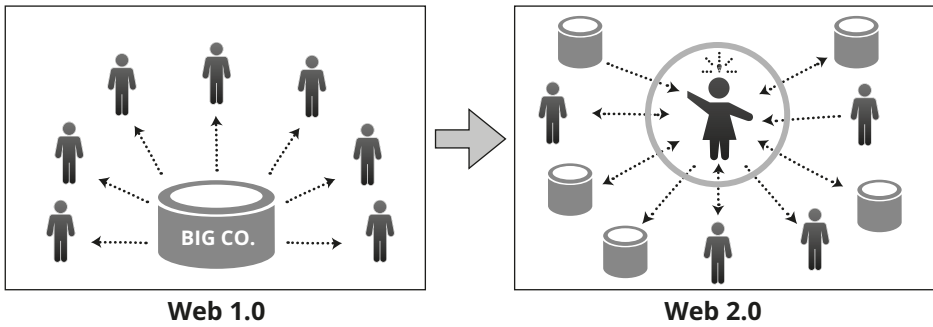


Figure 1.4. Based on a diagram by Johannes Ernst's 2006 slide presentation shared with the author.

Indie Web Camp

A grassroots group has been working on developing standards at the Indie Web Camp,¹² which has been organizing and supporting the development of simple protocols that anyone can implement to manage their own data.

Quantified Self

Since the development of the smartphone and sensor devices, a whole movement has emerged around self-tracking that individuals do for themselves, collecting data about their own activities. The Quantified Self was “named” and popularized by Gary Wolff and Kevin Kelly in 2008. Deborah Lupton,¹³ in recent work, outlines five different modes of self-tracking: private, communal, pushed, imposed, and exploited. Private self-tracking is the one that fits in me and my data and is done by individuals to “achieve self-awareness and optimize or improve their lives.”

Digital Human Rights

Aral Balkan describes himself as a cyborg rights activist and writes in an article¹⁴ that “[d]igital rights are human rights.” He goes on to articulate the issue that we are extending our biological capabilities with technology and that parts of ourselves are spread out among and within our things. He makes the argument that his iPhone is part of himself and that the push by governments and corporations to aggressively surveil and get into our devices are assaults on the self. We do have a “rich body of laws and regulations that protect the sanctity of the self and the rights of human beings.” The solution, he says, to this challenge of the current direction of surveillance by governments and corporations is to move to decentralized, zero-knowledge proof, alternative technologies.

¹² Indie Web Camp, “Main Page,” 2017, <https://indieweb.org>.

¹³ Deborah Lupton, “The Diverse Domains of Quantified Selves: Self-Tracking Modes and Dataveillance,” *Economy and Society* 45, no.1 (2016): 101–22. doi: 10.1080/03085147.2016.1143726.

¹⁴ Aral Balkan, “Digital Being,” *Arena Magazine (Fitzroy, Vic)*, no. 143 (2016): 18–20.

Self-Sovereign Identity

In the last few years, a new term has arisen out of the community focused on user-centric identity and personal data: “Self-sovereign identity.”

Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user’s identity across multiple locations, with the user’s consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can’t be locked down to one site or locale.¹⁵

Writing on his blog *Moxy Tongue*, Devon Loffreto wrote about self-sovereign identity concepts in early 2016:¹⁶

Self-Sovereign Identity must emit directly from an individual human life, and not from within an administrative mechanism created by, for, as abstractions of individual human activities, and must remain amenable in design and intent directly by individual humans with original source authority.

Self-Sovereign Identity references every individual human identity as the origin of source authority. A self-Sovereign identity produces an administrative trail of data relations that begin and resolve to individual humans. Every individual human may possess a self-Sovereign identity, and no person or abstraction of any type created may alter this innate human Right. A self-Sovereign identity is the root of all participation as a valued social being within human societies of any type. The denial of self-Sovereign identity disavows human authority to individuals in order to transmute this authority via an administrative chain of custody without root authority. While plausibly deniable, the resulting relationship infrastructure disavows self-Sovereign identity, and thereby achieves liability exposure at odds with human will and operational intent as expressed by individual humans across time and place of infinite design.

What Is the Correct Relationship between the Individual, the State, and Private Actors and Organizations, with Respect to My Identity?

These are big questions. The government registration chapter of this book discusses the contemporary processes for government registration. Individuals existed before states and we figured out how to interact with each other. We are living in a relatively unique time within a mass society at a state level with hundreds of millions of people.

¹⁵ C. Allen, “The Path to Self-Sovereign Identity,” *Life with Alacrity Blog*, April 25, 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.

¹⁶ Devon Loffreto, *Moxy Tongue Blog*, February 9, 2016, <https://www.moxytongue.com/2016/02/self-sovereign-identity.html>.

One of the challenges that self-sovereign identity efforts are trying to solve is supporting the individual having control over an identifier that was not issued by a corporation or a government and so cannot be taken away from them by either.

More data is being generated by people as they live their lives than ever before. It is being collected by the smartphones so many carry. The current structures mean that the companies that make these phones and the applications that run on them get enormous amounts of data about us and we never get copies of this data. These devices and applications in many cases simply will not work without this data. They have copies of our simulacrum, but we do not. There are efforts underway to try and change this, and companies like digi.me and Meeco are trying to build services with this as a core premise.

What Do Emerging Technical Architectures Do to Potentially Create Alignment?

There is a new group of companies collaborating to develop open standards for decentralized identifiers (DIDs) that are generated by and controlled by individuals.¹⁷ This new type of digital identifier serves as an anchor for verifiable credentials that can be issued to individuals or other institutions. Research into both the underlying infrastructure and user experiences to make this happen is supported by the US federal government.¹⁸

What Are the Gaps between How Delegation Is Managed with and without Digital Technology?

We have yet to see tools in the marketplace that fully empower the individual to collect and manage their identity digitally. The emergence of the cell phone and applications on it has enabled individuals to track data about themselves in whole new ways. There are also some promising new possibilities with decentralized or self-sovereign identity.

¹⁷ Drummond Reed and Les Chasen, "Requirements for DIDs (Decentralized Identifiers)," Rebooting the Web of Trust II: ID2020 Design Workshop (2016). <https://nbviewer.jupyter.org/github/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/final-documents/>

¹⁸ A. John, "Identity Management & Data Privacy Research, Development and Transition," Department of Homeland Security, Science and Technology, slide presentation (2017).

2. You and My Identity (Delegated Relationships)

There are three main types of delegation:

- 1. Person-to-person delegation.** The primary example of this is a parent's relationship with their children or adult children's custody of their elder parents. Another case is an individual delegating a particular portion of their affairs to another, for example, delegating interacting with the tax authority to a professional accountant. In a will, one can establish who becomes the executor of one's estate after one dies. There is also the new phenomena of intimate surveillance by household members.
- 2. Person-to-entity delegation.** An individual delegates something to a corporate entity (legal person). For example, an individual wanting to aggregate all their financial information. They pull it together using a service like Mint.com that logs into all their bank accounts, pulls the information, and centralizes it.
- 3. Entity-to-person delegation.** Corporations delegate the responsibility to act on their behalf to particular natural persons.

It should be noted that there are special cases of delegation where the government is given responsibility for people that are not covered in this book: (4) where parental responsibilities are taken from children's parents and held by the government, for example, when children enter foster care, and (5) after a person dies without a will and/or without an executor, the government fills this role.

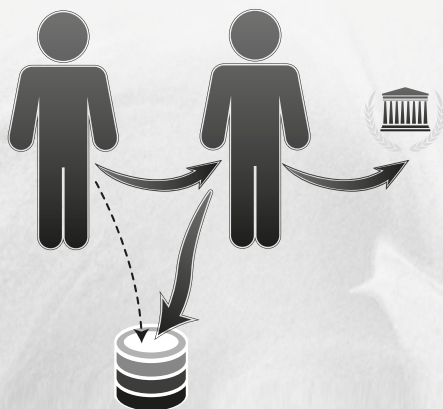


Figure 2.1. You and my identity (delegated relationships). The individual is represented by another individual to act on their behalf with institutions.

Roles/Actors

- Person acting for another person
- A person acting for another legal entity
- Legal entity acting for a person (foster care)
- Artificial intelligence (AI) agents acting for a person
- AI agents acting for a legal entity (Amazon Echo)

Sources of PII

- The individual
- The agent
- Sensors
- Interactions with AI agents
- Entities one is delegating to and from

Examples of Transactions

- Making health care decisions for another
- Preparing taxes and handle transactions
- A parent consenting to transactions on behalf of a child
- A corporate executive signing agreements or executing transactions on behalf of the firm

Types of PII

- Name
- Address
- Agent permissions
- Metadata from sensors
- Records from interactions with institutions (schools, hospitals, tax authorities)

Relationship to Other Domains

You and my identity is where activity related to individuals who cannot or choose not to act on their own behalf interact with identity and data systems. It was important to distinguish this from the me and my identity domain because not everyone acts on their own behalf in transactions. These two domains together are the source of the interactions with the next 12 domains covering the contexts of governments, commercial entities, civil society entities, and employment.

Who Is a Natural Person?

Before leaping into the details of the description of delegated identity between people, it is worth noting that only natural persons are given the right to delegate their identities in many contexts; thus, natural personhood is a prerequisite to delegation. It is therefore also worth considering who a natural person is and how this has changed over time.

In the United States and elsewhere, the right to act autonomously as an adult individual was not universal. Women who were married lost certain rights to act on their own behalf. Africans were captured in Africa and forcibly brought to the United States and subjected to enslavement. Until the Civil War and the Emancipation Proclamation, they were considered property and were not able to act on their own behalf.¹ The status of American Indians has changed over time and the US government put in place many rules to control the movement of indigenous peoples, requiring passes for them to leave their land. They were not citizens of the United States until the passage of the Indian Citizenship Act of 1924.²

¹ S. Browne, *Dark Matters: On the Surveillance of Blackness* (Durham, NC: Duke University Press, 2015 [1973]).

² Mawaki Chango, "Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity," PhD dissertation, School of Information Studies (2012), https://surface.syr.edu/it_etd/74.

What Is Person-to-Person Delegation?

"Identity delegation is where one [person] can authorize another to act on his or her behalf to access certain services provided by public institutions."³ The European Union defines the needed functionality in a 2005 paper:⁴ "eID compliant systems will support mechanisms to identify and authenticate natural persons together with their varying roles (principal, delegate, intermediary, authorized agent, etc.) including roles on behalf of legal persons (administrations or businesses)."

Delegated relationships for people start at the very beginning of life, when births are registered with the state. Parents fill out the forms they are given at a hospital after a child is born; they are acting as an agent for their child when registering the birth. Parents are the legal guardians for their children, and thus they are agents relative to transactions that involve their identities until the children reach adulthood. There are also instances where the state takes over in a guardian role for children it removes from their parents.

How Is It Managed?

In our system of common law, there are certain relationships where by default there is delegation of responsibility. Parents are the legal guardians of their children until the age of 18. There are also certain rights that come with marriage, where spouses are authorized to act on behalf of one another.

The law in the United States provides ways for others to have guardians appointed for them when they are not capable as adults of making decisions for themselves. This includes some of the elderly, people with mental illness or dementia, and the disabled. If the person is not able to grant this power on their own, the courts can impose conservatorship or guardianship.

There is also the creation of a power of attorney to act on another's behalf in private affairs and business or legal matters. For example, one can delegate dealings with the Internal Revenue Service (IRS) to a tax accountant. The person who authorizes the other to act is called the *principal*, *grantor*, or *donor* of the power, and the one who is authorized to act is the *agent*, *delegate*, or *power of attorney*. There is a whole set of common law around how the agent must act with a fiduciary duty toward the principal. For the power of attorney to become legally enforceable, a document must be signed and dated by the principal or by a court. This paperwork is required by institutions such as medical facilities, banks, and others to permit a person to act on another's behalf. Systems are in place to track that one person is acting on behalf of another.

How Is Document Signing Managed in the Digital World?

Globally, there are a few national electronic identity (eID) systems that actually support individuals being able to log on to a system with one set of credentials and

³ S. Sánchez García, A. Gómez Oliva, E. Pérez Belleboni, and I. Pau de la Cruz, "Solving Identity Delegation Problem in the E-Government Environment," *International Journal of Information Security* 10, no. 6 (2011): 351–72. doi: 10.1007/s10207-011-0140-7.

⁴ European Union, "Signposts towards eGovernment 2010," 2005, https://web.archive.org/web/20060711185811/http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf.

to have another set that is used to “sign” things. This is the case with the Belgian and Estonian eID cards. There are privacy issues with this type of architecture, but at least there are two different modes, one for authenticating an identity and one for signing something.

Gaps Delegation Management

To date, there has been very little market adoption in the way of digital tools to support delegation of authority and the exercise of delegated authority. Digital systems need ways for people to assign access from grantors’ primary accounts to agents. Once that ability is in place, we need to support ways for the agent to log on without the grantor’s primary credentials (the username and password). Agents need their own credentials to access grantor accounts, and with this comes accountability for agents’ actions on behalf of the grantor.

Peeters et al.⁵ defines three parties involved in the process of delegating electronic identity:

Delegator: The person or entity who shares one or more privileges in accessing a service with another person or entity by means of what is usually called a delegation assertion/token.

[*Delegate*]: A person who receives the privileges of the delegator, namely the delegation assertion, for access to a service.

Service Provider: An entity that provides services to the delegate following presentation of the delegation assertion.

Figure 2.2⁶ shows the flow of information between the parties in a digital transaction.

Figure 2.2 highlights two different modes of delegation. In the first diagram, the delegator is using a delegate to access a service on their behalf (such as a bank account or medical service portal). In the second diagram, the delegator is actually the owner of the resource and is giving the delegate permission to access it.

There are efforts to create some of this functionality with standards like Open Authorization (OAuth).⁷ This standard allows individuals the ability to delegate access to an account to another service. OAuth allows individuals to permit services to access their accounts on their behalf. An example of a use case for this is an individual hosting photos in one photo-sharing service and wanting to export those photos to a second service. Instead of giving the username and password for the first account to

⁵ Roel Peeters, Koen Simoens, Danny De Cock, and Bart Preneel, “Cross-Context Delegation through Identity Federation,” in *BIOSIG 2008: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, ed. Arslan Brömme, Christoph Busch, and Detlef Hühnlein (Bonn: Gesellschaft für Informatik, 2008), 79–92.

⁶ Figure 2.2, top: Justo Carracedo, Ana Gomez, Emilia Perez, and Sergio Sanchez, “Social and Legal Implications of Digital Identity in a Multi-national Environment,” 2010 IEEE International Symposium on Technology and Society; bottom: Laurent Bussard, Anna Nano, and Ulrich Pinsdorf, “Delegation of Access Rights in Multi-Domain Service Compositions,” *IDIS 2* (2009):137–54. doi: 10.1007/s12394-009-0031-5.

⁷ OAuth (2017): <https://oauth.net>.

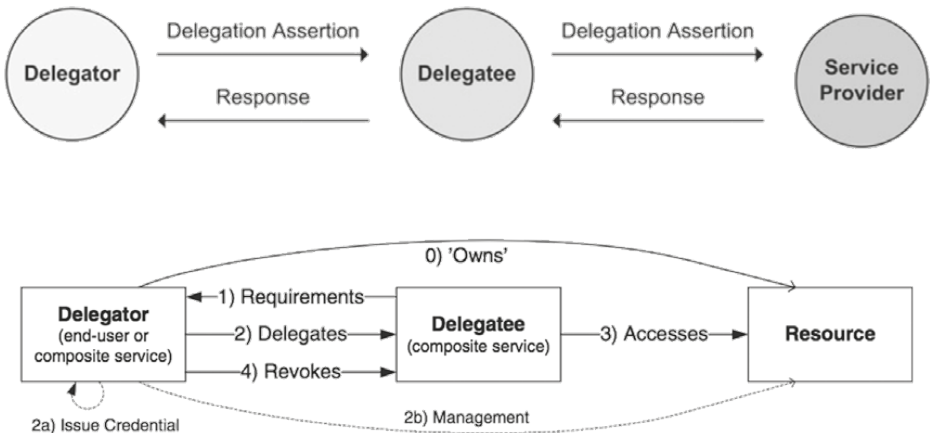


Figure 2.2. These two diagrams make clear different flows for delegators giving access to a service to a delegate.

the second service, they simply share a token to the first service to give them access. This is a safer way to give access without giving away the credentials (user name and password). However, it has limited use for these more sophisticated use cases with natural persons seeking to delegate access to their digital account to agents.

Some digital systems, like those related to education, support access by guardians to services related to their wards. The San Francisco Unified School district uses an online tool called School Loop to communicate to parents.⁸ However, the program only allows one parental account per student.⁹ This means that only one of two parents has access to the system. In families with co-parents who do not live together, this can pose challenges.¹⁰ It might also be the case that with blended families, there could even be four parents who might be involved in tracking things related to a child's education. It also cannot be assumed that children only have two legal parents; in British Columbia in 2013, they made it possible for children to have three parents listed on birth certificates if parenting agreements were signed ahead of time.¹¹

⁸ SFUSD (San Francisco Unified School District), "Student and Family Handbook 2016–17," 2016, <https://www.sfusd.edu/en/assets/sfusd-staff/parent%20resources/files/2016-2017%20SH-%20FINAL%20English.pdf> (p. 23).

⁹ Sarah Mei (@sarahmei), "Today's OH FFS SOFTWARE INDUSTRY: the @SFUnified saas for parents to track student progress can only issue one parent account per student," *Twitter*, September 6, 2017, 4:58 a.m., <https://twitter.com/sarahmei/status/905211153634148352>.

¹⁰ Sarah Mei (@sarahmei), "Or, I guess, you're assuming they're ok with sharing login credentials (which I wasn't even comfortable with when married, & less so now)," *Twitter*, September 6, 2017, 5:35 a.m., <https://twitter.com/sarahmei/status/905220451051249664>.

¹¹ The Early Edition, "1st Canadian Family with 3 Parents on Birth Certificate Grows," *CBC News*, February 9, 2015, retrieved from <http://www.cbc.ca/news/canada/british-columbia/1st-canadian-family-with-3-parents-on-birth-certificate-grows-1.2950107>.

In the domain of employee transactions, a special set of tools has been created to manage privileged accounts, administrative accounts for whole systems, and it has a lot of privileges. These types of accounts were used to commit large-scale fraud at some companies. Therefore, the US government passed new regulatory requirements. The Sarbanes–Oxley Act of 2002¹² requires that these types of accounts be managed/monitored in specific ways. “Privileged account management,” which does this, “lends out” the credentials to the privileged account to particular employees. It logs both who has access at particular times and what the privileged user does. There is currently very little consumer software that supports delegation and even less software that supports delegation to more than one agent.

Person-to-Entity Delegation Management in a Pre-Digital World

Just as with person-to-person delegation, legal paperwork is signed to give a corporation (that is a legal person) the permission to act on behalf of a grantor. Other institutions require this paperwork to allow transactions to take place on behalf of the grantor.

Gaps with Person-to-Entity Delegation in the Digital World

A technical protocol (OAuth) is a way to connect data belonging to a person to a set of services that person uses. New standards are being developed such as user-managed access (UMA)¹³ to support more complex use cases where individuals are pulling data from multiple sources/accounts to share with another entity to which they wish to provide the data. There are companies whose whole business is to fill an agency role for their customers. Banks hold our money and serve as our agents, acting on our behalf when we direct them to do things.

With the advent of digital systems and tools, individuals have the possibility to engage with digital agents who have permission to work on their behalf in a variety of contexts including digital markets. John Hagel III called these agents “customer-oriented infomediaries.” He says that “the early success of vendor-oriented infomediaries is likely to be undermined by the advent of technologies giving customers more control over personal information.”¹⁴

In “A Relationship Layer for the Web” (Figure 2.3),¹⁵ Bob Blakley¹⁶ outlines the challenge of the Internet where every relying party (business) needs to set up its own relationship with all the individuals it wants to interact with. This means that the vast majority of these relationships are weak and are costly to strengthen. The proposed solution to this dilemma is to designate parties whose job it is to know a lot about

¹² Sarbanes–Oxley Act. Pub. L. 107–204. 116 Stat. 745. July 30, 2002. <https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>

¹³ Kantara Initiative, “User Managed Access (UMA),” 2017, <https://kantarainitiative.org/confluence/display/uma/Home>.

¹⁴ J. I. Hagel and J. F. Rayport, “The New Infomediaries,” *McKinsey Quarterly*, no. 4 (1997): 54.

¹⁵ Bob Blakley, *A Relationship Layer for the Web . . . and for Enterprises, Too* (Midvale, UT: Burton Group, 2007).

¹⁶ Ibid.

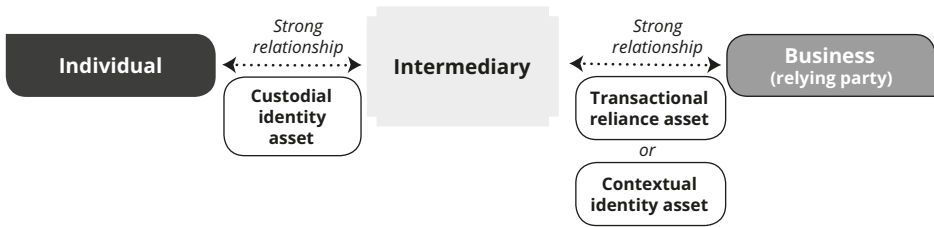


Figure 2.3. This figure shows how relationship intermediaries can use custodial identity assets, transactional reliance assets, and contextual identity assets to create strong relationships with both individuals and relying parties while meeting the needs of all parties.

individuals with whom they have a strong (ongoing) relationship as intermediaries, which can help connect individuals to relying parties and use their strong relationship to support higher confidence (trusted) interactions.

With the advent of new innovations in technology, personal assistants such as Alexa, Siri, and Google Home are acting as agents for individuals seeking to find information or make shopping lists. One can ask with a voice command for information or the answer to a question, and the agent works to find the information and answer. One can also attach different devices to the system and then turn them on or off with voice commands. These devices are run by sophisticated machine-learning algorithms that can listen to human speech, do natural language processing to figure out what an individual is actually asking for, and use that to find the information. This sometimes is called artificial intelligence (AI).

There are emerging legal questions about these devices and the agreements people make with the companies who create them. Concerns about privacy have also arisen, and some companies whose employees work at home are required to unplug them while on work conference calls.¹⁷

Gaps with Entity-to-Person Delegation in the Digital World

Entities in their incorporation paperwork outline which officers are authorized to sign contracts. After they grow larger, the board of directors articulates who these people are with resolutions. An entity delegates authority to a person to act on behalf of the entity just like the other forms of delegation with people signing paperwork.

As we learned above, corporations have systems to manage privileged accounts and also to support those who have signing authority on their behalf to do so digitally. There is a problem with how one actually signs contracts digitally. As we discussed above, there are a few jurisdictions that have state-issued eID cards that support both authentication, a proof of identity, and digital signatures. There is currently no card like this in the United States for residents. There are, however, companies like DocuSign that provide signature keys and digital signature services to their customers.

¹⁷ Bob Blakley, personal communication with the author, October 6, 2017.

3. Government Registration

Most individuals' first identity-related event with an institution occurs when parents register their child's birth (on behalf of the child) in a **government registration** process. Individuals also register with the government at other times in their life. These secondary government registrations include marriage and death, obtaining a license to drive, getting a passport, professional licensing, and registering to pay taxes or registering to vote (Figure 3.1). The first step is filling out registration forms once the government has accepted those and created a record in their systems they issue identification numbers and/or documents to the individual.



Figure 3.1. Government registration. The first instance of government registration is when (1) parents register their children at birth. In return, they are (2) issued a birth certificate for identification. Other secondary registrations require a birth certificate in the registration process, and identification such as driver's licenses and passports are issued to the individual.

Roles

- Individual/citizen/resident
- Government departments
 - Census takers
 - Social Security Administration
 - Birth registrar
 - Department of Motor Vehicles
 - Medical professionals involved in the birth process

Examples of Transactions

- Registering a birth
- Amending a birth record
- Registering with the government after birth for other things
 - Driving
 - Voting
 - Pension and other benefits contributions
 - Tax payment and tracking
 - Marriage
 - Divorce
 - Change of address

Sources of PII

- Assertions
- Reference documents issued by the government
- Government-issued documents issued in the process
- Documents from interacting with other organizations like utilities

Types of PII

- Name of individual
- Name of parents
- Birth date of individual
- Birth dates of parents
- Location of birth
- Location of birth of parents
- Date of marriage
- Date of divorce
- Name of medical professional or other witness of birth
- Number of the certificate issued at birth
- Current address of residence

Relationship to Other Domains

The first identity interaction people have with the state is when their parents register their birth with the state. This is an example of you and my identity where the parent is working on behalf of the organization. When the individual as an adult completes secondary registration with the state, they do so acting on their own behalf, in an example of me and my identity (while presenting the documents that originated from that first you and my identity transaction that lead to the birth certificate being issued to them).

Government registration is required before performing many government transactions that require identifiers and proof of claims that these registration processes produce. Many civil society registration processes also require proofs of claims that government registration requires. Commercial entities doing high-value transactions, restricted transactions (buying tobacco or alcohol), or transactions under regulatory requirements also need these proofs of claims from governments before individuals can register. Employers often require that employees provide proofs of various claims and particular government-issued identifiers to support taxation.

How Do Citizens Get Registered with the State?

When a child is born, parents usually register that child with the state through a process that involves filling out a birth registration form that is sent to a state birth registry, which issues a birth certificate. Birth registration is the official recording of a birth by the state. Modern nation-states establish citizenship via parents' citizenship or via the location of the child's birth. Birth registries publicly acknowledge an individual's existence. They also provide the basis for states to provide services to their citizens.¹

The birth registries are part of larger civil registry systems that form the foundation for governments collecting statistics about their populations and support planning for a variety of purposes.²

¹ Wendy Hunter and Robert Brill, "Documents, Please': Advances in Social Protection and Birth Certification in the Developing World," *World Politics* 68, no. 2 (2016): 191–228. doi:10.1017/S0043887115000465.

² Ibid.

Why Are People Registered with the State?

State practices that seek to register and enumerate people at various points in their life, (birth, census, death, etc.) shape both the state itself and its power as well as influencing how people in those states see themselves. States used personal identity documents to control their populations. They determined who a citizen was and who a foreigner was and even managing migration within countries. These registers were first used to help the state understand their population, but they also shape how the people see themselves.³

What Are Contemporary Birth Registration Processes?

In the United States, when a child is born in a hospital, before the child leaves, a form is filled out. The short form is seen by the parents and has approximately 37 questions; the long form is filled out by the hospital and has about 87 questions, requesting a lot of details about maternal care. It is used to inform health policies. There is a standard form across the United States.

In the United States, state laws require birth certificates to be completed for all births, and federal law mandates national collection and publication of births and other vital statistics data. The National Vital Statistics System, the federal compilation of this data, is the result of the cooperation between the National Center for Health Statistics (NCHS) and the states to provide access to statistical information from birth certificates.⁴

Some have studied the practices regarding how birth certificate information was collected and have found significant variance.⁵

Birth certificates are not just static. They are changed for a variety of reasons. These include adoption of various types (new two- and single-family parents, step-parent, family), court-ordered paternity, and voluntary declaration of paternity.⁶

The birth certificate becomes a document that is essential for other forms of government registration (SSN, driver's license). It is commonly referred to as a breeder

³ David Kertzer and Arel Dominique, *Census and Identity: The Politics of Race, Ethnicity, and Language in National Censuses* (Cambridge: Cambridge University Press, 2002).

⁴ Sally Northam, Shea Polancich, and Elizabeth Restrepo, "Birth Certificate Methods in Five Hospitals," *Public Health Nursing* 20, no. 4 (2003): 318–27. doi:10.1046/j.1525-1446.2003.20409.x. Quote from: Department of Health and Human Services (1998). Vital Statistics of the United States. Technical Appendix from 1998 Natality. Hyattsville, MD: CDC.

⁵ Ibid.

⁶ Jeffrey Duncan, Scott P. Narus, Stephen Clyde, Karen Eilbeck, Sidney N. Thornton, and Catherine J. Staes, "Birth of Identity: Understanding Changes to Birth Certificates and Their Value for Identity Resolution," *Journal of the American Medical Informatics Association* 22, no. e1 (2015 [2014]): e120–e129. doi:10.1136/amiajnl-2014-002774.

document, but I prefer the term that Chango⁷ uses. He calls it an “identity primitive,” referring to the core information that is on the certificate.

The practice of enumeration at birth began in 1987, which let parents apply for their children’s SSN when they apply for their birth certificate.

The Purpose of Identification Numbers and Their Usefulness

Identification numbers are issued by institutions to track people and things. Birth certificates do not issue individuals numbers, but the certificates themselves are numbered. Numbers issued to people in large administrative systems serve as indexes. They point at particular people. They are useful from a state’s perspective to be able to look up the citizen they are interacting with and be able to track ongoing interactions.

The Social Security Administration (SSA) issues SSNs in the United States. When this system was invented in 1935, it was created to give every worker a number to share with their employer to track deductions being made for their future pension. It was all tracked with punch cards. The SSN is a low-integrity identifier because few organizations using it have the ability to confirm or deny whether the number they are given is the number issued by the SSA to the person who is supplying them the number.⁸ However, there are some significant challenges with high-integrity identifiers.

Any high-integrity identifier represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the state and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-Utopian novelists. The highest-integrity scheme combines physically intrusive data-collection with a potentially ubiquitous inhabitant of power.⁹

The Indian Aadhaar system creates one that issues a 12-digit number (11 random digits with a check digit) to citizens. It enrolls citizens by taking 13 biometrics so that no resident can be given two numbers. The privacy risks and implications of a system that tracks activity across all uses of the number are huge. To learn more about this system, I strongly recommend Pam Dixon’s article.¹⁰ Inspired by Pam’s on-the-ground research in India, I had the opportunity to travel there as a New America India-US

⁷ Mawaki Chango, “Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity,” PhD dissertation, School of Information Studies (2012), https://surface.syr.edu/it_etd/74.

⁸ Roger Clarke, “Human Identification in Information Systems: Management Challenges and Public Policy Issues,” *Information Technology & People* 7, no. 4 (1994b): 6–37, <http://www.rogerclarke.com/DV/HumanID.html>.

⁹ Ibid.

¹⁰ Pam Dixon, “A Failure to ‘Do No Harm’: India’s Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.,” *Springer Nature, Health Technology*. doi: 10.1007/s12553-017-0202-6. <https://techscience.org/a/2017082901/>.

Public Interest Technology Fellow. I wrote “Key Differences between India’s Aadhaar System and the US Social Security Number System.”¹¹

Some scholars have noted that “contemporary biometric identification practices [are] part of a chain of transnational governance techniques that originated in the colonies.”¹² This includes the first known usage of fingerprinting by the British in the colonial center of Bengal as a means of identification.

What Are Alternatives That the Digital Technologies Provide to One Number?

The province of British Columbia in 2008 needed to figure out how to fix its health insurance system. There were four million residents of the province and nine million health insurance cards that had been issued.¹³ Sure, some of them were replacements for lost cards, but many were fraudulent, identifying nonexistent citizens of the province. Because health care is universal, everyone was paying for health care for the frauds. A solution was needed.

The province had a program-based approach to identity such that each agency offering a service did its own establishment of identity and a management of that identity of a citizen. This also was largely paper-based.¹⁴ The province already issued drivers licenses with photos. It couldn’t afford to reenroll its entire population in a health care card with a photo. One way to solve this problem is to issue one card with one identifier for both systems—the driver’s license system and the health care system. But that introduces new risks. They are two very different systems. Governments should not have an “uber” file with all of a citizen’s transactions with different departments in one place.¹⁵

So the province worked diligently to figure out an underlying technical architecture to allow it to issue one citizen services card that would serve as both a driver’s license and a health care card but with a very interesting property enabled by the underlying architecture. It would behave differently depending on the context where it was used. It was polymorphic. The province designed a system that was triple blind: the

¹¹ Kaliya Young, “Key Differences between the U.S. Social Security System and India’s Aadhaar,” *The Promise of Public Interest Technology: In India and the United States*, *New America*, 2019, <https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/key-differences-between-the-us-social-security-system-and-indias-aadhaar-system-kaliya-young/>.

¹² Elida K. U. Jacobsen, “Unique Identification: Inclusion and Surveillance in the Indian Biometric Assemblage,” *Security Dialogue* 43, no. 5 (2012): 457–74. doi:10.1177/0967010612458336.

¹³ News 1130, “BC Begins Phasing Out Care Cards Soon,” January 7, 2013, <http://www.news1130.com/2013/01/07/bc-begins-phasing-out-care-cards-soon/>.

¹⁴ Peter Watkins, “Trust and Identity Management: Experience and Perspective from the Province of British Columbia, Canada,” *Trust Conference: e-Government Identity Management Initiatives*, The Hague, Netherlands, November 21, 2007, <http://www.llbc.leg.bc.ca/public/PubDocs/bcdocs/437299/BCPaperTrustandIdentityManagement.pdf>.

¹⁵ *Ibid.*

card has a chip in it. It is first authenticated as an “active card” in the system. Then it accesses a totally different system with information about the person and then accesses again into whatever the context is. Thus, if one is being stopped by a police officer, the card accesses the driver’s license record system. If one is going to the doctor, and presents it in the third step, it hops over to the health care system. There is a different identifier for each system, so presenting the card in one context does not leak information from that context into another.¹⁶

Identity Required to Get Identity Documents?

The International Civil Aviation Organization (ICAO) worked hard in developing the standards for international passports. Machine-readable travel document (MRTD) standards were developed to reduce the ability of fraudulently creating passports. Naturally, fraud shifted to creating documents needed to actually obtain a passport. It is for this reason that the ICAO’s attention shifted to considering what the standards should be for “trusted evidence of identity”¹⁷ and for pushing countries to standardize their whole birth registration and vital records process.

ICAO is very clear that the concept of “identity” used in their paper about standards for trusted evidence of identity¹⁸ denotes a unique identity (identifier) used to represent a person within and across nations:

Evidence of Identity - EOI refers to the types of evidence that, when combined provide confidence that the individual is who they claim to be (e.g., a driver’s license, passport or birth certificate). Generally, the more evidence an applicant can provide, the higher an agency’s confidence that the identity is genuine and belongs to the presenter - particularly if evidence can be validated at the source.

Credential - Physical representation of an identity, the documentation part of evidence of identity (EOI) that is issued to and kept by an identity claimant. It can be a foundational document or a supporting document.

Identity Register Record - Records in the repository of identities for different entities providing reference for checking of a Credential.

To connect this to the above narrative: people get a credential issued to them, a birth certificate, and the fact that a certificate was issued is also recorded in an identity register. There is no enrollment of any authentication factors.

¹⁶ Zack Martin, “British Columbia Issues Combined ID for Driver License, Health, Online Use,” *SecureIDNews*, June 5, 2014, <https://www.secureidnews.com/news-item/british-columbia-issues-combined-id-for-driver-license-health-online-use/>.

¹⁷ Bian Yang, Christoph Busch, Julien Bringer, Els Kindt, Willem Ronald Belsler, Uwe Seidel, Edward Springmann, Uew Rabeler, Andreas Wolf, and Magnar Aukrust, “Towards Standardizing Trusted Evidence of Identity,” in *DIM ’13: Proceedings of the 2013 ACM Workshop on Digital Identity Management*, ed. Thomas Groß and Marit Hansen (New York: Association for Computing Machinery, 2013), 63–72. doi:10.1145/2517881.2517890.

¹⁸ Ibid.

ICAO developed a working paper with three principles of how to achieve a high confidence that the person applying for a document is eligible for the document:

1. The identity exists—that it is not fictitious and not from a deceased person.
2. The identity claimant is linked to the identity.
3. The claimed identity is actually used by the identity claimant.

The International Commission on Civil Status (ICCS) outlines what a birth certificate should contain. Proposals are being made to standardize security features of these documents and ways to look them up in identity registers.

We are still left with the challenge as Bohm articulates, “The most basic of documents, the birth certificate, does not provide evidence that the holder of the certificate is the person whose birth is recorded in it.”¹⁹

ICAO has continued to develop standards for passports and has pushed for radio frequency identification chips to become standard in passports.²⁰

What Role Do Biometrics Play in Government Registration?

The National Academies’ report on the topic defines biometrics as “[t]he automated recognition of individuals based on their behavioral and biological characteristics.”²¹ It refers to technologies that allow for measuring, analyzing, and processing biological characteristics that are unique, such as fingerprints, retinas, irises, facial patterns, hand geometry, and body odors.²²

Like other more traditional identity systems, the procedure of biometric identification consists of four stages:

Enrollment (digital representations of unique biological features are captured through a sensor device, and then processed through an algorithmic operation to produce a “[reference]”),

Storage (the produced [reference] is stored on a database or/and on a chipboard),

Acquisition (as with the enrollment stage, a biometric image is captured and transformed through similar algorithmic procedures into a [sample]), and

¹⁹ Nicholas Bohm, and Stephen Mason, “Identity and Its Verification,” *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 1 (2010): 43–51. doi:10.1016/j.clsr.2009.11.003.

²⁰ Shivani Kundra, Aman Dureja, and Riya Bhatnagar, “The Study of Recent Technologies Used in E-Passport System,” in *2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS)* (Trivandrum: 2014), 141–46. doi:10.1109/GHTC-SAS.2014.6967573.

²¹ Lynette I. Millett and Joseph N. Pato, eds., *Biometric Recognition: Challenges and Opportunities* (Washington, DC: National Academies Press, 2010).

²² Btihaj Ajana, “Asylum, Identity Management and Biometric Control,” *Journal of Refugee Studies* 26, no. 4 (2013): 576–95. doi:10.1093/jrs/fet030.

Matching (the [sample] is compared to the stored [reference] to establish whether the person is known to the system)²³

There are many issues with biometric identification systems and processes that need to be carefully considered.

Enrollment and Authentication, They Are Different

Enrollment is the process where a person first engages with a system and a row in an index database is created for that person—a number is issued to them. Technically, it points at them, and they can use it to support the institution being able to reference their records or files in the future.

If an individual wants to return to “prove” that they are the same individual who originally enrolled, they need ways to prove or “authenticate” that they are indeed the same person. Therefore, factors of authentication must also be defined.

There are three broad categories of authentication factors:²⁴

What You Know: Passwords, PINs, answers to questions like “What is your pet’s name?”

What You Have: This is a thing that you either have or is given to you that you present again. It can be a number that you are given. It can be a physical card that you are sent. It could be your phone so the bank sends a special code to your phone that you enter.

What You Are: These are biometrics one has to actually enroll to be able to check against them. When an individual first gets a driver’s license, they have their picture taken. If they lose their driver’s license, they go to the Department of Motor Vehicles (DMV) and say they lost it. The DMV can look up their name (an indexical identifier in their database, “who they say they are”) and see if the picture in the database matches the person standing before them—they authenticate the individual standing before them against the picture they have of the individual that was enrolled in the system when they first got a license.

New authentication factors include:

What You Do: These are behavioral biometrics such as how you type. This type of authentication factor has to be enrolled so that a pattern presented can be matched against a known behavioral pattern of the subject.

Where You Are: This is geolocation. If an individual is at a bank asking to take out money and they give the bank permission to use the individual’s geolocation via the phone location, they can check if the individual is next to the bank and use this to authenticate them.

As noted earlier, the SSN system is a low-integrity identifier in part because there is no process to enroll factors of authentication that are linked to the number. The SSN

²³ European Commission, *Biometrics at the Frontiers: Assessing the Impact on Society* (Brussels: European Commission, 2005), <https://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf>.

²⁴ Maryline Laurent and Samia Bouzefrane, *Digital Identity Management* (London: Iste Press, 2015).

is not a network endpoint under the control of the individual. A phone number and an email address are network endpoints. When you claim you are the person with a particular number or email address, an entity can ping the endpoint and ask you to prove you received the message and thus that you indeed are in control of the endpoint. (*Please note: individuals do not own their phone numbers; they rent them from the phone company. Individuals who get email services from a major service provider, such as Gmail, do not own their email addresses.*) This is not the case with an SSN. If you “fixed” the SSN system by enrolling factors of authentication and then used those every time you shared your SSN, the government would know all the places where you were using the number because it would provide the authentication service.

If Not Registered at Birth, How Can Registration Happen?

Not all people have their births registered at the time of birth. There is a growing international focus on the issue, and the World Bank estimates that up to 1.8 billion people on the planet today were not registered at birth.²⁵ Thus, figuring how to register people to support them having a legal identity is critical. The World Bank has an Identity for Development (ID4D) program.²⁶

A great example of a country that has focused on registering everyone is Peru. They faced a challenge resulting from a long civil war with the Maoist Shining Path guerrillas who as part of their effort to control rural populations proactively destroyed rural citizens’ paperwork. They invested in outreach to make sure that all citizens were included, and today they have 98 percent of the adult population registered.²⁷

Identity for Development and Birth Registration Challenges

Today, one-third of all children born in the developing world do not have their births registered.²⁸ One-half or more of the world’s population lives in countries that have no effective national universal system of birth registration.²⁹

²⁵ Mariana Dahan and Alan Gelb, “The Role of Identification in the Post-2015 Development Agenda,” World Bank Working Paper, 2015, <http://pubdocs.worldbank.org/en/149911436913670164/World-Bank-Working-Paper-Center-for-Global-Development-Dahan-Gelb-July2015.pdf>.

²⁶ World Bank Group, *Identification for Development: Strategic Framework*, January 25, 2016, <http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf>.

²⁷ William Reuben and Flávia Carbonari, “Identification as a National Priority: The Unique Case of Peru,” Center for Global Development Working Paper 454, 2017, <https://www.cgdev.org/sites/default/files/identification-national-priority-unique-case-peru.pdf>.

²⁸ Mia Elizabeth Harbitz, “The Civil Registry: A Neglected Dimension of International Development,” Inter-American Development Bank, Knowledge and Management Sector, Technical Note, May 2013, <https://publications.iadb.org/publications/english/document/The-Civil-Registry-A-Neglected-Dimension-of-International-Development.pdf>.

²⁹ Simon Szreter, “The Right of Registration: Development, Identity Registration, and Social Security—A Historical Perspective,” *World Development* 35, no. 1 (2007): 67–86. doi:10.1016/j.worlddev.2006.09.004.

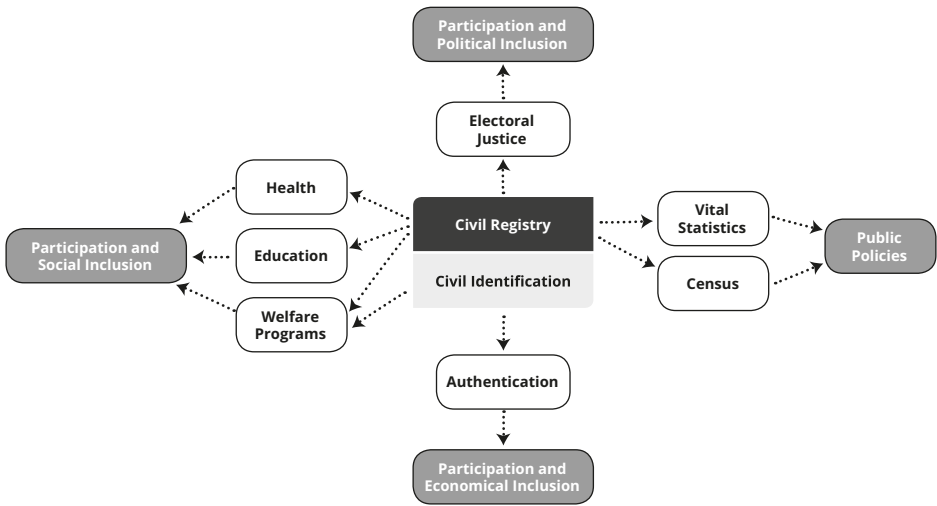


Figure 3.2. Conceptual model of civil registration and identification.

Derived from Figure 1 in Harbitz, and Arcos, "Identification and Governance Policies."

Research points to a correlation between birth registration and better outcomes for citizens because they can access services with the official documents (birth certificate) that come with registration (Figure 3.2).³⁰

Legal identity, often rooted in a formal birth certificate, is required to access economic opportunities in the formal economy. There are a whole range of challenges that some of the literature suggests will be solved in a sweeping way, if people just have a legal identity that is a birth registered with the state and a certificate to say so. These include the prevention of child marriages, preventing child labor, enabling inheritance and preventing dispossession, reducing statelessness, supporting greater punishment for crimes against children, having vital statistics, and health planning.

It is very clear from the academic work reflecting on the challenges that technology is not the main barrier or answer to making progress in increasing birth registrations and improving vital statistics systems, or supporting more people attaining secondary IDs like national ID cards that often require a birth certificate before they are issued.³¹

³⁰ Mia Elizabeth Harbitz and Iván Axt Arcos, "Identification and Governance Policies: The Legal, Technical and Institutional Foundations That Influence the Relations and Interactions of the Citizen with the Government and Society," Inter-American Development Bank, Technical Notes, September 2011, <https://publications.iadb.org/publications/english/document/Identification-and-Governance-Policies-The-Legal-Technical-and-Institutional-Foundations-that-Influence-the-Relations-and-Interactions-of-the-Citizen-with-the-Government-and-Society.pdf>.

³¹ Debra Ladner, Erik G. Jensen, and Samuel E. Saunders, "A Critical Assessment of Legal Identity: What It Promises and What It Delivers," *Hague Journal on the Rule*

There are a whole range of issues with obtaining a legal identity that are not solved with technology:³²

- (1) Financial barriers that can include standard fees, late fees, transportation expenses, time away from work, and bribes;
- (2) Burdensome procedures including for evidentiary requirements;
- (3) Discriminatory laws, practices, and attitudes that impact women, minority groups, and the poor. And on top of all of this, civil registration systems are often poorly managed, underfunded, and lack full time professional staff.

The reality is that only 10 percent of African countries and 50 percent of Asian and South American countries have complete civil registration systems capable of generating accurate vital statistics. What is clear is that birth certificates do not address institutional and cultural issues that lead to abuse and human rights violations.³³

In the marketplace of ideas, there is a claim that the lack of birth registration can be solved by companies that have businesses selling technology (smart cards, biometric readers, database technology) and consulting services to these developing countries. People with this perspective are being paid by development banks to articulate their strategies and educate governments with reports. One of the solutions proposed in the industry literature is to biometrically register every human being in giant databases. They see the Aadhaar program in India as successful and do not perceive any problems with the major privacy concerns raised by such systems. There is also an effort called ID2020 focused specifically on bringing digitally rooted self-sovereign-identities to very marginalized populations within states and to refugees who have left their own states.³⁴

What Are Alternatives to Government Registration Systems?

Modern states and their populations' perception of "belong to them" mutually evolved. As state systems in early modern Europe emerged, so did the systems to track and manage the people that were within these states. Over the last five hundred years, we have seen the systems we have today emerge slowly. It was not always this way (see the section "History to See the Future" for more details). We have not touched on it here, but it is worth noting that many developing world countries were occupied and ruled by European colonial powers, and part of that process was registering the population and defining who its subjects were.³⁵ Many of the countries where there is low birth registration were at one point colonies, and many of the people without legal identity paperwork are in countries that were once colonized.

Not all people trust their governments, or want to be registered by them, or see these systems as legitimate. As already noted, unlike many other services like health

of Law 6, no. 1 (2014): 47–74. doi:10.1017/S1876404513000043; Hunter and Brill, "Documents, Please."

³² Ladner et al. "Critical Assessment of Legal Identity."

³³ Ibid.

³⁴ ID2020 (2017): <http://www.id2020.org>.

³⁵ Jacobsen, "Unique Identification."

and education, only governments can register people into a government-run identity registry and issue identity documents to people based on their registration.

What Are Self-Sovereign Identity Systems?

Technical systems based on large distributed and shared database technology called blockchain are being used to develop a new kind of identity called self-sovereign identity. Some see this new form of identity as an alternative to government registration by proving a global registry of identity that exists in digital form. Organizations like ID2020 are looking at these new technologies to support a variety of marginalized populations such as (1) individuals who have no government documentation within their states and (2) refugees who have left their states.

This work is complementary to government registration. Governments could issue claims such as a proof of citizenship or identification to individuals with self-sovereign identities. It is worth noting that in the summer of 2017, the state of Illinois announced that it would pilot a program to issue birth certificates to citizens with the self-sovereign identity–shared ledger developed by the Sovrin Identity Foundation.³⁶

³⁶ J. Althaus, “Governments Eye Blockchain in Their Creation of National Identity Systems,” *CoinTelegraph*, October 6, 2017, <https://cointelegraph.com/news/governments-eye-blockchain-in-their-creation-of-national-identity-systems>.

HISTORY TO SEE THE FUTURE

When asked “What is your identity?” many people think of the physical documents issued to them by the state that have their names and other claims about them. These documents are part of almost everyone’s life and are referred to by those working on developing digital systems that function in similar ways to their physical identity documents. We take so many of these systems for granted, and we don’t even know why they came into being and what purposes they served originally. I believe that as we move into building digital systems for government registration and in other domains, understanding the past will help industry build better systems in the future.

What Are the Origins of These Practices?

In his thesis “Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity,” Mawaki Chango¹ examines “the modern state response to its need to control people and therefore to document the identity of individuals.” He looks at the origins of why and how they became the most common authoritative credential issued to people by governments. Chango defines an identity system as “a scheme that makes each and every individual a member of a given population consistently identifiable.”

It is always a challenge to decide where to begin a story like this. He has a good opening point, in medieval Europe around the turn of first millennium. This is admittedly a European centric view of identity, but it is this history and the practices that emerged over the next 1,000 years in Europe that lead directly to the systems of identity we have today and are used globally.

The Transition from Feudalism to the Church

In medieval Europe, a particular transition happened from feudal to church. Feudalism was the form of social organization based on fiefs, estate properties that were temporarily used for a fee by vassals (people) who were not landowners. There were rights and responsibilities that flowed from the landowners, lords, to their vassals. These rights and responsibilities were about a person’s position within the system and their personal relationships, not geography. There were no territorial borders and the political authority or institutions we have today. What existed was “the medieval church leveraged and built on the juristic legacy of the Roman Empire to establish a system of law and courts, ‘a kind of surrogated government’.”²

It was in this context that failing to meet a payment or contractual obligation became grounds for excommunication from the church. The “signing” of contracts

¹ Mawaki Chango, “Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity,” PhD dissertation, School of Information Studies (2012), https://surface.syr.edu/it_etd/74.

² Ibid.

was carried out during a ceremony that involved sealing the agreement under oath taken over some sacred item. Contracting was “a sacred commitment.”³

It was at this time that the authority of monarchs also arose, and they asserted power with the seals that were seen as “an earthly sign of supreme authority.” Kings began to use more than one type of seal for different types of transactions. Commoners also began to use seals as identity tokens. The seal was an attestation not just of the owner’s identity but also of his intent to stand behind the contents of the document.

The First Corporations Are Developed

It was also in this time that the idea of the corporation developed. A collective of individuals could have autonomy, agency, and the status of a legal person. They defined their own rules for who could be a part of their collective. Those who were able to act on behalf of the corporation needed to have the seal of the corporation. The legal status and privilege thus came from the seal and the ability to act on the corporation’s behalf. This ability to work on a corporation’s behalf was touched on in the you and my identity domain.

What Are the Origins of States (Governments)?

Can you have identity documents from governments without governments? Not really. Thus, although it may seem like a tangent, it is important to note the fact that the creation and emergence of nation-states in the last 500 years and the evolution of how the people who reside within those boundaries perceive themselves as being from those states is a reciprocal process.

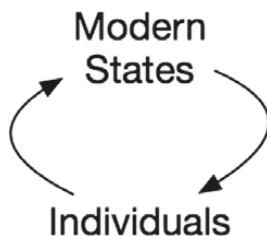


Figure 11. The relationship between modern states and individuals. The recursive relationship between individuals, their citizenship, and modern states. Modern states have processes and system of registration of the individuals within their borders. When people are “seen” by the state as citizens of the state, they form an identity as citizens of the state.

³ Ibid.

The formation of the modern state became intertwined with the emergence of the nation as formative of a quality or attribute of individuals, in other words, the emergence of the concept of nationality [...]. Nationality is the locus of reciprocal processes whereby the state “naturalizes” itself as a nation while (the people) are ascribed to the institution of the state. The transition towards the territory as the ultimate basis and one of the primary determinants of the authority to define the configuration of obligations and rights, in opposition to personal ties as we previously saw in the early feudalism, also signifies that impersonal procedures had to be put in place to reflect and sustain a similar mode of affiliation. It requires objective facts for instance “place of birth.”⁴

The processes of impersonal procedures are taken for granted but lay the foundation for government registration.

Citizens register with sovereign governments of nation-states and these governments confer on them identities as citizens. It is worth noting that government credentials are unique because they come with sovereign immunity for reliance failures. This means that if a government-issued ID is presented and it turns out to be fraudulent, you can't sue the government. Therefore, if a business can use a government identity document rather than issue them, it doesn't have to worry about being sued for a fraudulent identity document which it issued.⁵

What Are the Origins of Identity Papers?

In the first part of his thesis, Chango wrote about the emergence of seals and signing. These records were not kept by a central authority. However, the church was a key political force at the time, and they kept lists of who was a believer and if they had fulfilled their duties. The church was managing records for the courts.

Military regiments were managed with registers to monitor soldiers, subcontractors, and mercenaries, claims of service, and payment. “In 1462, Louis XI issued regulations that required all soldiers on leave to carry a document made out by their superior, bearing their name and confirming their proper discharge.”⁶

There was also a profession of courier that enabled and harnessed the mobility of written records emerging in this time. The king issued an order requiring that

⁴ Ibid.

⁵ Bob Blakley, personal communication with the author, November 16, 2017.

⁶ V. Groebner, “Describing the Person, Reading the Signs in Late Medieval and Renaissance Europe: Identity Papers, Vested Figures, and the Limits of Identification, 1400–1600,” in *Documenting Individual Identity*, ed. J. Caplan and J. Torpey (Princeton, NJ: Princeton University Press, 2001), 15–27.

identity papers known as “passports” be issued and handed to the couriers in sealed envelopes. As they traveled through border checks, their passports would be opened and then stamped and resealed until they arrived at their destination.

Municipalities keep registries to track people too. Cultural practices meant that some people fell below the “threshold of citizen’s right,” in particular, transient citizens.

It became an obligation during this time for people away from their residential location to bear travel documents that identified them, issued by authorities in their home towns.

The regimen of travel papers became an instrument of subjugation, control, and harassment. “The regime of identity papers it enforced had come to symbolize an arbitrary and bureaucratic coercive state.” The revolutionaries in “1789 abolished the royal passport of 1623 and 1699 and proclaimed that every citizen had the right to come and go as he or she pleased.” This didn’t last long, and a new passport legislation was passed in 1792 along with the establishment of the “état-civil.” This required individuals to register with the state rather than with the church. This change meant that everyone was included regardless of religion. With this centralized administrative registration, identification became the foundation of what we now see as modern citizenship in contemporary nation-states.⁷

What Are the Origins of Birth Registration?

In 1538, a nation-wide system for the registration of all births, deaths, and marriages was started at the parish level of the Church of England in the United Kingdom. The originator Thomas Cromwell explained its utility this way:

for the avoiding of sundry strifes, and processes and contentions arising from age, lineal descent, title of inheritance, legitimation of bastardy, and for knowledge, whether any person is our subject or no.⁸

The registry facilitated the workings of a legal system, endowing ordinary individuals with their identities and enabling them and their families to exercise their property and other rights.

The parish register system, argues Simon Szreter,⁹ was critical to actually sustaining the political and legal credibility of the comprehensive social security system of the

⁷ Chango, “Becoming Artifacts.”

⁸ E. Higgs, *The Information State in England: The Central Collection of Information on Citizens since 1500* (Basingstoke: Palgrave Macmillan, 2004).

⁹ Simon Szreter, “The Right of Registration: Development, Identity Registration, and Social Security—A Historical Perspective,” *World Development* 35, no. 1 (2007): 67–86. doi:10.1016/j.worlddev.2006.09.004.

Poor Laws. This, in turn, was important in ideologically legitimating the practices of an expanding market economy and providing it the means to address serious social problems of disruption caused by market growth.

Szreter makes a lot of compelling arguments about how this combination of registration, the laws requiring support for the aged, poor, disabled, and widowed, enabled the emergence of the market economy in the United Kingdom. The market, in quite a few ways, including the ability to clearly register who owned what land and which companies, along with specifying who is able to participate in a legal system that resolved disputes, was enabled by these identity systems.

It is worth noting that when the colonists came to the first American colonies, they were accustomed to these practices, and in 1639, Massachusetts began recording births.¹⁰

How did We Get to Universal Birth Registration?

The first child labor laws were passed in the 1870s in Wisconsin, and 20 years later, the laws had not been enforced. The problem was that children's ages were basically impossible to determine.¹¹ Between 1900 and 1940, reformers were active in lobbying to eliminate affidavits from parents attesting to the age of their children as acceptable "proof" of age.

The solution to the problem of enforcing child labor laws was, ironically, to shift the authority to authenticate a child's birth away from the people who had actually witnessed it—the parents. Professionally produced, birth certificates objectified child's age and identity making a truth that existed apart from the personal relations that created the child.

Reliance on birth certificates and other "documentary evidence" to establish the numerical age was part of a much larger shift in authority from families to the state and from personal, testamentary knowledge to written documents. This transition was, in other words, part of the bureaucratization, standardization, and quantification of information that accompanied modernization in the United States. Modern management techniques privileged writing and documents over the oral and the transient.¹²

¹⁰ H. L. Brumberg, D. Dozor, and S. G. Golombek, "History of the Birth Certificate: From Inception to the Future of Electronic Data," *Journal of Perinatology: Official Journal of the California Perinatal Association* 32, no. 6 (2012): 407–11. doi:10.1038/jp.2012.3.

¹¹ S. J. Pearson, "'Age Ought to Be a Fact': The Campaign against Child Labor and the Rise of the Birth Certificate," *Journal of American History* 101, no. 4 (2015): 1144–65. doi:10.1093/jahist/jav120.

¹² Ibid.

This change was not inevitable. It happened because a group of social reformers worked on changing the “meaning of chronological age and the social power of documents.”¹³

The Census Bureau developed a standardized form for the recording of live births in 1900, and by 1930, the standard form had been adopted by all the states. During World War II, birth registration was emphasized as proof of citizenship and it was needed to be eligible for employment. At this point, the birth registry and birth certificate had two purposes: one for epidemiological data and a legal document determining citizenship.¹⁴

¹³ Ibid.

¹⁴ Brumberg et al. “History of the Birth Certificate,” 407–11.

4. Government Transactions

Once an individual has been formally registered with the government and an identifier has been issued (a number in a government database that points at a particular person), the individual can use this number to do a **transaction with government**. For example, a transaction is the payment of taxes using the identifier issued (in the United States this is an SSN). These two types of interactions (registrations and transactions) with government are often thought of as the same, but they are quite different. For the most part, one needs to be registered with the government before transacting with it. Individuals present identification to their government and are able to transact with or receive services from the government.



Figure 4.1 Government transactions. The subject (1) presents identification to the government (issued to them by the government in a registration process) and in return (2) they are able to receive services.

Roles

- Citizen/resident
- Government identity provider
- Government agency
- Police

Sources of PII

- The individual
- Government-issued identity documents
- Credentials issued by organizations (professional licensing)

Examples of Transactions

- Paying taxes
- Crossing a border
- Receiving a pension
- Paying into a pension
- Collecting a government benefit (home loan, Medicare payment, etc.)
- Transactions through a hub between a private identity provider and a government agency

Types of PII

- Government-issued identifier (SSN (United States), Aadhaar number (India), Social Insurance Number (Canada), National ID)
- Name
- Address
- Information relevant to the service/transaction

Relationship to Other Domains

Before conducting many types of transactions with government, one needs to have gone through a government registration process. The government makes records of some transactions available publicly and data brokers can collect the information and use it. The data generated by transactions are also vulnerable to theft and use on the illicit market.

Detailed Description and Relevant Literature

The previous domain, *government registration*, reviews the evolution of contemporary practices that governments use to register their citizens and residents. Governments in the registration process, and particularly with birth registration, become the attribute provider for individuals. The registration in a registry of births and the associated birth certificate that corresponds to this is the authoritative source (the county government) of an individual's birth date, name and parent's names, and location of birth. Thus, the government "provides" this identity attribute to the individual. The location of birth determines citizenship status; if it is in the United States, they are citizens; if it is outside of the United States, they are not citizens unless they present other evidence.

When individuals present themselves to access government services and transact with the government, they require this attribute (birth date, place of birth) from an authoritative source (county vital statistic registry) in a trustworthy form (on a birth certificate) before proceeding. This attribute is also required for secondary registration processes with the government such as getting a driver's license, SSN, and passport. In doing this, one department or arm of one level of government is an "attribute provider" or "identity provider" to another government department that relies on the information and is a "relying party."

The pattern of one part of government relying on key registration documents and attributes from another part of government is repeatedly seen. It needs to be addressed to support these systems working well. Certain specific agencies do very particular registration processes producing very particular identity registries and corresponding documents.

Many departments providing services rely on these documents to support their interaction with citizens, residents, and subjects. Given our current technology, most of the time this reliance is rooted in the observation of the physical version of documents such as driver's license, passport, and birth certificate; and much of the time a claimant can just self-assert attributes like birth date and SSN.

In the United States, with so many different government departments and services, one must often present proof of some form of government registration before one interacts with a government department. In the United States, with so many different government departments and services, one must often present proof of some form of government registration before one interacts with a government department, failing which one will be directed to the appropriate agencies to obtain it. This requirement to present documentation to affirm proper registration affects people seeking social services when they are released from prison. With new requirements to have identity documents to get other identity documents, people can end up in some catch-22 loops.¹

¹ Amy Blank Wilson, "It Takes ID to Get ID: The New Identity Politics in Services," *Social Service Review* 83, no. 1 (2009): 111–32. doi:10.1086/599025.

What Are Typical Transactions with Government?

Transactions indicate that one is interacting with the government; examples include:

- (1) Receiving a benefit requires proof of eligibility;
- (2) Crossing a border which requires a passport;
- (3) Registering for government services such as public assistance;
- (4) Submitting government pension contributions and receiving pension benefits;
- (5) Paying taxes; and
- (6) Using any license that was issued by a government.

What Is the Difference between Registering for Primary Identifiers and Subsequent Registrations with Agencies One Is Interacting With?

Government agencies require individuals to have identity documentation from a registration process, and the associated numbers assigned in those processes (SSN, driver's license number, passport number), before they will interact with an individual because the documentation is seen as proof of identity.

When first presenting to an agency, one presents identity documents and goes through an agency-level registration process. How many agency-level registrations might a person go through? States have many different social service agencies; for example, Texas has 200.² Each has its own record of clients. After initially registering with an agency, one presents information to support the agency connecting to the individual again in ongoing interactions.

Often, agencies use an SSN as an index to be able to look up individuals when they subsequently present to the agency. States were long free to use this number in this way. However, in 1990, the federal government amended the Social Security Act to bar the disclosure of SSNs collected by federal, state, and local governments pursuant to any laws enacted on or after October 1, 1990. In 2010, 10 states enacted legislation or passed resolutions regarding the use and regulation of SSNs.³

Government agencies often use the name written on people's documents (the ones they received in the registration process) and the birth date also found on these documents. Together, one's name and birth date serve as the key indexes that are used to locate one's records with an agency when one presents again.

Can Individuals Sign Documents in These Transactions?

Agencies will also ask individuals to sign documents in various processes. This is often done with a physical signature. There are very few systems globally that allow

² S. Erp and A. Bennett, "Presentation: A State Government Perspective: Cybersecurity and People," 2017, MSIMS Class.

³ NCSL National Council of State Legislatures, "Social Security Number 2010 Legislation," 2010, <http://www.ncsl.org/research/financial-services-and-commerce/social-security-number-2010-legislation.aspx>.

individuals to log on with an official government-issued identifier and even fewer that support individuals actually doing “digital signatures.”

What Is the History in the United States around Requiring SSNs, Followed by the Shift to Stop Using Them?

The SSN, when originally issued to citizens in 1935, was just for supporting the collection and administration of social security—paying into the system and receiving benefits. In 1943, the IRS began using it for tracking people paying taxes. In the following decades, more and more agencies began using it. By the early 1970s, concerns arose about its use in so many different agencies. In 1976, states were authorized to use the SSN for tax purposes, public assistance, and for driver’s license or motor vehicle registration. A number of states used the SSN on the driver’s license; this is no longer permitted.⁴

What Role Does Authentication Play in Supporting Individuals Transacting with Governments?

There is a difference between authentication and enrollment or registration. To interact with services in person, authentication processes happen implicitly, so we often never think about them or understand they have actually happened. If one is asked for a driver’s license, the person asking for it checks to see if your face matches the one on the document. They also use the name and other information like birth date to look you up in their records. A presenting individual knowing of this information is often enough evidence that they indeed are the person they claim to be.

Standardized electronic identity issued by the government does not exist in the United States. SSNs are not network endpoints and cannot be authenticated against.

A network endpoint is an address where a message can be sent. Examples include a phone number (a call can be placed to it or a text message sent to it), an email address (an email can be sent to it), and a physical mailing address (a letter can be sent to it). The government or an employer who knows your SSN cannot “send you a message” using the number. It is just a number that points at you; it isn’t an address for you like the other types of identifiers.

Several issues are created because SSNs are not network endpoints. It is hard to prove a particular individual is indeed the person to whom a particular SSN points. When an individual enters a certain email address in a website, the website will often send a message to that address asking you to click on a link to prove you are in fact the person in control of that address. Another example is enrolling a phone number with an online bank. They often do a test to check that you are indeed the person with that phone number by sending a short message with a “code.” If you know the code they sent, then you must be the person who has that phone number. You cannot do this with an SSN.

When government departments have an SSN for an individual and want to communicate with them, they have to ask for network endpoints such as phone numbers, email addresses, and mailing addresses.

⁴ Kenneth Donaldson Meiser, *Opening Pandora’s Box: The Social Security Number from 1937–2018* (Austin: University of Texas, 2018).

Many government services ask individuals to create accounts with them to interact online in an ongoing manner and require a username and password. I recently went to renew a registration document and submit the application with the US government. The process involved creating an account with my email address as the username for integrating with the government website. I also enrolled two different authentication factors—setting a password and being asked to answer some “secret” questions to support account recovery if I forgot my password. I was also asked to upload digital photos or scans of the identity document the government has issued to me.

Creating single sign-on “approaches that allow a user to interact with multiple e-government systems may conflict with government policies intended to protect user privacy.”⁵ Therefore, this lack of a government-wide eID is a “good” thing because the government cannot see all the places where you use your identifier. Every time you share an identifier from an identity provider with a relying party, the relying party directs you to the identity provider for authentication. “An e-authentication solution that requires federal e-government users to use a common identifier might facilitate database linkages and, potentially, the creation of electronic dossiers.”⁶ Creative approaches, such as the system that British Columbia developed, to addressing this challenge need to be considered.⁷

The United Kingdom has implemented a system called UK Verify,⁸ where individuals enroll with a private institution and prove to the institution that they are indeed a named citizen; they then use these credentials to log on to the government portal where they match the attributes asserted by the private credential provider to the UK government. The US government has created a service called Login.gov⁹ that enables individuals to use various private identity providers (commercial entities) that register people and verify identity attributes. Login.gov provides a hub to support individuals logging into government services. Since the first version of this manuscript was written UK Verify and Login.gov are widely regarded as failures.

⁵ Stephen H. Holden and Lynette I. Millett, “Authentication, Privacy, and the Federal E-Government,” *The Information Society* 21, no. 5 (2005): 367–77. doi:10.1080/01972240500253582.

⁶ Ibid.

⁷ Peter Watkins, “Trust and Identity Management: Experience and Perspective from the Province of British Columbia, Canada,” Trust Conference: e-Government Identity Management Initiatives, The Hague, Netherlands, November 21, 2007, <http://www.llbc.leg.bc.ca/public/PubDocs/bcdocs/437299/BCPaperTrustandIdentityManagement.pdf>.

⁸ GOV.UK, “Guidance GOV.UK Verify,” accessed November 12, 2017, <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>.

⁹ US General Services Administration. “Login.gov,” accessed November 12, 2017, <https://login.gov>.

5. Civil Society Registration

Civil society registration happens when individuals begin relationships with any number of institutions: professional associations, nonprofit membership groups, religious congregations, sports leagues, and so forth. We also include educational and health care contexts in which people are patients and students. While some of these institutions are “for profit,” the nature of the transactional relationships suggests that it makes more sense to include these types of transactions in this domain (Figure 5.1). The first step is for the individual to go through a registration process possibly filling out forms. Once the organization has accepted those and created a record in their systems the organization issues a credential to the individual.



Figure 5.1. Civil society registration. This happens when individuals (1) register with a civil society organization and are (2) given credentials in return.

Examples of Transactions

- Registering to go to school
- Registering to join a soccer league
- Registering to join a professional association: American Medical Association, Certified Public Accountants, Nurses, Engineers, and so forth
- Registering to be part of a religious congregation
- Registering to be part of an association: neighborhood, bridge club, and so forth
- Registering to be part of a union
- Registering to be part of an association like the AARP
- Registering for an ORCID for scientific research and academic publishing
- Getting an identifier in a database—when one registers for school, one gets a student identification number

Roles

- Member/individual/student/patient
- Subject guardian
- Civil society institution

Sources of PII

- Individuals
- Identity documents issued to individuals by the government
- Credentials issued by other organizations

Types of PII

- Name
- Address
- Birthdate
- Information relevant to the institution
 - Educational history
 - Medical records from other providers
 - Records of engagement with religious institutions
 - Credentials

Relationship to Other Domains

Many civil society registration processes require claims verified by documents that are derived from government registration. Before interacting with a civil society organization in an ongoing way, a civil society transactions registration with that organization is required. Some employment registration processes require certification or verification from civil society organizations derived from civil society registration and transactions. Data from civil society organizations is sold to the data broker industry. Data is vulnerable to theft and appearing on the illicit market.

What Is the Process of Enrollment?

To register in any system, one has to first enroll in it. How does this happen in civil society institutions? For the sake of having a common vocabulary, we will call the subject a member, but they could be a patient, student, or some other term depending on the type of institution.

Our first interaction with civil society institutions is often when we are born: we become a patient in a health care institution.

When we are enrolling children in institutions, we are asked to share with the institution a copy of an “identity primitive” contained on a birth certificate. This is for several purposes including the need to know a child’s real age,¹ to know that the parents presenting are indeed the parents of the child being enrolled. These institutions may also request to see state-issued identity documents from the parents (as listed on the birth certificate) as well.

As adults, we are asked to present state-issued identity documents to prove who we are when joining some organizations, particularly those managing professional credentialing.

Some types of civil society institutions only require individuals to self-assert who they are and never ask for any identity paperwork. Examples of this include churches and social clubs.

Institutions in civil society often issue their own credentials to individuals. This includes a reference or identity number for the member enrolled (a patient number, student number, or membership number). This becomes an index that can be

¹ S. J. Pearson, “‘Age Ought to Be a Fact’: The Campaign against Child Labor and the Rise of the Birth Certificate,” *Journal of American History* 101, no. 4 (2015): 1144–65. doi: 10.1093/jahist/jav120.

referenced when the member appears again and it supports the linking of subsequent activities together. Organizations may issue this number on a membership card that can be used when presenting to the institution or to other institutions.

There are distinctions among institutions that primarily interact with individuals in person versus those that primarily interact with individuals online and those that do both. They have different methods that support recognizing the individual again when they transact with the institution after registration.

A membership card is a “what you have” credential that can be presented in person. The number can be an identifier when asserted in an online interaction and it can be paired with a factor of authentication associated with the number (a password).

If the institution takes a photograph of the individual to store in a record, this becomes a “what you are” authentication factor that can be referenced to check if the member is presenting in person. It is increasingly likely this authentication factor could be used remotely because of the proliferation of cameras in consumer devices.

If the institution is supporting the creation of a digital or online account associated with a membership, the institution will likely ask the individual to pick a password as a “what you know” factor of authentication that the individual member can use to authenticate the account when they want to interact digitally. The institution may also ask the member some security questions when an individual requests a password reset. This is a different form of “what you know.” If the institution is sophisticated, they may ask the individual to also enroll a device (laptop, phone) that they will use to log in. They may even issue a hardware token such as a Yubikey² to use in the process of logging in. These are “what you have” factors of authentication.

They might also set up a one-time password mechanism through either a hardware token, software defined token via an application on the phone, or by text messaging a code to a phone number. These are a combination of the “what you have” and “what you know” types of authentication.

How Is It Similar or Different from Government Registration?

In government registration with infants at birth, the parents are applying on behalf of the child, and in the process the child is issued an “identity primitive” in the form of a birth certificate. The birth certificate information is required by secondary government registration events to obtain driver’s licenses, passports, and other identity documents.

In civil society registration enrollment processes, the prospective member is often presenting documents issued by government in one of several different registration processes (birth certificate, driver’s license, passport). Then the member is enrolled with the institution, given a column in an index database of members, and given a particular identity for a particular institution (or network of institutions).

How Do You “Prove” Attributes That the Government Has Authority Over Digitally?

It is currently very complicated and difficult to enroll digitally in civil society institutions that require proof of identity attributes such as age, citizenship, or address issued.

² Yubico, “Why Yubico for Individuals,” 2017, <https://www.yubico.com/why-yubico/for-individuals/>.

One way is to scan the paper documents and then submit them. This creates challenges for documenting and keeping track of these documents with sensitive information on them.

Services are starting to provide identity proofing for individuals, including children, enrolling online to membership institutions.³

Companies are springing up to try and meet digital know your customer (KYC) requirements for adults. These take several forms. Some are provided by data brokers who have extensive records about individuals and ask them about their past addresses, mortgage payments, or other things to gain confidence that they are indeed the people they assert to be. This type of checking, that someone is who they claim to be, is called knowledge-based authentication (KBA) where individuals are assumed to be who they say they are because they have knowledge of certain facts, like the amount of their mortgage payment.⁴ Others ask individuals to upload photos of their documents and check these against government records.⁵

We are at the early stages of the issuance of identity credentials in digital form for citizens to use when enrolling with other institutions requiring government-asserted attributes about those they will enroll.

The United Kingdom has implemented a system called UK Verify where individuals enroll with a private institution and prove to the institution that they are indeed a certain citizen. Then they use these credentials to log on to a government website where they match the attributes asserted by the private credential provider.

The State of Illinois is beginning a pilot program to issue digital birth certificates.⁶ Estonia has a national electronic identity (eID) for residents, and people outside of the country can even become e-Residents.⁷ Digital electronic benefit transfer (EBT) cards have been available in California in all 58 counties since 2005, and the Aadhaar Card in India has some qualities of an eID.⁸

Delegation and the Role It Plays with This Activity

Any institution enrolling children needs to think about how it supports delegation to a parental or guardian account to manage activity of the children. A use case outlined in the You and My Identity domain highlights the challenges this poses to institutions.

³ USA Water Polo, "FAQ - Birth Date Verification," 2017, <https://web.archive.org/web/20180702045937/http://www.usawaterpolo.org/membership/faq-birthdate-verification-faqs.html>.

⁴ IDology, "Dynamic KBA," 2017, <https://www.idology.com/identity-verification-solutions/dynamic-kba/>.

⁵ Yoti (2017): <http://www.yoti.com>.

⁶ J. Althaus, "Governments Eye Blockchain in Their Creation of National Identity Systems," *CoinTelegraph*, October 6, 2017, <https://cointelegraph.com/news/governments-eye-blockchain-in-their-creation-of-national-identity-systems>.

⁷ Estonia, "What is E-residency?" 2017, <https://e-resident.gov.ee>.

⁸ B. Pon, C. Locke, and T. Steinberg, *Private-Sector Digital Identity in Emerging Markets* (Caribou Digital Publishing, 2016).

6. Civil Society Transactions

Civil society transactions are all the interactions with civil society institutions after registration: the classes you attend and the resulting transcripts that document those transactions, the visits to the doctor, hospital and labs, the accumulation of continuing education credits (CEC) as a professional, or the participation in any regular meetings/activities and voting as a member (Figure 6.1). Individuals present their credentials to the organization and are able to transact with or receive services from the organization.

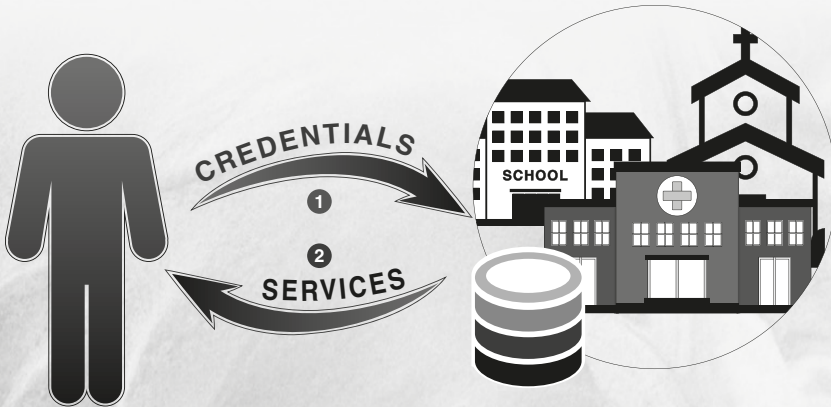


Figure 6.1. Civil society transactions. These happen when individuals (1) present credentials issued to them by civil society organizations and (2) in return they receive services or permitted to offer services such as volunteering.

Roles

- Individual (member, student, patient)
- Administrator
- Staff Member
- Cloud service provider
- Volunteer
- Donors

Types of PII

- Name
- Address
- Information relevant to the service/ transaction

Sources of PII

- Individuals
- Civil society credentials
- Identification documents issued by governments
- Lots of these: union membership status, religious affiliation, health conditions, and so forth

Types of Transactions

- Receiving medical care
- Attending classes and receiving grades in educational institutions
- Participating in an organization's meeting
- Volunteer service records

Relationship to Other Domains

Before being able to transact with civil society organizations, individuals need to go through a civil society registration process. Some employment registration processes require proof of membership in professional associations and proof of current educational attainment from the domain of civil society transactions. Data from civil society organizations are sold to the data broker industry. Data is vulnerable to theft and appear on the illicit market.

What Is the Relationship between Initial Registration and Ongoing Interaction?

During the civil society registration process, individuals are enrolled and have a unique record created for them within the system. This might be just a name or a name and birth date. However, often it involves the issuance of a member number that allows the individual to assert who they are relative to the database index.

This number allows for the persistence and connecting together of records about an individual over the time period of their interaction.

To support both in-person and digital authentications, that is, the process of checking that indeed the individual presenting again is the individual who originally registered, they are asked to enroll any one of a number of authentication factors.

It is in the process of ongoing interaction and transactions with a civil society institution that individuals are asked to authenticate with the factors that were enrolled.

How Were These Managed with the Technology of Paper?

Formerly, institutions that tracked people and their interactions did so with index cards and other paper-organizing and filing technologies.

Tracking individual's interactions with institutions over time involved a lot of paper. Health records of patients created by doctors were all paper-based and involved lots of filing and maintaining of local records at the site of treatment, not in a digital repository.

Schools kept paper records of students in a similar way, but over the last 40 years, these have shifted to digital records.

Many organizations issue their members physical identity cards. These could just be made of paper. They are used to verify membership in an organization.

How Are They Managed Now Digitally?

Today, these institutions often have ways for the individual member to interact with their system digitally, but they also have other systems that allow those in a service role (doctors, teachers, etc.) to interact with the members records.

Most complex institutions like universities have multiple systems to serve students. They have a master record index of students—a student number is issued and enrollment factors set up. Then, when students interact with various university systems and services, they present their student number and a password. The systems check with the master index and present the authentication factor (usually a password). If it matches the enrolled factor of authentication (the password they chose at registration), the individual is allowed into the system.

Professional accrediting institutions have membership and track the educational credits of individuals as they complete training. Now, much of this training is done with online courses, and even the in-person training is tracked with digital systems.

Some hospitals have biometric systems to support the tracking of patients. Medical networks support patients having accounts and logging into them to access messages from doctors and to see medical status updates.

Organizations with physical buildings like churches may issue electronic card keys to volunteers to give them physical access their buildings.

How Is Delegation Managed?

Delegation is a critical function to support these systems serving all kinds of people including children, the elderly, and the disabled.

However, supporting the connecting and linking of delegated accounts is not easy. Many of the tools for identity management were developed to serve enterprises where they are enrolling and interacting with employees who are themselves the only people showing up at work and logging into enterprise IT systems.

I have theorized that this market focus on enterprise identity and access management is one reason why the civil society registration process and the tools for ongoing management do not have a well-developed delegation capacity.

What Are the Range of Transactions That Might Involve the Collection and Management of Data?

- (1) Attending school as a student—records include attendance
- (2) Logging into a learning management system to get assignments, work on assignments and submit assignments, records of grades, participation in extracurricular activities
- (3) Being treated as a patient
- (4) Participating in a soccer league and participation in games; needing to prove the age of an athlete
- (5) Participating in a professional association, paying dues, and logging educational credit hours
- (6) Participating in a religious congregation, paying dues
- (7) Participating in an association—neighborhood, bridge club, and so forth—might include knowing about various events happening, logging participation, and tracking success/achievements
- (8) Participating in a union, paying dues, logging activity, and maintaining certification
- (9) Participating in an association like the American Association of Retired Persons (AARP), receiving discounts at retailers when presenting a membership card
- (10) Using an ORCID when submitting a scientific research paper and when logging into research networks that accept ORCIDs

How Does One Prove Current Membership in an Organization?

This context is huge. It involves all transactions with all types of institutions other than governments and commercial entities. Many transactions and records are created after one is registered with the institution.

In the case of school records, data can now include all the records with EdTech platforms and with service providers like Google when they provide email accounts and Google Docs to educational institutions.

There are a range of civil society organizations that provide benefits for members, such as the AARP. Traditional benefits such as discounts at businesses were provided by showing a current membership card. There are no simple solutions yet for doing this across a range of institutional settings. An example of a company starting to provide this type of service is ID.me, which works with veterans to support them claiming discounts at various retailers, including Under Armour. New work is emerging to support individuals having verifiable claims from many different sources issued to them by institutions under their control using self-sovereign identity tools.

7. Commercial Registration

Commercial registration happens when one creates an account with a merchant or service provider (Figure 7.1). The first step is for the individual to go through a registration process possibly filling out forms. Once the company has accepted those and created a record in their systems the company issues a credential and/or number to the individual.

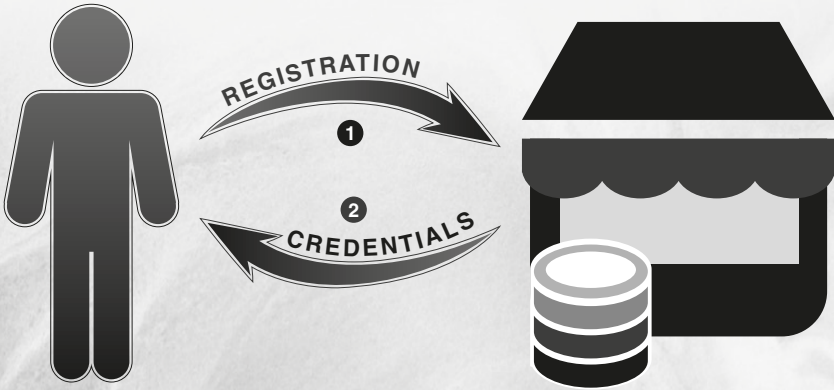


Figure 7.1 Commercial registration. This is when a potential customer goes through a (1) registration process and is entered into the company's database. They are (2) given a credential by the merchant for future use.

Roles

- The customer
- The network endpoint providers (phone company, email provider)
- Merchants

Sources of PII

- Government ID
- Individual assertions
- Consumer credit history

Examples of Transactions

- Individuals sign up for a loyalty program
- Individuals sign up for a bank account
- Individuals sign up for a store credit account
- Individuals sign up to access utility services

Types of PII

- Name
- Number issued to the customer
- Birthdate
- Address
- Phone number

Relationship to Other Domains

Commercial registration happens before individuals are able to do commercial transactions. For some commercial registration processes, documents and proofs of claims from government registration processes are required. Data from commercial

registration are actively sold to the data broker industry. Databases of customers are vulnerable to theft and use on the illicit market.

What Is the Explicit Process of Enrollment in Person?

Since the dawn of time, merchants have offered accounts so their customers can buy on credit and be more likely to make purchases. Account enrollment happened in small communities where the merchants knew their clientele and supported them being able to buy goods on credit. Merchants relied on community knowledge to know who was in the community. They typically maintained these records with pen and paper in log books, tracking what goods were sold on credit and how much individuals owed.¹

Merchants also tracked and rewarded the purchases of goods by regular customers. These were tracked on paper.

As people moved into cities, a new service arose to support retailers knowing to whom they should issue credit. They would check with credit-reporting agencies to know more about the credit worthiness of their customers.² Today we call these agencies data brokers. Due to the PII involved, this industry has its own domain (see below).

Today, retailers enroll individuals in loyalty programs by issuing them cards that give them a unique identification number, often encoded in a bar code on the card. They also often enroll an individual's phone number and use this to link activity. When an individual at a point of sale is asked to assert a phone number to link their purchase activity together with their loyalty card account, the phone number ends up being an identifier and a factor of authentication (the fact they know their phone number and can recite it).

The need to have accurate information about the consumer in the case of loyalty point enrollment is very low. If we look at the history of retail and examples of such as S&H Green Stamps, or, as another example, Canadian Tire Dollars, they were bearer tokens. One could give a million green stamps, or thousands of Canadian Tire dollars, to your aunt, and the merchant didn't know or care. Retailers do not typically ask for proof of identity or check that any of the attributes/identifiers asserted such as a phone number or address are accurate. The retailer is interested in the linking of activity over time more than they are in the detailed identity attributes, like the real name of the person.

Companies that offer credit to customers do check identity information about the individual and run a credit check, using data broker services, before issuing the credit.

Some enrollment processes for services are regulated. Banks are required by law to know their customers. These laws known as KYC regulations require the bank to ask for identifying information about individuals and have clear requirements about types of identification accepted. There are also laws known as anti-money laundering (AML) regulations that require banks to monitor who their customers transact with, to prevent money laundering. The banks on the other end of transactions need to provide customer identity information to the transacting banks. Banks ask individuals

¹ J. Lauer, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America* (New York: Columbia University Press, 2017).

² Ibid.

wanting to open new accounts to present driver's licenses, passports, and proof of address by showing bills from utility or telecommunications providers.

Some enrollment processes for services primarily consumed in person (like a gym) include enrolling a photograph as a biometric that can be used when the individual arrives to use the service, to check that they are indeed the member.

Some countries have national identity cards that have a citizen number. In countries like Singapore, individuals feel comfortable with the number on that card being used as a registration number for all manner of transactions including commercial ones.³ When prompted to enroll, individuals in these systems will just share this number and be enrolled with this as their main index number.⁴

What Is the Process of Explicit Enrollment Online?

Retailers often ask individuals to create an account with them to support ongoing interactions—making multiple purchases over time and having all transactions linked together.

Retailers are interested in getting more customers and getting paid. They are not particularly interested in doing identity proofing as part of this process by asking for government-asserted identity attributes because it is expensive and makes customers less likely to enroll.

Customers are often asked for an identifier that is a network endpoint such as an email address or phone number. Before the enrollment process is fully complete, a code is sent to that endpoint and the individual asked to enter it. This process is a step to ensure that the individual actually is the person at the end of the asserted network endpoint because they are in control of it and see the code entered.

Regulated industries have a harder time doing enrollment smoothly. In the domain of government registration, there are very limited options for the assertion of attributes from a government registration process in digital form. The same issues that are present in civil society transactions requiring proof of government asserted attributes are true for retailers.

Companies are springing up to offer digital KYCs. These take several forms. Some are supplied by data brokers who have extensive records about individuals and ask them about their past addresses, mortgage payments, or other transactions to gain confidence that they are indeed the people they claim to be. Others ask individuals to upload photos of their documents and check these against government records.⁵

What Is the Second Stage of Enrollment?

Once individuals make a first purchase from the retailer and choose a payment method, they take the next step in the enrollment process. If they are using a credit

³ Irene Tham, "All SingPass Users to Be Auto Enrolled in Digital Data Vault MyInfo by Year End," *Straits Times*, September 26, 2017, <https://www.straitstimes.com/tech/all-singpass-users-to-be-auto-enrolled-in-digital-data-vault-myinfo-by-year-end>.

⁴ Irene Tham, "Watchdog Seeks Stricter Protection of NRIC Data," *Straits Times*, November 8, 2017, <https://www.straitstimes.com/tech/watchdog-seeks-stricter-protection-of-nric-data>.

⁵ Yoti (2017): <http://www.yoti.com>.

card, they are asked to enter the number on the card, its expiration date, and the name on the card. It is worth noting that when signing up for a credit card, one can sometimes get a card issued in names other than one's own. Therefore, individuals might have an online purchasing pseudonym. This card information might be saved with a customer's account information so they can use it again in subsequent transactions.

Before the purchase is approved, the retailer sends credit card information to their bank for processing. It is cleared back to the bank that issued the credit card through the payment network so that it can be verified as a valid card that is good for the payment. With electronic transaction methods like PayPal, the merchant redirects individuals to a PayPal website where they enter the email address that is the identifier/username for their PayPal account. They are prompted to enter the authentication factors associated with it (this could be the "what you know" or the "what you have" authentication factor if they have a one-time password token). Individuals using a payment method in a digital transaction to buy something from a retailer are doing so with an account from a service provider (credit card from a bank or PayPal account) that requires a KYC enrollment process.

Many retailers use behavioral analytics to monitor for fraud. They are collecting PII and passing this along to services like ThreatMetrix⁶ that use this information to figure out if the person is legitimate.

How Is It Similar to or Different from Government Registration?

In government registration, one is actually applying to get source identity documentation. In commercial registration enrollment processes, one is presenting government documentation to become enrolled with the retailer or service provider and is given a customer number for the purposes of presenting and using the same customer account again in the future.

What Are Examples of Explicit Commercial Registration?

- (1) Becoming a member at a gym/ongoing service provider
- (2) Joining a loyalty program with a company
- (3) Getting an account with a company—early credit
- (4) Opening a new financial account
- (5) Getting services from a utility
- (6) Joining an online service

What Are Examples of Implicit Commercial Registration?

Implicit commercial registration involves processes where an individual's activity over time is linked to a common customer record, but they themselves do not go through an explicit registration process.

Examples include using a persistent electronic endpoint such as an Internet Protocol (IP) address or a phone number. These are unique network endpoints

⁶ ThreatMetrix (2017): <https://www.threatmetrix.com>, which, since the writing of the first version, was acquired by LexusNexus.

and retailers and service providers can link activity coming from the same network endpoints together.

When individuals use the same credit card at a retailer or service provider, these vendors can link together activity into a customer record.

How Do Individuals Un-Enroll?

In new European regulations, known as general data protection regulation (GDPR), there is a requirement to support individuals leaving a service and ending an account.⁷

⁷ Oxford Internet Institute (OII), "GDPR: The Right to Be Forgotten," 2016, <https://www.oii.ox.ac.uk/blog/gdpr-the-right-to-be-forgotten/>.

8. Commercial Transactions

Commercial transactions take place when a customer transacts for goods and services with a merchant or service provider (Figure 8.1). Individuals present their credentials to the company and are able to buy goods or services and have those transactions linked to their customer record.



Figure 8.1 Commercial transactions. These happen when the individual (1) presents a credential issued from the commercial entity in the registration process, (2) pays for a good or service, and then (3) receives the good or service.

Roles

- Customer
- Merchant
- Merchant services for credit card processing
- Loyalty card service provider
- Social login provider
- Email provider

Types of PII

- Name
- Phone number
- Address
- Financial account number
- Email address
- Goods purchased

Sources of PII

- Customers
- Earlier transactions that link all activity together
- Information about the person learned in the transaction process
- The systems of the company that process the transactions

Example of Transactions

Example registrations were highlighted in the above commercial registration domain. Here are some example transactions:

- Presenting a membership card to enter a gym
- Presenting an identifier with the loyalty program with a company via scanning a card, entering a customer number, or sharing a persistent identifier from another context such as a phone number
- Receiving gifts/rewards for participation in a loyalty program
- Using utility telecommunication or a telecoms provider
- Returning to an online service and then transacting
- Processing a credit card
- Using a credit card to purchase goods from a retailer or online merchant

Relationship to Other Domains

Individuals often need to register with a commercial entity before being able to do transactions. This is particularly true for transactions that happen online. In-person transactions that involve cash require no registration. When individuals are doing commercial transactions, they are subject to commercial surveillance. Data collected in commercial transactions are often sold to the data broker industry and are vulnerable to theft and use on the illicit market.

How Do Individuals Use the Identifier from Registration for Transactions?

There are a variety of strategies that retailers and service providers use to support individuals linking their activity together into a customer record.

Service providers such as gyms ask people to preset a card with a code on it, which, when scanned, brings up a photo of the individual that the person at the desk can verify is a match.

Retailers that have enrolled people into loyalty card programs ask them to present the card again or to share a unique identifier like a phone number to bring up the customer account and record the transition in their database. With these types of systems, individuals receive rewards via a digital version of their account.

In financial services, banks issue individuals a card that can be used to transact with the bank. This card is sent to the individual's home at the address provided. This card and the number on it becomes a "what you have" authentication factor. The bank also issues a personal identification number (PIN) to individuals, which is a password that the bank asks for when the individual presents the card. This is a "what you know" authentication factor. When a card is entered into a bank machine and the PIN is supplied, the customer has shared two factors of authentication ("what you have" and "what you know") and the bank proceeds with the transaction.

For online transactions, individuals must assert an identifier that is associated with their account. This might be a username they chose or were assigned, or it might be an email address that they asserted at the time of enrollment. They must also then provide a method of authentication that was enrolled; this could be a password ("what you know").

What Happens to the Records and the Data?

Records are kept of individuals who transact with commercial entities. Most of the time, individuals never get to see records of their transactions. There is the business of big data emerging where companies take all the data collected from their business transactions (and surveillance) and use it to analyze customer behavior, as well as gaining insights that will help them sell more to their customers. Attention came to this practice when the *New York Times* wrote about the case of a young woman who was pregnant and had purchased items from Target. The retailer inferred that she was pregnant and sent pregnancy-related coupons to her family home. Her father was very upset by this because he didn't know his daughter was pregnant.¹

¹ Kashmir Hill, "How Target Figured Out a Teen Girl Was Pregnant before Her Father," *Forbes*, February 16, 2012, <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#160ea0796668>.

What Regulation Is Coming in Europe?

The European Commission passed regulations five years ago, the General Data Protection Regulation took effect in May 2018, that mandate very strong rights for consumers to control what information is shared with commercial entities along with giving consumers the right to choose what can be done with their data. These regulations also stipulate that individual consumers be able to see all of the transaction data that a company collects while doing business with them.

9. Government Surveillance

Lawful **government surveillance** can include surveillance of the whole society by a census, labor department surveys of employment trends, surveillance as part of lawful Internet tracking, or law-enforcement surveillance via warrant access. Examples of unlawful surveillance include warrantless mass surveillance of communications, revealed by Edward Snowden (Figure 9.1).

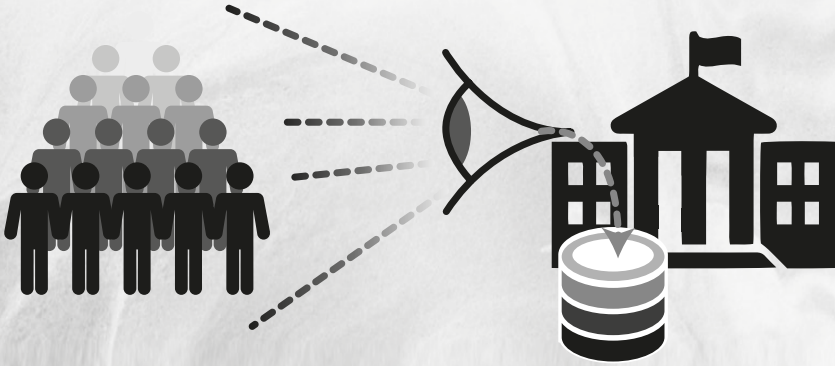


Figure 9.1 Government surveillance. This happens when the government collects data about citizens and residents.

Roles/Actors

- The subject, the person being surveilled
- Courts that issue warrants
- The agency that is surveilling
- The computer/machine AI that flags
- Fusion centers and domain awareness centers
- Surveillance agencies
- Police at all levels: local, county, state, and federal

Examples of Transactions

- Census
- AML/banking notification
- OBIM (Office of Biometric Identity Management) collecting biometrics from a whole range of government services
- Crossing borders
- Transportation and security administration NSA surveillance
- FBI surveillance
- Labor market tracking
- Prescription drug tracking
- Public health monitoring
- License plate readers
- Face recognition readers
- StingRays and international mobile subscriber identity (IMSI)-catchers to intercept cell phone communications

Sources of PII

- Biometric features: face, fingerprint
- Any information that is about a person collected in dataveillance

Types of PII

- Biometrics
- Identifiers that are network endpoints (phone number, email address)
- Identifiers that are not network endpoints (SSN, name, address)
- Metadata from dataveillance

Relationship to Other Domains

Individuals don't know they are being surveilled by the government and are just being themselves in the me and my identity domain. The data collected in government surveillance are not usually sold to data brokers, but governments buy data from data brokers to support filling out surveillance profiles.

What Is Surveillance?

Wright et al.¹ defines surveillance as “[t]he purposeful routine, systemic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection.”

Theorists musing about the cultural grounding of surveillance point to roots in the Western tradition that come from the “all-seeing eye” at the heart of Judeo-Christian beliefs. The all-seeing eye creates a “fear of getting caught,” and this fear is internalized by citizens as they navigate the world.² If behavior can be seen, then it can be controlled to create order. This is a privileging of vision that is rooted in the Enlightenment tradition.³

It is worth noting that surveillance differs from registration and enrollment discussed earlier in a range of contexts in that there is no enrollment process where individuals “sign up” and thus know that there is an entry in a database about them that will be used when they interact with the system in the future. With surveillance, individuals are tracked and their activity over time is linked together in databases.

What Are the Power Dynamics of Surveillance?

Surveillance is something that institutions do to individuals. This creates an inherent power asymmetry.⁴ Surveillance studies often reference a discussion of the panopticon design envisioned by Jeremy Bentham in 1791 and published in 1834. Modern prisons

¹ David Wright, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Wadhwa, and Didier Bigo, “Sorting Out Smart Surveillance,” *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 4 (2010): 343–54. doi:10.1016/j.clsr.2010.05.007.

² Kirstie Ball, “All Consuming Surveillance: Surveillance as Marketplace Icon,” *Consumption Markets & Culture* 20, no. 2 (2017): 95–100. doi:10.1080/10253866.2016.1163942.

³ David Lyon, *Theorizing Surveillance: The Panopticon and Beyond* (Cullompton: Willan, 2006 [1948]).

⁴ Kirstie Ball, “Organization, Surveillance and the Body: Towards a Politics of Resistance,” *Organization* 12, no. 1 (2005): 89–108. doi:10.1177/1350508405048578.

were not yet built and his diagram was a theoretical design. Simone Brown in *Dark Matters: On the Surveillance of Blackness*⁵ compares Bentham's drawing of the panopticon with that of the plan of the slave ship *Brookes* published in 1788 that was a literal prison at sea for carrying 609 people. Capturing Africans and sending them across the Atlantic in ships with this layout had been practiced since the sixteenth century. She goes on to highlight some of the scholars that have examined the historical formation of surveillance within the historical formation of slavery. This includes the rules that were prescribed for maintaining control on plantations and rules for the slave pass system. This is one of the first examples of identity documents in widespread use in the United States. "The system of radicalizing surveillance of the slave pass system was a violent regulation of black mobilities. On and off the plantation, black mobility needed to be tightly regulated in order for slave owners to maintain control."⁶ These roots of our contemporary systems were not considered by any of the other surveillance studies academics that I read for this research. The exploration of how contemporary identity systems are informed by radicalized systems of social control, like slavery, Jim Crow, and prison-industrial complex, are worth further research.

How Has Technology Changed Surveillance?

Technology makes it much easier for surveillance. Gary Marx outlined in a 1985 article in *Dissent Magazine*, "I'll Be Watching You: Reflection on the New Surveillance," how newer technology is different from more traditional, coercive, penal surveillance⁷

- Able to overcome distance, lack of light, and other physical barriers;
- Able to transcend time;
- Capital-rather than labor-intensive;
- Focus on all possible wrongdoers, not particular suspects;
- Focus on the prevention of violations rather than simply pursuing violations;
- Decentralized and thereby encouraging self-policing and inhibition;
- Actually and nearly invisible;
- Attempt to delve into personality and self, not simply the body;
- Deepen and widen surveillance to new areas.

He wrote this before the current wave of information technology. However, it is prescient noting that surveillance will delve into personality and self, beyond the surveillance of just the body, through the collection and analysis of data. "Dataveillance," a term coined by Roger Clarke,⁸ is the "systemic use of personal data systems in the investigation of monitoring of the actions or communications of one or more persons."

⁵ Simone Brown, *Dark Matters: On the Surveillance of Blackness* (Durham, NC: Duke University Press, 2015 [1973]).

⁶ *Ibid.*

⁷ Gary T. Marx, "I'll Be Watching You: Reflection on the New Surveillance," *Dissent Magazine* 32, no. 1 (Winter 1985): 26–34.

⁸ Roger Clarke, "Information Technology and Dataveillance," *Communication of the ACM* 31, no. 5 (May 1988): 498–512, <http://www.rogerclarke.com/DV/CACM88.html>.

This book is centered on activities that lead to individuals having PII recorded into databases. Thus, dataveillance is of particular interest. Advances in modes of surveillance that are focused on the body such as CCTV, facial recognition technology, and permanent data storage capacity means that retroactive analysis and tracking is also possible.

What Are the Different Kinds of Surveillance?

To think clearly about surveillance, it is helpful to break it down into three categories:

1. **Voluntary Known:** the subject understands that they are being surveilled and makes a choice to participate with the surveillance.
2. **Involuntary Known:** the subject understands they are being surveilled but does not have a choice in their surveillance.
3. **Involuntary Unknown:** the subject does not know they are being surveilled.

Voluntary Surveillance by Government

The census is a form of surveillance that began in the eighteenth century. It is structured and carried out by the government. The “census enables a population to be seen and known in statistical space and its findings can inform policy decisions by local and national administrative bodies.”⁹ While there are provisions requiring citizens to participate in the census, it is a voluntary act to fill out the forms and submit them to the government.

Governments departments perform various forms of surveillance for statistical and other purposes including public health and labor department tracking. These systems are not the focus of this book, and most of these programs do not track specific people but rather surveil by doing surveys and having specific reporting requirements for doctors.

Particularly in the financial industry, regulations mandate reporting to the government the specifics of large transactions that are required for anti-money laundering (AML), with rules laid out in international bodies like the OECD.¹⁰

In the last decade, state prescription drug programs have come into being that create statewide electronic databases to collect information about prescriptions.¹¹ These track patients who received prescriptions for controlled substances to prevent prescription shopping.

In the United States, beginning in the early part of the twentieth century, laws were effected that required registration of vital events (births and deaths) with counties and that they be reported to state authorities.¹²

⁹ Ball, “All Consuming Surveillance,” 97.

¹⁰ David M. Wood and Kirstie Ball, “Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism,” *Marketing Theory* 13, no. 1 (2013): 47–67. doi:10.1177/1470593112467264.

¹¹ Drug Enforcement Agency (DEA) “State Prescription Drug Monitoring Programs,” June 2016, https://www.deadiversion.usdoj.gov/faq/rx_monitor.htm.

¹² H. L. Brumberg, D. Dozor, and S. G. Golombek, “History of the Birth Certificate: From Inception to the Future of Electronic Data,” *Journal of Perinatology* 32, no. 6 (2012): 407–11. doi:10.1038/jp.2012.3.

Known Involuntary Surveillance by Government

Customs and border patrol uses surveillance at points of entry at both airports and land crossings. Transport Security Administration checkpoints at airports are surveillance activities that check for bombs and weapons and prevent them from getting on planes. They are known and involuntary. Subjects cannot get into the country or on a plane without passing through these checkpoints. Subjects also present identity documents and in the process “transact” with the government when they are surveilled passing through these checkpoints.

The Office of Biometric Identity Management (OBIM) is a part of the Department of Homeland Security, which collects and manages biometric information collected from all persons who interact with the Department of Homeland Security. They currently hold more than two hundred million unique identities in their IDENT database.¹³ When residents of the United States enrolled in the database cross the border, their fingerprints are checked against the records in this database (as a form of authentication). This database is also used by officers patrolling the border to actually identify people they stop. In this case, the biometrics are used as an identifier.

Semi-Known Involuntary Surveillance by Government

Some surveillance is in between the known and unknown. This is particularly true as devices get smaller and smaller. Police departments around the country deploy video cameras throughout their cities (Chicago has 10,000). License plate readers are commonplace in police cars across the country, and newer technology that can recognize faces as they pass by police cars are coming into use.¹⁴

The police and other law enforcement officers have the ability to surveil people with a warrant. This type of surveillance is “known” to the courts because police have to get a warrant to be permitted to tap a phone or place a GPS tracking device on a person’s car. The surveillance is not known to the subject of the surveillance. We have laws that outline what is permitted and required to get the types of warrants known as lawful intercept.

In the post-9/11 world, new fusion centers and domain awareness centers developed by the Department of Homeland Security are being created to pool government surveillance across levels of government and different agencies. These centers are new and advocacy groups like Oakland Privacy have been challenging legal scope of their ability to track citizens.¹⁵

Digital dossiers are part of greater information sharing that emerged post 9/11. The Department of Homeland Security set up law enforcement information sharing

¹³ OBIM (Office of Biometric Identity Management), “Biometrics,” *Department of Homeland Security*, 2017, <https://www.dhs.gov/biometrics>.

¹⁴ ACLU, *Chicago’s Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy, a report from the ACLU of Illinois* (2017), http://dig.abclocal.go.com/wls/documents/Surveillance_Camera_Report.pdf.

¹⁵ Nathan Sheard, “Oakland Privacy and the Fight for Community Control,” *Electronic Frontier Foundation*, October 26, 2017, <https://www.eff.org/deeplinks/2017/10/oakland-privacy-and-fight-community-control>.

service¹⁶ after 9/11. It has 489 participating agencies representing 26,000 user accounts and covers all major geographic regions of the United States. The number of agencies participating is expected to triple over the next year.¹⁷

Unknown Surveillance by Government

After World War II, the government was concerned about internal security. It conducted surveillance of citizens by the military outside of the rules of lawful intercept:

Surveillance was carried out on participants in the Poor People's March on Washington in 1968—visitors to Martin Luther King Jr.'s grave, black nationalists, socialist organizations, and those engaged in antiwar demonstrations of more than 20 people across the country. The Army had 1,500 plain clothes agents, working out of three hundred offices.¹⁸

This resulted in the army having dossiers on seven million US citizens. These and other systemic unlawful surveillance cases during the 1950s and 1960s were uncovered by the Church Commission.

Law enforcement got a whole new range of tools with cell phones and began deploying tools—StingRays and IMSI-catchers—that pose as towers often times outside of the terms of lawful intercept. Recent revelations have shown that the CIA has sophisticated electronic surveillance tools to target specific individuals.¹⁹

In 2011, Edward Snowden revealed extensive NSA surveillance and collection of metadata about the communication of Americans that was previously unknown.²⁰

¹⁶ ICE (Immigration and Customs Enforcement), "Law Enforcement Information Sharing Initiative," 2017, <https://www.ice.gov/le-information-sharing>.

¹⁷ Ibid.

¹⁸ John B. Foster and Robert W. McChesney, "Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age," *Monthly Review* 66, no. 3 (2014): 1.

¹⁹ Jeremy Scahill and Margot Williams, "STINGRAYS: A Secret Catalogue of Government Gear for Spying on Your Cellphone," *The Intercept*, December 17, 2015, <https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/>.

²⁰ Joseph Verble, "The NSA and Edward Snowden: Surveillance in the 21st Century," *ACM SIGCAS Computers and Society* 44, no. 3 (2014): 14–20. doi:10.1145/2684097.2684101.

10. Civil Society Surveillance

Civil society surveillance is not yet widespread. However, there is more and more tracking of health care and educational activities. Professional associations may also be surveilling their members. Civil society groups may organize to perform collective citizen surveillance of corporations or governments (Figure 10.1).

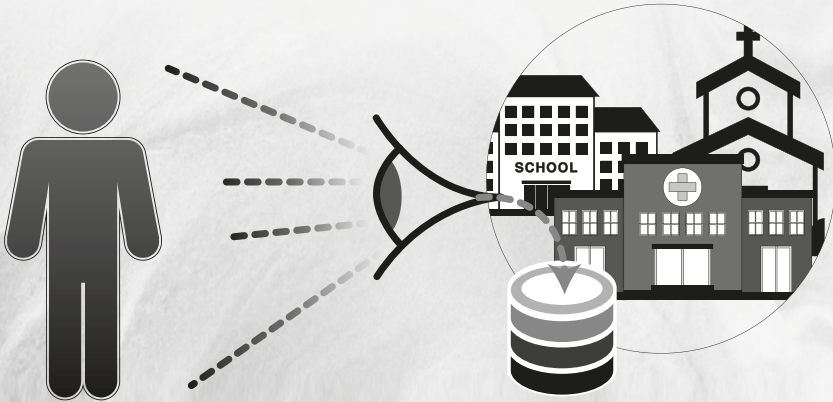


Figure 10.1. Civil society surveillance. This happens when a civil society organization tracks people they interact with, the people they provide services to.

Roles/Actors

- Patient–health care provider–health care institution
- Student–educational institution
- Citizen advocacy groups
- Professional organizations

Examples of Transactions

- Medical tracking devices
- Student facilities access tracking

Types of PII

- Medical device information
- Student ID cards

Sources of PII

- Wearable devices voluntarily worn
- ID cards voluntarily carried

Relationship to Other Domains

Individuals, while being surveilled by civil society institutions, don't necessarily know they are being surveilled and think they are just being in the me and my identity domain minding their own business. Data collected in civil society surveillance could be sold to data brokers, are vulnerable to theft, and could appear on the illicit market.

Detailed Description and Relevant Literature

Civil society surveillance is primarily voluntary and known. Patients accept wearable health-monitoring devices that collect data to be retrieved by health care providers, or the patients send the data directly to these providers. Some providers are also installing medical sensors in homes.¹

Some school systems have issued identification cards enabled with radio frequency identification (RFID) near-field communication (NFC) to students, which can be scanned at checkpoints² or seen by sensors that can then share with administrators where students are located in a school.

There is very limited academic research about this surveillance. In one of the articles I read on the topic, I found one book that focused in this area, *Under Observation: The Interplay between eHealth and Surveillance*.³ Most of the studies within it examine patients' acceptance of these types of technologies and their relative invasiveness.

The physical institutions of schools, hospitals, and other civil society organizations have within them a range of surveillance tools for security such as CCTV cameras. These, however, are not likely logging an individual's activity into databases with PII attached.

Can Civil Society Conduct Sousveillance?

The term "sousveillance" was coined by Steve Mann. "Sur" is a prefix that means "above," so "surveillance" means "watching from above." The prefix "sous" means "below." So, "sousveillance" means "watching from below."⁴ It has come to reference watching those in power such as watching video recordings made by civilians of police action. It includes collective organized watching of surveillance by various state agencies. The Oakland Privacy group is an example of a citizens group that is tracking government surveillance activity and monitoring all new ordinances related to it in Oakland, California, and neighboring jurisdictions.⁵

¹ David Wright, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Wadhwa, and Didier Bigo, "Sorting Out Smart Surveillance," *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 4 (2010): 343–54. doi: 10.1016/j.clsr.2010.05.007.

² Emily Richmond, "Tagging Students," *Scholastic Administrator*, Spring 2013, <http://www.scholastic.com/browse/article.jsp?id=3757964>.

³ Samantha Adams, Nadezhda Purtova, and Ronald Leenes, *Under Observation: The Interplay between eHealth and Surveillance* (Cham: Springer, 2017).

⁴ Jascha Hoffman, "Sousveillance," *New York Times Magazine*, December 10, 2006, <https://www.nytimes.com/2006/12/10/magazine/10section3b.t-3.html>.

⁵ Nathan Sheard, "Oakland Privacy and the Fight for Community Control," Electronic Frontier Foundation, October 26, 2017, <https://www.eff.org/deeplinks/2017/10/oakland-privacy-and-fight-community-control>.

Surveillance



Sousveillance

Figure 10.2. Sousveillance is people working together to watch the surveillers.

11. Commercial Surveillance

Commercial surveillance is vast as the push is to get more information about consumers and use it to shape their purchasing activity. It happens in person in stores with CCTV and sensor networks. It also happens with digital tools and services via cookies, and beacons from advertising networks in web content (Figure 11.1).

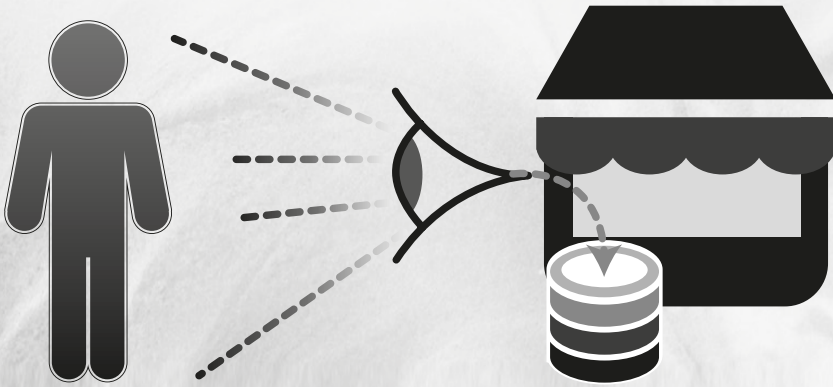


Figure 11.1. Commercial surveillance. This happens when commercial organizations gather information about their customers and potential customers.

Roles

- Potential customer
- Customer
- Commercial entity
- Data analytics firm

Sources of PII

- The customer
- Inferred data from surveillance activity
- Customer affinity cards and accounts
- Customer cell phone identifiers tracked by beacons

Examples of Transactions

- Watching a customer's body in a store using CCTV
- Tracking user activity via digital beacon technology
- Tracking customer purchase history through affinity accounts
- Tracking the individual's activity on the website
- Using applications on customer phones to gather information

Types of PII

- Metadata
- Identifiers
- Biometrics

Relationship to Other Domains

Commercial surveillance happens in the context of individuals interacting with commercial entities in person or online. Individuals, when they are being surveilled, don't

see the surveillance and think of themselves as being me and my identity. Therefore, commercial transactions are likely to be occurring in parallel with commercial surveillance. Data from commercial surveillance are sold to data brokers and are vulnerable to leaks and hacks and could end up on the illicit market.

What Is Surveillance in the Context of Commercial Enterprises?

This was touched on in the domain of government surveillance, but it is worth revisiting with an eye to what it means in the specific context of commercial surveillance. Lyon defines surveillance as “any collection and processing of data whether personally identifiable or not, for the purposes of influencing those whose data have been garnered.”¹ Commercial entities are trying to observe and record personal details to manage their customers and influence potential customers.

Corporate marketing and media systems emerged out of World War II to entice people to buy things to absorb the surplus production of the economy. “Marketing evolved quickly in its period of greatest advance in the 1950s into highly organized system of customer surveillance, targeting propaganda and psychological manipulation of populations.”²

The metaphors of Big Brother and the type of totalitarian government intrusion into people’s lives that it would create are contrasted with the corporate surveillance as “merely interested in providing goods and services.”³ It goes deeper with surveillance-based reality television, which equates submission to comprehensive surveillance with self-expression and self-knowledge. Andrejevic’s research shows that people’s exposure to television increases their acceptance of ideas such as “the more businesses know about me the better they can meet my individual needs.”

The asymmetry of information is increased with commercial surveillance done by companies because they can aggregate it.

Corporations are in a good position to extract information from consumers who often have little choice but to surrender information in order to complete a transaction, [...] but consumers have very little access to the information about corporations or what is doing with their information.⁴

¹ David Lyon, *Surveillance Society: Monitoring Everyday Life* (Milton Keynes: Open University Press, 2001).

² John B. Foster and Robert W. McChesney, “Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age,” *Monthly Review* 66, no. 3 (2014): 1.

³ Mark Andrejevic, “The Kinder, Gentler Gaze of Big Brother: Reality TV in the Era of Digital Capitalism,” *New Media & Society* 4, no. 2 (2002): 251–70. doi:10.1177/14614440222226361.

⁴ Ibid.

The data sources in commercial surveillance are data from computer-mediated transactions, data from billions of sensors embedded in a widening range of objects, bodies, and places, and data bought from various data brokers.⁵

“Dataveillance” is a term coined by Roger Clarke⁶ referring to the surveillance using the data gathered by people. People’s individuality is rescued from mass society with mass customization, which requires surveillance. Thus, the gaze does not create the threat of mass homogeneity. It creates the promise of mass individuation.⁷

What Are the Different Kinds of Surveillance?

The three types of surveillance introduced in the domain of government surveillance apply to commercial surveillance as well. All three types of surveillance happen in this domain both on and offline.

Forms of Voluntary Surveillance by Commercial Entities

When individuals present their loyalty cards when making purchases from companies, these transactions are recorded, linked together, and used by the company to make marketing decisions. This is a form of known voluntary surveillance.

People install applications on their mobile phones to share location data and traffic data with these applications, which then aggregate the data and share them with others via the app. Many applications ask if they can have your location data—this is all being collected to get more information about individuals and is used to surveil them for commercial purposes. They volunteer this information.

When individuals are signed in to a device, search engines like Google or Bing collect all the information about what individuals search and aggregate it. This is on the border between a transaction with a company and surveillance by them.

Forms of Known Involuntary Surveillance by Commercially Entities

When people enter into physical stores they are often on CCTV, which can be seen. It is a common practice so people know they might be on CCTV in a store even if they can’t see the camera. The reason for the camera surveillance is to prevent theft. Newer technologies coming into stores offer ways for commercial entities to evaluate how people move through stores and evaluate traffic patterns.

Las Vegas has invested heavily in face-recognition technology to identify patrons and in particular patrons that companies do not want to permit into their

⁵ Shoshana Zuboff, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” *Journal of Information Technology* 30, no. 1 (2015): 75–89. doi:10.1057/jit.2015.5.

⁶ Roger Clarke, “Information Technology and Dataveillance,” *Communication of the ACM* 31, no. 5 (May 1988): 498–512. <http://www.rogerclarke.com/DV/CACM88.html>.

⁷ David Lyon, *Theorizing Surveillance: The Panopticon and Beyond* (Cullompton: Willan, 2006 [1948]).

establishments.⁸ This type of technology has migrated into stores to identify known shoplifters.⁹ Amazon has conducted experiments to let people shop at its stores without actually going through a checkout process. Instead, they are automatically checked out by systems in place that surveil what people pick up and carry out of the store using their enrolled biometric face print to know who they are to charge their account.¹⁰

Are tracking cookies on websites and online beacons known or unknown? They are now required to be announced when surfing sites based in Europe.¹¹ It depends on the person, but largely they fit into the unknown category. These get sent to individual's computers, sit in their browsers, and help build user profiles for advertising networks. Many features on the web break unless they have cookies that help session persistence. Surfing the web with cookie tracking turned off makes it an unpleasant experience. This leaves a question about whether they are voluntary or involuntary.

Forms of Unknown Involuntary Surveillance by Commercially Entities

When people use loyalty cards to make purchases, they are making a conscious choice of linking their activities together and sharing it with a company. A similar linking and tracking of customer behavior can be achieved with the use of credit cards as a persistent identifier—the credit card number—linking all the transactions to a particular customer and which can be stored for future analysis.

Retailers have begun to use “beacon” technology, which lets them track users based on the signals the cell phones in their pocket emit. The brick-and-mortar retailers see this technology as a kind of “equalizer” to get information about their customers that online retailers and networks get from cookies. They can create maps of where people move about in the store and what they look at (equivalent in some sense to what they click on online). Mobile phones that interact with the network have unique identifiers so stores can identify returning customers.¹²

The marketplace of companies that use technology related to surveilling potential customers has grown from around 150 companies in 2011 to 5,000 companies today.

⁸ CBS News, “Smile! You’re On Casino Camera,” February 26, 2001, <https://www.cbsnews.com/news/smile-youre-on-casino-camera/>.

⁹ Chris Frey, “Revealed: How Facial Recognition Has Invaded Shops – and Your Privacy,” *Guardian*, March 3, 2016, <https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto>.

¹⁰ Paul Sawers, “Amazon Launches Amazon Go, a Mind-Blowing Brick-and-Mortar Grocery Store with No Checkouts,” *Venture Beat*, December 5, 2016, <https://venturebeat.com/2016/12/05/amazon-launches-amazon-go-a-brick-and-mortar-grocery-store-that-does-away-with-checkouts/>.

¹¹ European Commission, “Information Providers Guide: Cookies,” 2017, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm.

¹² Stephanie Clifford and Quentin Hardy, “Attention, Shoppers: Store Is Tracking Your Cell,” *New York Times*, July 14, 2013, <http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html>.

The ecosystem of activity and the exchange of data in these networks is vast. There are a wealth of terms that describe this industry and the core functionality including customer relationship management, marketing automation platform, content management system, iPaaS integration management as a services, customer data platform, data management platform, and real-time integration management.

The Grey Zone

This is a term I coined to talk about things that consumers have consented to or are informed about without comprehending the scope or extent of what is really happening. This is a result of the consent and privacy policy-based framework of privacy in the United States, where companies are obligated to tell users via privacy policies what will happen to their data but not in language they can comprehend.

An example of this is individuals with mobile phones being asked by applications to agree to share location data. These data are used to infer a huge amount about customers and their movements. For example, in the week following the acquisition of Whole Foods by Amazon, an analysis was done by a company called Thasos showing that regular shoppers at Walmart and Kroger were 40 percent of the new customers coming into Whole Foods that week.¹³

The collection of data about consumer behavior by retailers is widespread. This trend, called Big Data, uses the large amount of collected information about customer shopping patterns to analyze what people buy, and infer what might be happening in their lives and what they might be interested in buying in the future. They link all the information about a customer to a Guest ID. These practices were brought to public attention when a story emerged about how Target figured out a young woman still living with her parents was pregnant before her dad did. They had analyzed her shopping and saw she was buying prenatal vitamins and sent some coupons to her house. The father saw they were for items for pregnant women and went to Target furious they were sending the coupons to his daughter. She had not told him that she was pregnant.¹⁴

The dominant online advertisers seek to link the ads that individuals are shown to real-world in-store purchases and do so by tracking individuals with applications on their phones. Google introduced the ability of advertisers to track in-store visits in 2014.¹⁵ Facebook introduced this feature in 2016.¹⁶

¹³ Jordan Valinsky, "Whole Foods Is Stealing Walmart and Trader Joe's Customers with Its Low Prices," *CNN Money*, October 3, 2017, <http://money.cnn.com/2017/10/03/news/companies/whole-foods-competition/index.html>.

¹⁴ Charles Duhigg, "How Companies Learn Your Secrets," *New York Times Magazine*, February 16, 2012, <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

¹⁵ Mark Bergen, "Google Adds YouTube to Suite of Ad Tools Tracking Retail Sales," *Bloomberg News*, May 23, 2017, <https://www.bloomberg.com/news/articles/2017-05-23/google-adds-youtube-to-suite-of-ad-tools-tracking-retail-sales>.

¹⁶ Kurt Wagner, "Facebook's New Ads Will Track Which Stores You Visit: Facebook Wants to Prove That Its Ads Lead to Actual Purchases," *ReCode*, June 14, 2016, <https://www.recode.net/2016/6/14/11926124/facebook-ads-track-store-visits-retail-sales>.

12. Employment Registration

Employment registration the process that a new hire goes through to begin work with an employer. It starts with the application process where PII is shared from a prospective employee with an employer, there is an evaluation process where more PII might be shared and finally after a job offer is made to an employee they are enrolled in to the enterprise identity and access management system and then issued credentials (Figure 12.1).

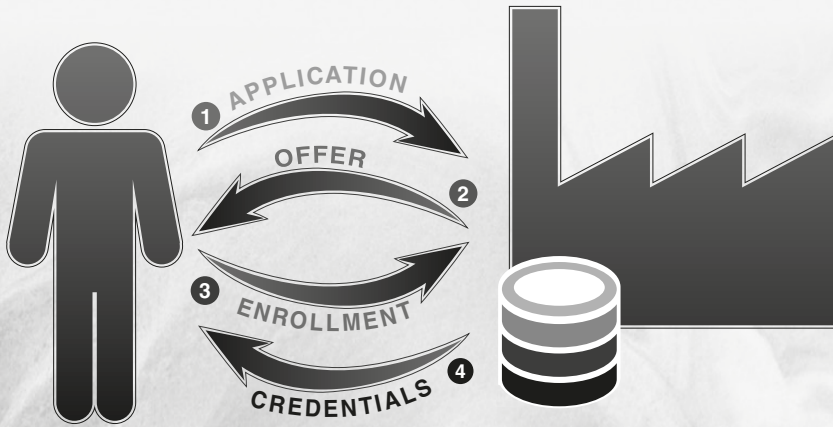


Figure 12.1. Employment registration. This happens when prospective employees (1) applying for jobs are (2) given offers for employment, (3) registered, or enrolled and have given (4) employee credentials.

Roles/Actors

- Employee
- Employer
- Cloud service provider
- Background check services for potential employees
- Government agencies responsible for determining employment eligibility

Sources of PII

- Job application
- Surveillance of the applicant by the potential employer based on the job application
- Information collected from the employee during registration
- Government criminal history databases
- Professional association accreditation and complaint databases

Examples of Transactions

- Employers identity-proofing applicants
- Employers conducting eligibility and background-check processes
- Job seekers sharing PII in the application process
- HR getting PII from new employees
- The IT department enrolling the new employee into their digital system

Types of PII

- Name
- Address
- Tax identification number
- Citizenship status
- Educational credentials

Relationship to Other Domains

When individuals seek employment, they go through an employment registration process. They must do this before they start work and do employment transactions. In the process of going through employment registration, they present themselves and their identity, bringing the me and my identity domain into play. Individuals also need to present documents and identifiers from government registration processes. The database of employees and prospective employees from the application process is vulnerable to theft and appearance on the illicit market. Some employment data end up being circulated to data brokers.

Description

This domain is one of three focused on the employment context. In much of the industry, “enterprise identity and access management” is a term of art that combines functions from all three employment domains in this book. This context has been separated into three separate domains to clarify thinking regarding different aspects of identity management in each of them. The purpose of gathering data about employees that are stored in employer databases varies.

What Are Pre-Enrollment Processes?

During the process of seeking employment, individuals share their résumés with employers and fill out application forms. Both contain PII. Employers who regularly hire have systems to track these people and information about them. This is also called applicant surveillance.¹ Many employers will use various types of background checks to vet people before hiring them. These type of checks require PII and the approval of the individuals. The potential employers have a database of this information about people.

Identity Proofing and Credential Verification

Once an employer has decided to hire a person, the employee goes through a process to become registered in the different enterprise systems. There is a process the HR department uses to gather exact identity information including name, birthdate, and Social Security number (an identifier issued by the federal government to the person in a government registration), which they need to know to be able to report income and submit taxes to the federal government.

They also may do background checking at this point to fulfill various professional requirements, which could include checking of professional credentials. For instance, if hiring a doctor, is their certification current or not? This type of check can end up being part of an ongoing “reregistration” process that happens every year. Some professionals spend many days each year sharing their certifications with the institutions they work with.²

¹ Christian Fuchs, “Political Economy and Surveillance Theory,” *Critical Sociology* 39, no. 5 (2013): 671–87. doi:10.1177/0896920511435710.

² Lily Brag, entrepreneur building decentralized credential tracking systems for doctors, interview with the author.

The federal government has a whole set of standards for identity proofing and onboarding of employees called “Policy for a Common Identification Standard for Federal Employees and Contractors,” as a result of the Homeland Security Presidential Directive 12³ signed by President Bush in August 2004. It specified these requirements:⁴

- (1) Sound criteria for verifying an individual employee identity;
- (2) A credential that is strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation;
- (3) Can be rapidly authenticated electronically;
- (4) Issued by a department with processes whose reliability has been established by official accreditation.

How Does Onboarding in the Digital Systems Work?

The processes of registering in the digital identity management system of the company also involves some steps. The first step is to be enrolled within the core directory of employees. This directory is like the master record of employees. Employees are likely assigned an employee number and given identifiers that they can use in the process of doing their job, such as an email address. This may also include the issuance of devices they can use during their employment, like a phone and/or computer.

The individual must also have authentication factors enrolled so they can prove they are in fact who they claim to be (a particular employee) when they log on to the enterprise systems. There are several different broad categories of authentication factors:⁵

What You Know: Passwords, PINs, answers to questions like “What is your pet’s name?”

What You Have: This is an object the employer gives to you, such as a physical card with a digital chip in it, that you present.

What You Are: These are biometrics. One has to actually enroll them to be able to check against them. Employers often take photos of their employees to put on their badges. They may also take other forms of biometrics like a fingerprint or palm print and use this to support access control to physical space or devices.

New authentication factors include:

What You Do: These are behavioral biometrics such as how you type—again, this has to be enrolled so that a pattern can be matched against a known behavioral pattern.

³ Homeland Security, “Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors,” 2004, <https://www.dhs.gov/homeland-security-presidential-directive-12>.

⁴ NIST (National Institute of Standards and Technology), “Personal Identity Verification (PIV) of Federal Employees and Contractors,” *Federal Information Processing Standards Publication*, August 2013. doi:10.6028/NIST.FIPS.201-2.

⁵ Maryline Laurent and Samia Bouzefrane, *Digital Identity Management* (London: Iste Press, 2015).

Where You Are: This is geolocation so you could enroll your phone, which is likely with you and accurately reflects your location. The employer might only let you into an account if you are actually near your phone.

Whatever be the employers' choice of authentication methods, they need to enroll the factors so that they can be used in the beginning of transactions.

When an individual logs into the system to do something in their role as an employee, they are completing a transaction (that is the next domain).

Even moderately sized enterprises have many applications that employees use. A whole set of tools arose to support managing employee access via what was called single-sign-on across the enterprise. They all tie back to this core directory and the enrolled authentication factors. Each application an employee uses requires that they have an account provisioned for that particular system. Enterprise applications use a standard called SAML (Security Assertion Markup Language)⁶ to communicate. This includes adding an employee to a list of users for a system (provisioning) or withdrawing that access (de-provisioning).

How Is It Similar to or Different from Government Registration?

Registration in the context of employment is different from government registration. Most people seeking employment are adults, and a good portion of government registration is done for infants by their parents (birth registration). This involves several people, parents, doctors, and so forth asserting that indeed a new person exists. Many government registration processes do not involve enrolling authentication factors. All employee registrations do.

What Happens When Employees Stop Being Employees?

The final phase in the life cycle of identity management in the enterprise is de-provisioning or termination. It is the opposite of provisioning: ending access to accounts for an employee who should no longer have access. Not having effective systems to do this is a major security risk for the enterprise because disgruntled employees could access systems after the end of their employment and either steal information or cause damage to enterprise systems.

Once employees are no longer working for a company, there are records that are kept by the company about their employment. There are also post-employment benefits, such as retirement accounts, that are provided, which will require the ongoing management of an identity for the former employee.

⁶ OASIS Security Services (SAML) TC (2018): https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

13. Employment Transactions

Employment transactions are all the logins and authorizations that happen when employees do their job while physically present on site, for example, entering a building for work. It also may happen when they log on to digital systems (Figure 13.1). Individuals present the credentials issued to them by the enterprise, do their work within the context of their employment and in turn are paid.

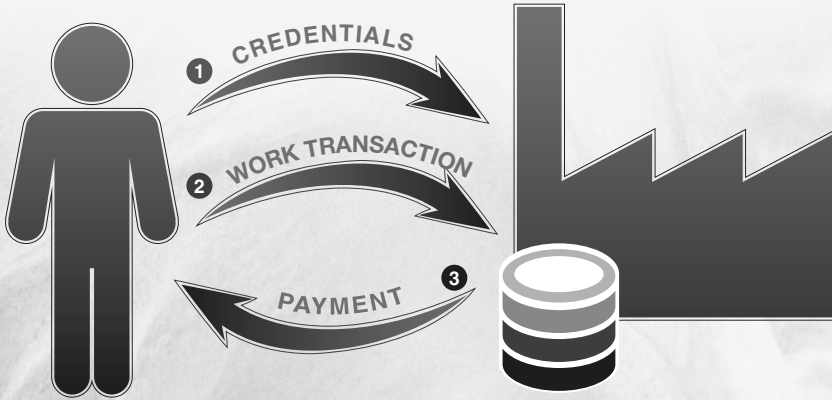


Figure 13.1. Employment transactions. This happens when employees present their (1) credentials to an employer and then (2) work transactions happen. In return, they (3) receive payment for their work.

Roles

- Potential employee
- Employees
- Employer
- Employer subcontractors
- Cloud service providers

Sources of PII

- The employee record
- All the employee's activity logs

Examples of Transactions

- Logging into systems
- Writing documents
- Working on manufacturing machines
- Accounting
- Creating spreadsheets
- Entering data in databases
- Looking up data in databases
- Claiming benefits
- Transacting as a delegate of the business

Types of PII

- Name
- Employee ID number
- Metadata relative to interactions with the employers system

Relationship to Other Domains

Individuals who become employees and do employment transactions have to go through the process of employment registration first. Once they do employment transactions, they are surveilled by their employers. The next domain is employment surveillance. Data from employment transactions are vulnerable to data breaches and theft, and could end up on the illicit market. It isn't likely that employers are selling employment transaction data to data brokers, but they might be selling data inferred from transaction data to them. Data generated while employed and doing employment transactions might be part of me and my identity data too, in the form of work portfolios and credentials earned as part of employment. One of three types of delegation outlined in the you and my identity domain happens when employers delegate capabilities to individual employees to act on their behalf.

Description

Employment transactions are all employee activities in the context of their work that create digital records. This includes simple things like punching in to a time clock when they arrive at work and clocking out when they leave. If an employer has a door with logical access control, the employee would need to swipe their employer-issued ID card on the door to gain access.

In the process of becoming an employee, individuals are issued an identifier—an employee number. This number is what they use when logging on to the digital systems of the employer. However, this is not enough to get into the systems. They must also present an authentication factor that the employer checks, matching it against the factors of authentication that the employee included in the employee registration.

An identity management system's purpose is to regulate access to resources.¹ Administering employees' access to sensitive applications and data is a central challenge for today's organizations.² Employers have many digital systems, and quite a few of them contain important financial and nonfinancial information. It is important that they manage employee access to all the various applications and information in a way that reduces risk. One key type of control to manage employees' transactions is role-based access control (RBAC) and attribute-based access control (ABAC). Both use roles and attributes assigned in the company directory to manage what employees can access and what privileges their accounts have.³

There are laws such as the Sarbanes-Oxley and Gramm-Leach-Bliley Acts that require specific monitoring of these systems in banks and publicly traded companies. These laws include requiring records of who accessed what systems, when (logs), and the ability to audit these logs.

¹ M. Kunz, M. Hummer, L. Fuchs, M. Netter, and G. Pernul, "Analyzing Recent Trends in Enterprise Identity Management," paper presented at the 2014 25th International Workshop on Database and Expert Systems Applications, Munich, 2014, 273-77. doi: 10.1109/DEXA.2014.62.

² Ibid.

³ Ibid.

A special type of account was created to manage a particular type of risk in enterprise systems. Privileged account management (PAM) or privileged identity management (PIM) tools are designed to support the access control to privileged accounts. Privileged accounts (administrative or root accounts) have a lot of power within IT systems, both in the overall IT system as well as in particular applications. Managing access to these became part of regulatory requirements due to high-profile fraud cases and major data breaches that occurred when these accounts were compromised. These accounts are very powerful and can be exploited by insiders and external attackers. It is critical that they are actively monitored so that unusual activity is flagged and investigated.

There is a special type of employee interaction that a whole suite of technology tools were built to help manage. When two companies collaborate or have the need to access one another's systems, an arrangement called Federation⁴ is deployed. It is both a legal agreement and set of technical protocols that permit the identity of an employee provisioned by one enterprise to be accepted within the identity management system of another enterprise. An example might be a technician, who works for the company that designed and built an airplane engine, getting access to the records of said engine within an airline's system. With a federation agreement, the airline does not have to "provision" an identity for the jet engine company employee. The airline just accepts the credentials presented by the employee of the jet engine company. One of the protocols used to manage this type of interaction is Security Assertion Markup Language.⁵

It is within this domain that companies delegate from the corporate entity to natural persons who act on their behalf in relationship to other corporate entities and with the government.

How Is It Similar to or Different from Government Transactions?

In this context, there is a clear power relationship: the employee whose identity is being managed works under or for the enterprise. The enterprise has control over the identifiers it issues to the employee and the authority to determine the scope of access, including terminating the account once the employee no longer works for the company. This power dynamic is very different from the relationship between a citizen and a government or between a customer and a supplier. Because of these differences, the terminology and technologies developed for enterprise identity and access management are not directly translatable to those other contexts.

⁴ Ping Identity, "SAML: How It Works," 2016, <https://www.pingidentity.com/en/resources/articles/saml.html>.

⁵ *Ibid.*

14. Employment Surveillance

Employment surveillance is something that happens in the workplace and isn't new. Taylorism was created in the early part of the twentieth century to track and shape how workers work in order to reduce employer costs and increase employee productivity. With the rise of computerized technology, its form is changing. When individuals work they are surveilled by their employers (Figure 14.1).

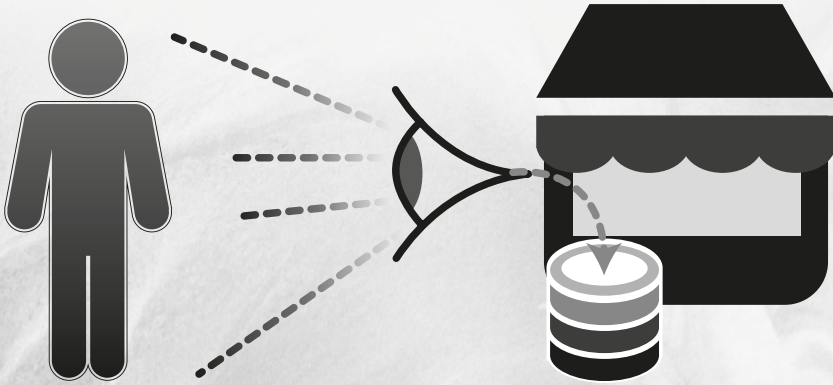


Figure 14.1. Employment surveillance. This happens when employers track employee behavior and actions both physically and digitally while they are at work. Surveillance may be extended beyond work.

Roles

- Employee
- Employer
- Contractor
- Service provider doing insider threat analysis
- Data loss prevention services provider

Types of PII

- Information about the employee
- All the data about the employees' work activity

Examples of Transactions

- Watching via CCTV employees while they work
- Physically searching employees when they leave work
- Tracking all employee activity in digital systems
- Logging employee entry and entrances to buildings and rooms

Sources of PII

- Information submitted to the employer during the application and registration processes
- All the activities done during work

Relationship to Other Domains

While individuals are doing their work, all the things in the domain of employment transactions, they are potentially being surveilled by their employer. Employers in the

process of hiring, which happens within the employment registration domain, may also surveil a prospective employee by researching them. Employers may also surveil employees while they are interacting in their everyday life with governments, the commercial sector, and civil society. Databases developed during the time of employment are vulnerable to theft and sale on the illicit market.

Description

We could think of employment surveillance as beginning when individuals apply for a job and the employer goes to find out more about them. A good term for this is “preenrollment surveillance” or preemployment surveillance practices. A traditional corporation pays thousands of dollars to learn a lot about a prospective employee before it makes a hiring decision.¹

What is surveillance in the context of the workplace? “Management’s ability to monitor, record and track employee performance, behaviors and personal characteristics in real time as part of organizational processes”.² Since the existence of organizations, surveillance to track what their employees are doing has been practiced.³ There was a particular time in the mid-nineteenth century when the expansion of the railways and other industries experienced growing organizational complexity. They used information technologies—paper, index cards, punch cards, and the telegraph—to manage the flow of information within the organization. By internalizing information about customers, pricing, and competitors, this means that firms avoid having to obtain it and they lower transaction costs.⁴

In the contemporary system we live in today, there’s a relationship between production, wages, and consumption. Fordism, the paying of wages high enough for workers to be middle-class consumers, impacts the demand side of the economy (the government does surveillance of the labor market), and Taylorism on the production side requires information for worker control. They operate in concert with each other.⁵

Europe at the time Fordism arose was focused on maximizing productivity on the assembly line to serve the employer. Europe developed the science of work to support improving how the employee did work, developing practices around ergonomics, for example, that have a focus on improved employee well-being.⁶

¹ Bob Blakley, *A Relationship Layer for the Web . . . and for Enterprises, Too* (Midvale, UT: Burton Group, 2007).

² Kirstie Ball, “Workplace Surveillance: An Overview,” *Labor History* 51, no. 1 (2010): 87–106. doi:10.1080/00236561003654776.

³ Ibid,

⁴ Kirstie Ball, “All Consuming Surveillance: Surveillance as Marketplace Icon,” *Consumption Markets & Culture* 20, no. 2 (2017): 95–100. doi:10.1080/10253866.2016.1163942.

⁵ Mark Andrejevic, “The Kinder, Gentler Gaze of Big Brother: Reality TV in the Era of Digital Capitalism,” *New Media & Society* 4, no. 2 (2002): 251–70. doi:10.1177/14614440222226361.

⁶ Christopher O’Neill, “Taylorism, the European Science of Work, and the Quantified Self at Work,” *Science, Technology, & Human Values* 42, no. 4(2016): 600–621. doi:10.1177/0162243916677083.

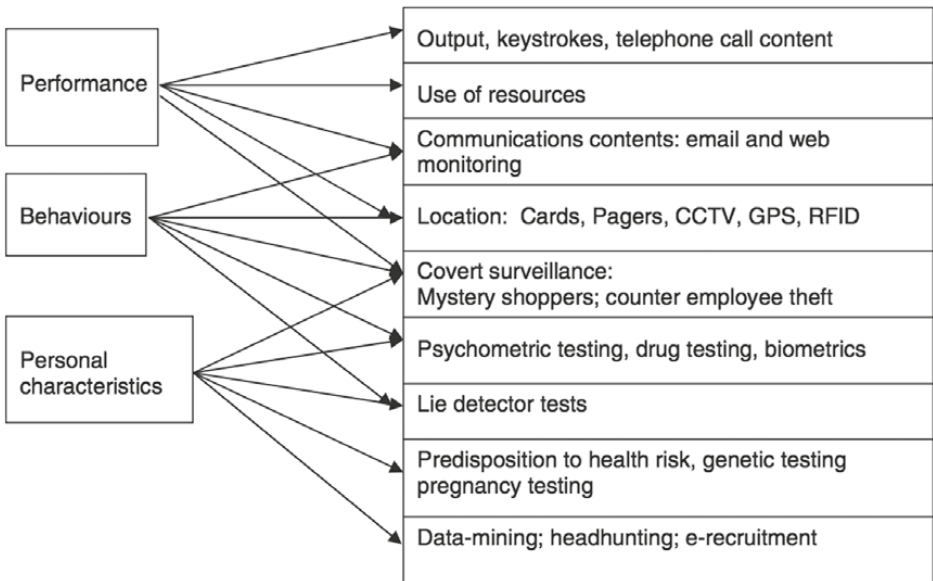


Figure 14.2. The range of employee surveillance techniques used by organizations.

The current debate about workplace surveillance began in the 1980s. This led to the US Office of Technology Assessment writing up a report, “Electronic Supervisor: New Technologies, New Tensions.”⁷ Two tracks of academic research have proceeded to engage with the topic. “Surveillance” is the term used by industrial and organizational sociologists concerned with power, politics, resistance, and meaning-making of employees. “Monitoring,” a term used by psychologists, doesn’t carry the dystopian baggage that surveillance does. However, the two terms are used interchangeably.

Workplace surveillance is very common place. A Forrester survey found that one-third of employers with more than a thousand employees hire people to review employee emails for rule breaking. Seventy-five of US companies monitor communication and on-the-job activities. Companies also do drug and alcohol testing.⁸ Companies don’t just monitor employees with data about their activity on the job. The trend toward team working has led to peer surveillance and the creation/enforcement of social and cultural norms via the social process of management.⁹

There is both overt and covert surveillance of employees. Westin, in a 1992 study, found that if employers implemented surveillance practices in a nonparticipatory way, it damages employee trust.¹⁰ It has been found in research that intensive monitoring by employers increases employee subversion of surveillance. Workplaces can get into negative loops with surveillance practices.

⁷ Ball, “Workplace Surveillance: An Overview.”

⁸ Ibid.

⁹ Ibid.

¹⁰ Ibid.

There are four main reasons that organizations surveil their employees: to maintain productivity, monitor resource use by employees, protect corporate interests including trade secrets, and to protect them from legal liability.¹¹ Figure 14.2¹² captures the full range of this surveillance.

Figure 14.2 makes clear that there is a whole range of activities that happen in the workplace that can be classified as surveillance. Performance evaluations, tracking of behaviors, and evaluation of personal characteristics are all common.

What Is the Connection between Self-Tracking and Employment Surveillance?

With the emergence of a whole range of self-tracking practices, individuals begin to self-monitor with various self-monitoring devices. There are five main self-tracking modes and dataveillance. Two at play in this domain are pushed, imposed, and exploited. “The workplace has become a key site of pushed self-tracking where financial incentives or the importance of contributing to team spirit and productivity may be offered for participating.”¹³ This is particularly common with digital wellness tools.

Imposed self-tracking happens with the use of RFID chips and other sensors that are used to monitor employees to “record sound, geo-location, and physical movement to monitor aspects of the wearers tone of voice, posture, and who they speak to and for how long.”¹⁴ Examples of this include the Humanyze and VoloMetrix tools created out of Sandy Pentland’s work to measure how people interact with each other within their organizations.¹⁵

¹¹ Ibid.

¹² Adapted from Priscilla Regan, “Genetic Testing and Workplace Surveillance: Implications for Privacy,” in *Computers, Surveillance and Privacy*, ed. D. Lyon and E. Zureik (Minneapolis: University of Minnesota Press, 1998), 21–46.

¹³ Deborah Lupton, “The Diverse Domains of Quantified Selves: Self-Tracking Modes and Dataveillance,” *Economy and Society* 45, no. 1 (2016): 101–22. doi:10.1080/03085147.2016.1143726.

¹⁴ Ibid.

¹⁵ O’Neill, “Taylorism, the European Science of Work.”

15. Data Broker Industry

The **data broker industry** collects and links together data about millions of people in massive databases. There is no direct relationship between the companies that do this and the individuals they gather or buy information about. While there is no direct relationship in the collection of the data, brokers who are subject to the Fair Credit Reporting Act are required to provide consumers access to the information they have about them and the ability to correct it. This industry gets the data they use to compile these databases from the government, civil society, and commercial and employment contexts. They package the data about people into digital dossiers and sell them raw or in the form of scores on which they rate the subjects in their database on dimensions important to their clients (Figure 15.1).

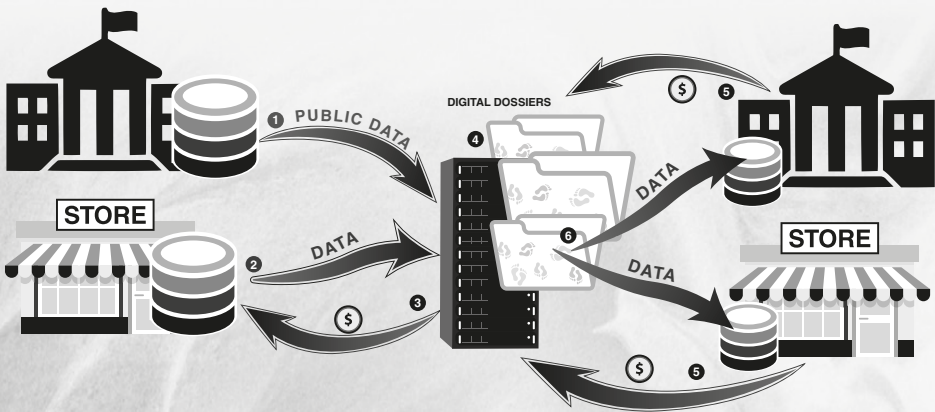


Figure 15.1. The data broker industry (1) draws data from public sources, (2) and (3) buys it from commercial sources, and (4) organizes it into digital dossiers about people. It (5) and (6) sells these digital dossiers to a whole range of entities including governments and commercial entities.

Roles

- Individuals whose data are in the data broker database
- Sources of data for the data broker databases
- Public records posted by government
- Civil society organizations with publicly available records
- Commercial entities that sell data to data brokers
- Civil society organizations that sell data to data brokers
- Organizations that buy data from data brokers

Examples of Transactions

- Buying data
- Collecting data
- Analyzing data and creating scores
- Selling lists of potential customers
- Selling scores about existing or potential customers

Types of PII

- Everything imaginable: some data brokers claim to have up to 3,000 data points on individuals

Sources of PII

- The databases of personal data from interactions individuals have with organizations in all the domains

Relationship to Other Domains

The data broker industry draws on data from all the government, commercial, civil society, and employment contexts. If the data are publicly available, the data broker companies will just take and use them. If the data are held in private databases, the companies will buy and integrate them with other data. The me and my identity and you and your identity domains have no direct relationship to the data broker industry domain because individuals do not contribute their data to, or interact in any direct way with, companies in this industry. Data brokers are vulnerable to data theft and having data breaches that end up on the illicit market.

Description

The data broker industry seems like it could not have evolved before the contemporary computer era; however, it began long before. The tracking of commercial creditworthiness began in the 1840s. The agencies doing this started tracking the personal habits of individuals in massive ledger books. By the late 1850s, they were publishing rating books on the creditworthiness of individuals. This created the modern concept of a financial identity.¹ The history of this mass consumer surveillance is integral to the development of modern consumer capitalism.

The data broker industry domain is similar but distinct from the commercial surveillance domain. In the data broker industry domain, as with the involuntary known and involuntary unknown types of commercial surveillance, there is no enrollment process. People do not “sign up” and do not know there is a row in a database associated with them.

With commercial surveillance, an individual actually knows they have entered into a context where there might be surveillance, such as going into a physical store or visiting a website. This is in contrast to data brokers that have absolutely no connection with the individuals they are collecting and aggregating information about. All of the information a data broker has about an individual comes from sources that do have some direct connection to the individuals.

Brokers draw on public records held by the government that were generated in the government registration process and subsequent government transactions that are publicly available. They buy and trade data from the commercial context. They use publicly available information from the civil society sector such as lists of licensed doctors and lawyers. The Federal Trade Commission (FTC) in a 2014 study of the data

¹ J. Lauer, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America* (New York: Columbia University Press, 2017).

broker industry found that it collects data from “numerous sources largely without consumer’s knowledge.”²

The data broker industry has an even greater informational asymmetry and power imbalance between individuals and institutions than in the domains described earlier. The amount of information data brokers aggregate on individuals from so many different contexts is huge. The current technology that provides even more intimate tracking of people, including whether they hesitated over but did not click on a link or how long they read each item on a page, only increases this asymmetry. It is also worth noting that other domains such as government surveillance, commercial surveillance, and employment surveillance use data purchased from the data broker industry to fill out data sets they have about individuals.

What Are the Types of Data Brokers?

The industry is regulated by the FTC, and it describes three different types of brokers.³

1. **Entities are subject to the Fair Credit Reporting Act (FCRA).** This legislation was passed in 1970. The law pertains to consumer information that is used for decisions involving credit, employment, and insurance. It protects data from disclosure to unauthorized persons. It requires data brokers, which it calls consumer reporting agencies, to maintain the accuracy of consumer report information in order to ensure that the information is not used incorrectly to deny consumer credit, employment, insurance, housing, or other rights. The Act also gives consumers the right to access data about them held by these agencies and correct mistakes in the data. It is enforced by the FTC.
2. **Non-FCRA-covered entities maintain data for non-marketing purposes that are outside of FCRA,** such as to detect fraud (mitigate risk) or locate people. For risk mitigation, clients use the data brokers’ service to check if identity information presented by a new potential buyer/client is accurate. For people location products, data brokers provide “people search” websites through which a user can search for publicly available information about consumers.
3. **Entities that maintain data for marketing purposes.** The products in this marketplace include the ability to buy a consumer’s email or mailing address to solicit them for business. Businesses can also purchase information about existing customers/clients. Data brokers offer a variety of products in this realm including analytic services to figure out what channels to use to advertise to consumers and consumer scores to figure how likely a prospect a person is. Data brokers have no obligation to share what data they have or where they got them with the individuals whose data they have. Some provide access to

² FTC (Federal Trade Commission), *Data Brokers: A Call for Transparency and Accountability* (2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

³ *Ibid.*

this information and some provide the ability to opt out of the use of their data for marketing purposes.

Where Does the Data Come From?

The data broker industry is complex. In a 2014 report by the FTC that looked into the detailed working of nine different brokers of different sizes, they found that the brokers sold and exchanged information with each other.

What Are the State and Local Government Data Sources?

State and local governments provide a wide variety of information, including:

- Professional licenses (e.g., licenses for pilots, doctors, lawyers, architects)
- Recreational licenses (e.g., hunting and fishing licenses)
- Real property and assessor records:
 - Taxes
 - Assessed value
 - Liens
 - Deeds
 - Mortgages
 - Mortgage releases
 - Pre-foreclosures
 - Identifying information about the owner
 - Information about the property (e.g., square footage, number of bathrooms and bedrooms, and whether the property has a pool)
- Voter registration information (e.g., name, address, date of birth, and party affiliation)
- Motor vehicle and driving records
- Court records
 - Criminal records
 - Civil actions and judgments
- Birth, marriage, divorce, and death records

What Are the Data Sources from the Commercial Sector?

- Retailers and merchants via cooperative databases
- Transaction data and customer lists
- Financial sector non-credit information
- Commercial data brokers
- Multichannel direct response
- Survey data, especially online
- Catalog/phone order/online order
- Warranty card registration
- Internet sweepstakes
- Kiosks
- Social media iterations
- Loyalty card data
- Website interaction, including specialty or knowledge-based websites

- Lifestyle information: fitness health, wellness centers, and so forth
- Subscriptions (online or offline content)

What Are the Data Sources in the Civil Society?

Nonprofit organization's member or donor lists
Professional license listings

How Many Data Brokers Are There?

There are about four thousand data brokers.⁴ The FTC does not have a list of companies that resell personal information. Privacy Rights Clearinghouse⁵ has identified over 240 companies that they have listed on their website. Ghostery, an ad- and cookie-blocking application, has identified 3,000 companies who do tracking.⁶

How Much Data Do Data Brokers Have?

According to the 2013 GAO report,⁷ there is a rapid increase in the amount of personal data circulating about people, and there are no statutes that address the new technologies such as mobile devices and online behavioral tracking.

Axiom has data on 700 million consumers worldwide and includes 3,000 propensities for nearly every US consumer. They manage 15,000 customer databases for 7,000 companies.⁸

Oracle has several data broker products and companies. BlueKai has 700 million global profiles from more than 200 data providers. Its primary market is online advertising and it works to combine first- and third-party tracking data to support personalized marketing and online targeting. Datalogix has data on \$2 trillion of consumer spending from 1,500 data partners and has data of about 110 million US households. Much of the data is derived from loyalty card programs. The Oracle Data Cloud has access to over one billion profiles and has 300 data partners. Oracle Data Graph unites device IDs for consumers and tracks 229 million of them. It works to match online consumer activity with offline activity via these device IDs.⁹

⁴ Kashmir Hill, "Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'," *Forbes*, December 19, 2013, <https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#4b600df81d53>.

⁵ Privacy Rights Clearinghouse (2017): <https://www.privacyrights.org>.

⁶ Wolfie Christl and Sarah Spiekerman, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy* (Wien: Facultas Verlags- und Buchhandels AG, 2016).

⁷ GAO (United States Government Accountability Office), "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent," *Report to Congressional Requesters*, December 2013, <https://www.gao.gov/assets/660/659572.pdf>.

⁸ Christl and Spiekerman, *Networks of Control*.

⁹ *Ibid.*

Experian has credit information on 220 million US consumers and demographic data on 235 million people living in 117 million households.¹⁰

ID Analytics has 700 billion instances of PII about more than 315 million unique people in the United States. It also has aggregated more than 1.7 billion consumer transactions that contain this PII including 2.9 million fraud reported events.¹¹

AnalyticsIQ has data about 210 million individuals in 110 million households and gets data from 120 different data sources.¹²

SenseNetworks uses mobile location data and analytics with profiles on 150 million mobile users. It processes 170 billion location data events per month, adding them to profiles.¹³

MasterCard has data on 95 billion transactions by its two billion card holders.¹⁴

The main trade association for the data broker industry states that their member products are used in more than nine billion transactions each year.¹⁵

Data Brokers and Data Breaches

The risk of data breaches exists across all the domains outlined in this book. However, it is the realm of the broker industry where breaches can be even more severe. The amount of data that is held by the companies in this industry is huge. There have been a number of major breaches that have affected this industry in the last 20 years.

ChoicePoint began life as a spin-off of Equifax in 1997. After that, it acquired 60 companies in what was a wave of consolidation of the local credit ratings/data broker companies into large national conglomerates. Its main business at the time of the breach was providing background checks to many of the top companies in the United States. The article written in 2007 states that ChoicePoint had acquired 19 billion public records. In 2005, the company had a breach of 163,000 records. This came to light because California had in place data breach notification laws that required reporting to residents.

The Experian data breach happened in 2015 and affected 15 million consumer records that were from T-Mobile customers.¹⁶

The Equifax breach happened in 2017 and affected 143 million consumers in the United States, Canada, and the United Kingdom. The breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers. They also stole

¹⁰ Ibid.

¹¹ Ibid.

¹² Ibid.

¹³ Ibid.

¹⁴ Ibid.

¹⁵ CDIA (Consumer Data Industry Association), "About CDIA," 2017, <https://www.cdiaonline.org/about/about-cdia/>.

¹⁶ Robert Hackett, "Experian Data Breach Affects 15 Million People Including T-Mobile Customers," *Fortune*, October 2, 2015, <http://fortune.com/2015/10/01/experian-data-breach-tmobile/>.

credit card numbers from about 209,000 people and dispute documents with PII from about 182,000 people.¹⁷

What Are Consumer Scores?

Consumer scores are distinct from credit scores that are regulated by FCRA. The World Privacy Forum defines them this way:

A consumer score describes an individual or sometimes a group of individuals (like a household), and predicts a consumer's behavior, habit or predilection. Consumer scores use information about consumer characteristics, past behaviors, and other attributes in statistical models that produce a numeric score, a range of scores or a yes/no. Consumer scores rate, rank, or segment consumers. Business and governments use scores to make decisions about innocuous to important. Businesses and others use consumer scores for everything from predicting fraud to predicting the health care costs of a [sic] individual to eligibility decisions to almost anything.¹⁸

A key issue with these scores, identified by the World Privacy Forum report,¹⁹ is that the scores are secret. The data types and sources that are used to create the scores are not known and there is no obligation to disclose them. Single scores can be composed of many hundreds if not thousands of factors and data streams.

There are thousands of different types of scores. Here is a sampling:²⁰

Cres predict, identify, and target marketing prospects in households likely to be profitable and pay debt.

The Job Security Score claims to predict future income and capacity to pay.

Churn Scores seek to predict when a customer will move his or her business or account to another merchant (eg. bank, cell phone, cable TV etc).

The Affordable Care Act (ACA) Health Risk Score creates a relative measure of predicted health care cost for particular enrollee. In effect, it is a proxy score for how sick a person is.

The Medication Adherence Score predicts how likely you are to take your medication according to your doctor's orders.

Fraud Scores indicate that a consumer may be masquerading as another, or that some other mischief is afoot. These scores are used everywhere from the post office, to point of sale retailers, to behind-the-scenes credit card transactions.

¹⁷ US Fed News Service, "Office of Information Technology Shares Details of Equifax Data Breach," September 13, 2017.

¹⁸ Pam Dixon and Robert Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* (San Diego, CA: World Privacy Forum, 2014).

¹⁹ Ibid.

²⁰ Ibid.

What Rights Do Consumers Have to Access the Data That Brokers Have about Them?

There is no overarching law in the United States that provides the right to know what information is held or who holds the data.²¹ Brokers regulated by the FCRA are required to provide consumers access to their own data that has been used to make decisions and, if it is erroneous, to correct it.²²

²¹ GAO (United States Government Accountability Office), "Information Security."

²² FTC (Federal Trade Commission), *Protecting Consumer Privacy in an Era of Rapid Change: Recommendation for Business and Policymakers* (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

16. Illicit Market

The illicit market is where the information about individuals ends up after it is stolen or hacked by criminals from any of the discussed domains, including data brokers. There are two primary types of illicit market activity: criminal networks and state-sponsored data theft and collection. Criminal networks are more likely managing the stolen data in spreadsheets rather than “organizational databases.” Data from state-sponsored theft are ending up in large databases and being correlated with other data sets from other sources, including publicly available data (Figure 16.1).

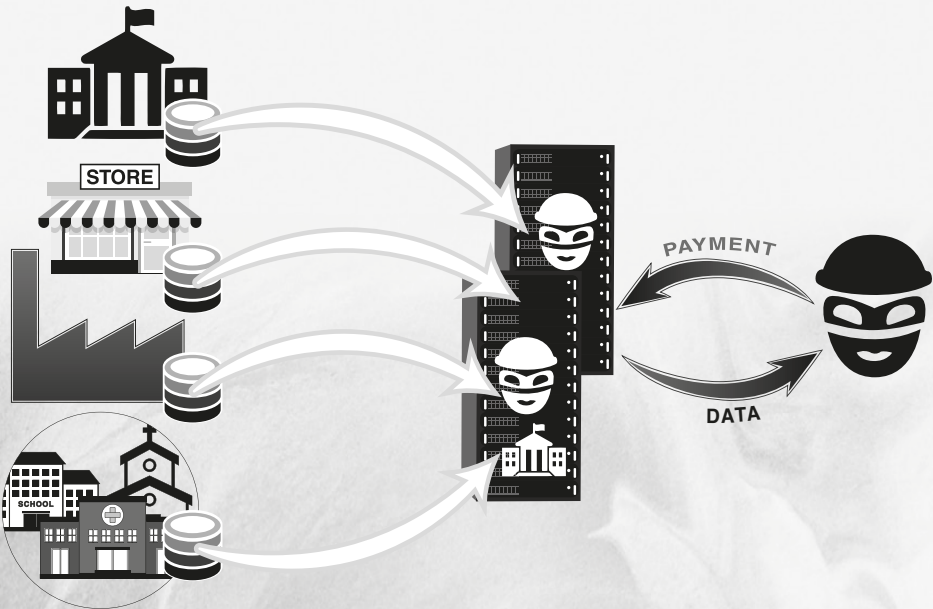


Figure 16.1. The illicit market is where criminals and state actors steal data (1) from all of the above contexts, government, commercial entities, employers, and civil society organizations. They resell this data to criminal enterprises (2) and (3).

Roles/Actors

- Individuals whose PII is taken by criminals or state actors
- Criminals who steal PII
- Companies who have their databases breached and data stolen
- Investigative agencies

Examples of Transactions

- Data theft
- Selling data on the illicit market
- Using data to compromise individuals for intelligence

Types of PII

- Any type of PII stored in any of the discussed domains since they are all vulnerable to by hacking by criminal or state actors

Sources of PII

- Databases that are stolen

Relationship to Other Domains

Actors from the illicit market are actively involved in stealing data from all of the other domains articulated in this research.

Description of the Illicit Market

The illicit market is where data stolen by criminals from large databases of PII are traded. Just like the data broker industry, there is no enrollment process for individuals and no direct connection between individuals and the entities stealing their data. The main difference between the illicit market actors and the data broker industry is that data brokers operate legally, buying data from their sources and then reselling it to other legitimate businesses. The illicit market actors are stealing the data of people and using it for criminal activity themselves or repackaging the data to sell to criminal enterprises.

We can also compare this domain to the categories of surveillance. It is not voluntary known surveillance because people don't agree to it. If you actually know your data was stolen because of a data breach notification, your condition is similar to the involuntary known state of surveillance. Individuals who know their data has been stolen can take steps to try and mitigate harm with credit freezes and credit-monitoring services. When individuals do not know their data has been stolen, it is similar to involuntary unknown surveillance.

The information asymmetry created between an individual and the actors in the illicit market is very high. This is especially true given that it is an entirely illegal activity. So, unlike some data brokers, illicit market actors have little or no incentive to provide a way to see information they hold about individuals. There is no way to know that actors in the illicit market hold information about particular individuals until they use the information to impersonate those individuals and take out accounts in their name.

A 2009 study determined that 60 percent of the time, identity theft is carried out by friends and family.¹ That is an individual using the PII of someone they know to open accounts in their name. One in six cases of identity theft are caused by purse snatching, pick-pocketing, burglary, or robbery.² Five percent of the thefts were the result of mail theft. None of these have to do with the breach of databases with PII. Since 2009, there has been a significant increase in criminal activity and data breaches.

In recent years, there have been many data breaches and thefts by what has been determined to be state actors. The Office of Personnel Management, which

¹ Martin T. Biegelman, "Chapter 18: Identity Theft Research," in *Identity Theft Handbook: Detection, Prevention, and Security* (Hoboken, NJ: John Wiley), 263–76.

² Ibid.

coordinates a range of employment functions for the federal government, suffered two big breaches in 2015. The first affected 4.2 million records and the second affected 21.5 million records, including Social Security numbers and sensitive information gathered in background checks.³ The investigation by the Federal Bureau of Investigation and others led to the conclusion that it was likely the Chinese state behind the breach. In August 2017, they arrested a Chinese national in connection with the breach.⁴

Anthem, a major health insurer, was attacked and 78 million records containing PII were stolen from its servers.⁵ The investigation about the hack has led back to the Chinese state sponsoring the theft.⁶ It is presumed that the Chinese are combining data from these thefts into large databases to gain an information advantage and potentially exploit the information to get access to defense and intelligence secrets.

³ P. Zengerle and M. Cassella, "Estimate of Americans Hit by Government Personnel Data Hack Skyrockets," *Reuters*, 2015. Retrieved July 9, 2015, <https://www.vox.com/2015/7/9/11614608/estimate-of-americans-hit-by-government-personnel-data-hack-skyrockets>.

⁴ Evan Perez, "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach," *CNN*, August 24, 2017, <https://edition.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html>.

⁵ Anna Wilde Mathews, "Anthem: Hacked Database Included 78.8 Million People," *Wall Street Journal*, February 24, 2015, <https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364>.

⁶ Michael Riley and Jordan Robertson, "Chinese State-Sponsored Hackers Suspected in Anthem Attack," *Bloomberg*, February 6, 2015, <https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack>.

CONCLUSION

The Domains of Identity covers a lot of ground. The first domain pertains to the individual and their data and the second domain covers the cases where an individual acts on behalf of another. These two domains are the source of data for the next twelve where individuals register, transact are surveilled by governments, civil society organizations, commercial entities and operate within the context of their employment.

In all of the above domains, there is a relationship between the individual and the entity but in some domains the individual may not be aware of the relationship. In the case of registration and transactions the relationship is explicit and understood by both parties. In the case of surveillance the individual is being passively watched/tracked by the institution but there is a one way relationship wherein data about an individual is flowing into the data systems of an institution with or without the individual's knowledge.


With the final two domains there is no connection between the individuals involved and their data. The data broker industry collects and links together data about millions of people in massive databases and then re-sells this data. The illicit market is where the information about individuals ends up after it is stolen or hacked by criminals from databases in any of the above domains.

I wrote this book to support a whole range of stakeholders being able to understand the domains and then use it to locate different identity management problems in a landscape. I also hope that it spurs others to do research that can address the challenges within and amongst different domains with new collaborations between industry and academia.

There are several significant research directions that arise from this book including:

- (1) Looking at complex use cases through the lens of the domains.
- (2) Considering how these 16 domains interact with one another. What different types of transactions and business/society activity happen within each intersection of these domains? This matrix of domains could then be used to understand various use cases and allow for the consideration where the keystone systems and infrastructure is missing.
- (3) Thinking through what legal and regulatory frameworks cover various domains and intersections of domains and considering what intersections are not well covered by existing laws. What are the gaps in the law or zones of un-regulation?
- (4) Classifying various identity and access management and other identity products into the different domains.

Identity systems are critical to how modern society operates. How these identity systems work, the laws surrounding them and the cultural norms shaping them have



huge implications for all people in all aspects of their lives. In the last several years there has been an enormous amount of attention paid to the ethical consequences and societal impacts of artificial intelligence and machine learning. Identity technologies are consequential and have received significantly less attention and investment by funders and philanthropists. I hope this work can inspire putting resources into the organizations like the Decentralized Identity Foundation, ID2020, MyData and the Me2B Alliance, that are proactively seeking to build and shape the development of new identity technologies that are good for people.

Bibliography

- ACLU. 2017. *Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy, a Report from the ACLU of Illinois*. http://dig.abclocal.go.com/wls/documents/Surveillance_Camera_Report.pdf.
- Adams, A., and S. Williams. 2014. "What's Yours Is Mine and What's Mine's My Own: Joint Accounts and Digital Identity." *ACM SIGCAS Computers and Society* 44, no. 1: 15–26. doi:10.1145/2602147.2602150.
- Adams, Samantha, Nadezhda Purtova, and Ronald Leenes. 2017. *Under Observation: The Interplay between eHealth and Surveillance*. Cham: Springer.
- Ajana, Btihaj. 2013. "Asylum, Identity Management and Biometric Control." *Journal of Refugee Studies* 26, no. 4: 576–95. doi:10.1093/jrs/fet030.
- Albrechtslund, Anders, and Peter Lauritsen. 2013. "Spaces of Everyday Surveillance: Unfolding an Analytical Concept of Participation." *Geoforum* 49: 310–16. doi:10.1016/j.geoforum.2013.04.016.
- Allen, C. 2016. "The Path to Self-Sovereign Identity." *Life with Alacrity Blog*. April 25. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.
- Althausser, J. 2017. "Governments Eye Blockchain in Their Creation of National Identity Systems." *CoinTelegraph*, October 6, <https://cointelegraph.com/news/governments-eye-blockchain-in-their-creation-of-national-identity-systems>.
- Andrejevic, Mark. 2002. "The Kinder, Gentler Gaze of Big Brother: Reality TV in the Era of Digital Capitalism." *New Media & Society* 4, no. 2: 251–70. doi:10.1177/14614440222226361.
- Asian Development Bank. 2007. *Legal Identity for Inclusive Development*. December. <https://www.adb.org/publications/legal-identity-inclusive-development>.
- . 2016. *Identity for Development in Asia and the Pacific*. November. <https://www.adb.org/publications/identity-development-asia-and-pacific>.

- Ball, Kirstie. 2005. "Organization, Surveillance and the Body: Towards a Politics of Resistance." *Organization* 12, no. 1: 89–108. doi:10.1177/1350508405048578.
- . 2010. "Workplace Surveillance: An Overview." *Labor History* 51, no. 1: 87–106. doi:10.1080/00236561003654776.
- . 2017. "All Consuming Surveillance: Surveillance as Marketplace Icon." *Consumption Markets & Culture* 20, no. 2: 95–100. doi:10.1080/10253866.2016.1163942.
- Balkan, A. 2016. "Digital Being." *Arena Magazine (Fitzroy, Vic)*, no. 143: 18–20.
- Bergen, Mark. 2017. "Google Adds YouTube to Suite of Ad Tools Tracking Retail Sales." *Bloomberg News*, May 23. <https://www.bloomberg.com/news/articles/2017-05-23/google-adds-youtube-to-suite-of-ad-tools-tracking-retail-sales>.
- Biegelman, Martin T. 2009. "Chapter 18: Identity Theft Research," in *Identity Theft Handbook: Detection, Prevention, and Security*, 263–76. Hoboken, NJ: John Wiley.
- Blakley, Bob. 2007. *A Relationship Layer for the Web . . . and for Enterprises, Too*. Midvale, UT: Burton Group.
- . 2017a. Personal communication with the author, October 6.
- . 2017b. Personal communication with the author, November 16.
- Borcea-Pfutzmann, Katrin, Marit Hansen, Katja Liesebach, Andreas Pfutzmann, and Sarah Steinbrecher. 2006. "What User-Controlled Identity Management Should Learn from Communities." *Information Security Technical Report* 11, no. 3: 119–28. doi:10.1016/j.istr.2006.03.008.
- Bohm, Nicholas, and Stephen Mason. 2010. "Identity and Its Verification." *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 1: 43–51. doi:10.1016/j.clsr.2009.11.003.
- Bollier, D. 2013. "Sousveillance as a Response to Surveillance." November 24. <http://www.bollier.org/blog/sousveillance-response-surveillance>.
- Lily Brag, entrepreneur building decentralized credential tracking systems for doctors. Interview with the author.
- Browne, S. 2015 (1973). *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
- Brumberg, H. L., D. Dozor, and S. G. Golombek. 2012. "History of the Birth Certificate: From Inception to the Future of Electronic Data." *Journal of Perinatology* 32, no. 6: 407–11. doi:10.1038/jp.2012.3.

- Bussard, Laurent, Anna Nano, and Ulrich Pinsdorf. "Delegation of Access Rights in Multi-Domain Service Compositions." *IDIS* 2 (2009):137-54. doi:10.1007/s12394-009-0031-5.
- Carracedo, Justo, Ana Gomez, Emilia Perez, and Sergio Sanchez. "Social and Legal Implications of Digital Identity in a Multi-national Environment." 2010 IEEE International Symposium on Technology and Society.
- Castells, Manuel. 2003. *The Power of Identity: The Information Age: Economy, Society, and Culture Volume II*. Malden, MA: Wiley-Blackwell.
- CBS News. 2001. "Smile! You're On Casino Camera." February 26. <https://www.cbsnews.com/news/smile-youre-on-casino-camera/>.
- Center for Popular Democracy. 2013. "Who We Are: Municipal ID Cards as a Local Strategy to Promote Belonging and Shared Community Identity." <https://populardemocracy.org/news/who-we-are-municipal-id-cards-local-strategy-promote-belonging-and-shared-community-identity>.
- CDIA (Consumer Data Industry Association). 2017. "About CDIA." <http://www.cdiaonline.org/about/index.cfm>.
- Chango, Mawaki. 2012. "Becoming Artifacts: Medieval Seals, Passports and the Future of Digital Identity." PhD dissertation, School of Information Studies. https://surface.syr.edu/it_etd/74.
- Christl, Wolfie, and Sarah Spiekerman. 2016. *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy*. Wien: Facultas Verlags- und Buchhandels AG.
- Clarke, Roger. 1988. "Information Technology and Dataveillance." *Communication of the ACM* 31, no. 5 (May 1988): 498-512. <http://www.rogerclarke.com/DV/CACM88.html>.
- . 1993. "Computer Matching and Digital Identity." Prepared for presentation at CFP'93. <http://www.rogerclarke.com/DV/CFP93.html>.
- . 1994a. "The Digital Persona and Its Application to Data Surveillance." *The Information Society* 10, no. 2: 77-92. <http://www.rogerclarke.com/DV/DigPersona.html>.
- . 1994b. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." *Information Technology & People* 7, no. 4: 6-37. <http://www.rogerclarke.com/DV/HumanID.html>.
- Clifford, Stephanie, and Quentin Hardy. 2013. "Attention, Shoppers: Store Is Tracking Your Cell." *New York Times*, July 14. <http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html>.

- Dahan, Mariana, and Alan Gelb. 2015. "The Role of Identification in the Post-2015 Development Agenda." World Bank Working Paper. <http://pubdocs.worldbank.org/en/149911436913670164/World-Bank-Working-Paper-Center-for-Global-Development-Dahan-Gelb-July2015.pdf>.
- digi.me. 2017. Accessed November 12, 2017. <https://www.digi.me/about>.
- Digital Beyond. 2017. *Online Services List*. <http://www.thedigitalbeyond.com/online-services-list/>.
- Dixon P. 2010. The One-Way-Mirror Society: Privacy Implications of the New Digital Signage Networks. <http://www.worldprivacyforum.org/wp-content/uploads/2013/01/onewaymirrorsocietyfs.pdf>.
- . 2013. *What Information Do Data Brokers Have on Consumers, and How Do They Use It?* Testimony of Pam Dixon, Executive Director, World Privacy Forum. http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf.
- . 2017. "A Failure to 'Do No Harm': India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S." Springer Nature, Health Technology. doi:10.1007/s12553-017-0202-6.
- Dixon, Pam, and Robert Gellman. 2014. *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*. San Diego, CA: World Privacy Forum.
- DocuSign. 2017. <http://www.docusign.com>.
- Drug Enforcement Agency (DEA). 2016. "State Prescription Drug Monitoring Programs." June. https://www.deadiversion.usdoj.gov/faq/rx_monitor.htm.
- Dubé, Line. 2016. Autopsy of a Data Breach: The Target Case. *International Journal of Case Studies in Management* 14, no. 1. https://www.academia.edu/35735325/Autopsy_of_a_Data_Breach_The_Target_Case.
- Duhigg, Charles. 2016. "How Companies Learn Your Secrets." *New York Times Magazine*, February 16. <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.
- Duncan, Jeffrey, Scott P. Narus, Stephen Clyde, Karen Eilbeck, Sidney N. Thornton, and Catherine J. Staes. 2015 (2014). "Birth of Identity: Understanding Changes to Birth Certificates and Their Value for Identity Resolution." *Journal of the American Medical Informatics Association* 22, no. e1: e120–e129. doi:10.1136/amiajnl-2014-002774.
- Earnst, Johannes. 2006. Image clipped from presentation by Johannes on use-centric digital identity.

- The Economist. 2015. "Digital Taylorism." *The Economist*, September 10, 2015. <https://www.economist.com/business/2015/09/10/digital-taylorism>.
- Erp, S., and A. Bennett. 2017. "Presentation: A State Government Perspective: Cybersecurity and People." MSIMS Class.
- The Early Edition. 2015. "1st Canadian Family with 3 Parents on Birth Certificate Grows." *CBC News*, February 9. <http://www.cbc.ca/news/canada/british-columbia/1st-canadian-family-with-3-parents-on-birth-certificate-grows-1.2950107>.
- Emanuel, Gabrielle. 2014. "Three (Parents) Can Be a Crowd, But for Some It's a Family." *WBUR News*. March 30. <http://www.wbur.org/npr/296851662/three-parents-can-be-a-crowd-but-for-some-its-a-family>.
- Estonia. 2017. "What is E-residency?" <https://e-resident.gov.ee>.
- European Commission. 2005. *Biometrics at the Frontiers: Assessing the Impact on Society*. Brussels: European Commission. <https://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf>.
- . 2017. "Information Providers Guide: Cookies." http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm.
- European Union. 2005. "Signposts towards eGovernment 2010." https://web.archive.org/web/20060711185811/http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf.
- Evernym. 2017. <http://www.evernym.com>.
- Everplans. 2017a. "How to Name a Digital Executor." <https://www.everplans.com/articles/how-to-name-a-digital-executor>.
- Everplans. 2017b. "State-by-State Digital Estate Planning Laws." <https://www.everplans.com/articles/state-by-state-digital-estate-planning-laws>.
- Exploring Privacy. 2009. "Personal Data Ecosystem." Submitted to the Federal Trade Commission. https://www.aclu.org/files/pdfs/privacy/dataeco_full.pdf.
- Foster, John B., and Robert W. McChesney. 2014. "Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age." *Monthly Review* 66, no. 3: 1.
- Frey, Chris. 2016. "Revealed: How Facial Recognition Has Invaded Shops – and Your Privacy." *Guardian*, March 3. <https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto>.

- FTC (Federal Trade Commission). 2012. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*. <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.
- . 2014. *Data Brokers: A Call for Transparency and Accountability*. <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.
- Fuchs, Christian. 2013. "Political Economy and Surveillance Theory." *Critical Sociology* 39, no. 5: 671–87. doi:10.1177/0896920511435710.
- GAO (United States Government Accountability Office). 2011. Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards. Report to Congress Requestors.
- . 2013. "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent." *Report to Congressional Requesters*, December. <https://www.gao.gov/assets/660/659572.pdf>.
- Gill, B. C., A. M. Zampini, and N. B. Mehta. 2015. "Digital Identity: Develop One before You're Given One." *Urology* 85, no. 6: 1219–23. doi:10.1016/j.urology.2015.02.056.
- Goffman E. 1959. *Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.
- GOV.UK. "Guidance GOV.UK Verify." <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>.
- Groebner, V. 2001. "Describing the Person, Reading the Signs in Late Medieval and Renaissance Europe: Identity Papers, Vested Figures, and the Limits of Identification, 1400–1600," in *Documenting Individual Identity*, edited by J. Caplan and J. Torpey, 15–27. Princeton, NJ: Princeton University Press.
- GSMA & Security Identity Alliance. 2014. *Mobile Identity - Unlocking the Potential of the Digital Economy: A Joint White Paper by GSMA and SIA*. https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf.
- GSMA. 2016. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation: A Joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper, June*.
- Hackett, Robert. 2015. "Experian Data Breach Affects 15 Million People Including T-Mobile Customers." *Fortune*, October 2. <http://fortune.com/2015/10/01/experian-data-breach-tmobile/>.

- Hagel, J. I., and J. F. Rayport. 1997. "The New Infomediaries." *McKinsey Quarterly*, no. 4: 54.
- Hammond, W. Ed. 1997. "The Use of the Social Security Number as the Basis for a National Citizen Identifier," in *The Unpredictable Certainty: White Papers*, 286–91. Washington, DC: The National Academies Press. <https://www.nap.edu/read/6062/chapter/37#289>.
- Harbitz, Mia Elizabeth. 2013. "The Civil Registry: A neglected dimension of international development." Inter-American Development Bank, Knowledge and Management Sector, Technical Note, May. <https://publications.iadb.org/publications/english/document/The-Civil-Registry-A-Neglected-Dimension-of-International-Development.pdf>.
- Harbitz, Mia Elizabeth, and Iván Axt Arcos. 2011. "Identification and Governance Policies: The Legal, Technical and Institutional Foundations That Influence the Relations and Interactions of the Citizen with the Government and Society." Inter-American Development Bank, Institutional Capacity and Finance Sector, Technical Notes, September. <https://publications.iadb.org/publications/english/document/Identification-and-Governance-Policies-The-Legal-Technical-and-Institutional-Foundations-that-Influence-the-Relations-and-Interactions-of-the-Citizen-with-the-Government-and-Society.pdf>.
- Harper, Jim. 2014. "REAL ID: A State-by-State Update." *Cato Institute*, Policy Analysis Number 749. May 12. <https://www.cato.org/publications/policy-analysis/real-id-state-state-update>.
- Higgs, E. 2004. *The Information State in England: The Central Collection of Information on Citizens since 1500*. Basingstoke: Palgrave Macmillan.
- Hill, Kashmir. 2012. "How Target Figured Out A Teen Girl Was Pregnant Before Her Father." *Forbes*. February 16. <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#160ea0796668>.
- . 2013. "Data Broker Was Selling Lists of Rape Victims, Alcoholics, and 'Erectile Dysfunction Sufferers'," *Forbes*, December 19. <https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#4b600df81d53>.
- Hoffman, Jascha. 2006. "Sousveillance." *New York Times Magazine*, December 10. <https://www.nytimes.com/2006/12/10/magazine/10section3b.t-3.html>.
- Holden, Stephen H., and Lynette I. Millett. 2005. "Authentication, Privacy, and the Federal E-Government." *The Information Society* 21, no. 5: 367–77. doi:10.1080/01972240500253582.

- Homeland Security. 2004. "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors." <https://www.dhs.gov/homeland-security-presidential-directive-12>.
- Hunter, Wendy, and Robert Brill. 2016. "'Documents, Please': Advances in Social Protection and Birth Certification in the Developing World." *World Politics* 68, no. 2: 191–228. doi:10.1017/S0043887115000465.
- ICE (Immigration and Customs Enforcement). 2017. "Law Enforcement Information Sharing Initiative." <https://www.ice.gov/le-information-sharing>.
- ID2020. 2017. <http://www.id2020.org>.
- IDology. 2017. "Dynamic KBA." <https://www.idology.com/identity-verification-solutions/dynamic-kba/>.
- Indie Web Camp. 2017. "Main Page." <https://indieweb.org>.
- Internet Identity Workshop (IIW). 2005–18. <http://www.internetidentityworkshop.com>.
- Jacobsen, Elida K. U. 2012. "Unique Identification: Inclusion and Surveillance in the Indian Biometric Assemblage." *Security Dialogue* 43, no. 5: 457–74. doi:10.1177/0967010612458336.
- John, A. 2017. "Identity Management & Data Privacy Research, Development and Transition." Department of Homeland Security, Science and Technology. Slide Presentation.
- Jordan, Ken, Jan Hauser, and Steven Foster. 2003. "The Augmented Social Network: Building Identity and Trust into the Next-Generation Internet." *First Monday* 8, no. 8. <https://journals.uic.edu/ojs/index.php/fm/article/view/1068/988>.
- Kantara Initiative. 2017. "User Managed Access (UMA)." <https://kantarainitiative.org/confluence/display/uma/Home>.
- Kearns, D., Kuppinger M. 2014, May. *IAM predictions and Recommendations 2014–2018: KuppingerCole Report Advisory Note*. Germany, KuppingerCole.
- Kertzer, David, and Arel Dominique. 2002. *Census and Identity: The Politics of Race, Ethnicity, and Language in National Censuses*. Cambridge: Cambridge University Press.
- Kim, Mun-Cho. 2004. "Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea." *International Sociology* 19, no. 2: 193–213. doi:10.1177/0268580904042900.

- Known. 2017. <http://www.withknown.com>.
- Kundra, Shivani, Aman Dureja, and Riya Bhatnagar. 2014. "The Study of Recent Technologies Used in E-Passport System," in *2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS)*, 141–46. Trivandrum: 2014. doi:10.1109/GHTC-SAS.2014.6967573.
- Kunz, M., M. Hummer, L. Fuchs, M. Netter, and G. Pernul. 2014. "Analyzing Recent Trends in Enterprise Identity Management." Paper presented at the 2014 25th International Workshop on Database and Expert Systems Applications, Munich, 2014, 273–77. doi:10.1109/DEXA.2014.62.
- KuppingerCole, M. 2014. *Enterprise Single Sign-On, KuppingerCole Report: Leadership Compass*. Germany, KuppingerCole. <https://www.kuppingercole.com/report/lc70962>.
- Ladner, Debra, Erik G. Jensen, and Samuel E. Saunders. 2014. "A Critical Assessment of Legal Identity: What It Promises and What It Delivers." *Hague Journal on the Rule of Law* 6, no. 1: 47–74. doi:10.1017/S1876404513000043.
- Lauer, J. 2017. *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York: Columbia University Press.
- Laurent, Maryline, and Samia Bouzefrane. 2015. *Digital Identity Management*. London: Iste Press.
- Levy, Karen E. C. 2015. "Intimate Surveillance." *Idaho Law Review* 51, no. 3: 679–93.
- Loffreto, Devon. 2016. "Moxy Tongue Blog." February 9, 2016. <https://www.moxytongue.com/2016/02/self-sovereign-identity.html>.
- Luppicini, Rocci. 2013. *Handbook of Research on Technoself: Identity in a Technological Society* (2 volumes). Hershey, PA: Information Science Reference.
- Lupton, Deborah. 2016. "The Diverse Domains of Quantified Selves: Self-Tracking Modes and Dataveillance." *Economy and Society* 45, no. 1: 101–22. doi:10.1080/03085147.2016.1143726.
- Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Milton Keynes: Open University Press.
- . 2006 (1948). *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan.
- Mathews, Anna Wilde. 2015. "Anthem: Hacked Database Included 78.8 Million People." *Wall Street Journal*, February 24. <https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364>.

- Martin, Zack. 2014. "British Columbia Issues Combined ID for Driver License, Health, Online Use." *SecureIDNews*, June 5. <https://www.secureidnews.com/news-item/british-columbia-issues-combined-id-for-driver-license-health-online-use/>.
- Marx, Gary T. "I'll Be Watching You: Reflection on the New Surveillance." *Dissent Magazine* 32, no. 1(Winter 1985): 26–34.
- Meeco.me. 2017. *You are Not the Product*. Retrieved November 12, 2017. <https://meeco.me/why-meeco.html>.
- Mei, Sarah (@sarahmei). 2017a. "Today's OH FFS SOFTWARE INDUSTRY: the @SFUnified saas for parents to track student progress can only issue one parent account per student." *Twitter*, September 6, 4:58 a.m. <https://twitter.com/sarahmei/status/905211153634148352>.
- . 2017b. "I'm lucky I have a good relationship with my co-parent, who got the one account. Otherwise I'd have no visibility into anything." *Twitter*, September 6, 5:01 a.m. <https://twitter.com/sarahmei/status/905211804191621121>.
- . 2017c. "I'm having a really hard time imagining the circumstances under which assuming 'every kid only has one main parent' is a good idea." *Twitter*, September 6, 5:25 a.m. <https://twitter.com/sarahmei/status/905217920082485248>.
- . 2017d. "Or, I guess, you're assuming they're ok with sharing login credentials (which I wasn't even comfortable with when married, & less so now)." *Twitter*, September 6, 5:35 a.m. <https://twitter.com/sarahmei/status/905220451051249664>.
- Meiser, Kenneth Donaldson. 2018. *Opening Pandora's Box: The Social Security Number from 1937–2018*. Austin: University of Texas.
- Millet, Lynette I., and Joseph N. Pato. 2010. *Biometric Recognition: Challenges and Opportunities*. Washington, DC: National Academies Press.
- Mordini, Emilio, and Andrew P. Rebera, 2012. "No Identification without Representation: Constraints on the Use of Biometric Identification Systems." *Review of Policy Research* 29, no. 1: 5–20. doi:10.1111/j.1541-1338.2011.00535.x.
- News 1130. 2013. "BC Begins Phasing Out Care Cards Soon." January 7. <http://www.news1130.com/2013/01/07/bc-begins-phasing-out-care-cards-soon/>.
- NCSL (National Council of State Legislatures). 2010. "Social Security Number 2010 Legislation." <http://www.ncsl.org/research/financial-services-and-commerce/social-security-number-2010-legislation.aspx>.

- NIST National Institute of Standards and Technology. 2013. "Personal Identity Verification (PIV) of Federal Employees and Contractors." *Federal Information Processing Standards Publication*, August 2013. doi:10.6028/NIST.FIPS.20
- Northam, Sally, Shea Polancich, and Elizabeth Restrepo. 2003. "Birth Certificate Methods in Five Hospitals." *Public Health Nursing* 20, no. 4: 318–27. doi:10.1046/j.1525-1446.2003.20409.x.
- OASIS Security Services (SAML) TC. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.
- OAuth. 2017. <https://oauth.net>.
- OBIM (Office of Biometric Identity Management). 2017. "Biometrics." *Department of Homeland Security*. <https://www.dhs.gov/biometrics>.
- OECD (Organisation for Economic Cooperation and Development). 1980. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.
- . 2007. "At a Crossroads: 'Personhood' and Digital Identity in the Information Society," Directorate for Science, Technology and Industry, STI Working Paper 2007/7, February 29, 2008.
- Office of the Assistant Secretary for Planning and Evaluation. 1973. "Records, Computers and the Rights of Citizens." July 1. <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>.
- O'Neill, Christopher. 2016. "Taylorism, the European Science of Work, and the Quantified Self at Work." *Science, Technology, & Human Values* 42, no. 4: 600–621. doi:10.1177/0162243916677083.
- Oxford Internet Institute (OII). 2016 "GDPR: The Right to Be Forgotten." <https://www.oii.ox.ac.uk/blog/gdpr-the-right-to-be-forgotten/>.
- Pearson, S. J. 2015. "'Age Ought to Be a Fact': The Campaign against Child Labor and the Rise of the Birth Certificate." *Journal of American History* 101, no. 4: 1144–65. doi:10.1093/jahist/jav120.
- Peeters Roel, Koen Simoens, Danny De Cock, and Bart Preneel B. 2008. "Cross-Context Delegation through Identity Federation," in *BIOSIG 2008: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, edited by Arslan Brömme, Christoph Busch, and Detlef Hühnlein, 79–92. Bonn: Gesellschaft für Informatik.

- Perez, Evan. 2017. "FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach." *CNN*, August 24. <https://edition.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html>.
- PDEC (Personal Data Ecosystem Consortium). 2017. "History." <http://pde.cc/aboutus/history/>.
- Ping Identity. 2016. "SAML: How It Works." <https://www.pingidentity.com/en/resources/articles/saml.html>.
- Pon, Bryan, Chris Locke, and Tom Steinberg. 2016. *Private-Sector Digital Identity in Emerging Markets*. Surrey: Caribou Digital. <https://www.cariboudigital.net/wp-content/uploads/2019/01/Caribou-Digital-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf>.
- Privacy Rights. 2017. <https://www.privacyrights.org>.
- Regan, Priscilla. "Genetic Testing and Workplace Surveillance: Implications for Privacy," in *Computers, Surveillance and Privacy*, edited by David Lyon and Elia Zureik, 21–46. Minneapolis: University of Minnesota Press, 1998.
- Reed, Drummond, and Les Chasen. 2016. "Requirements for DIDs (Decentralized Identifiers)." Rebooting the Web of Trust II: ID2020 Design Workshop.
- Richmond, Emily. 2013. "Tagging Students." *Scholastic Administrator*. <http://www.scholastic.com/browse/article.jsp?id=3757964>.
- Riley, Michael A., and Jordan Robertson. 2015. "Chinese State-Sponsored Hackers Suspected in Anthem Attack." *Bloomberg*, February 6. <https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack>.
- Reuben, William and Flávia Carbonari. 2017. "Identification as a National Priority: The Unique Case of Peru." Center for Global Development, Working Paper 454. <https://www.cgdev.org/sites/default/files/identification-national-priority-unique-case-peru.pdf>.
- Royal Society of Engineering. 2007. Dilemmas of Privacy and Surveillance: Challenges of Technological Change. <https://www.raeng.org.uk/publications/reports/dilemmas-of-privacy-and-surveillance-report>.
- Sarbanes–Oxley Act. Pub. L. 107–204. 116 Stat. 745. July 30, 2002.
- Sánchez García, S., A. Gómez Oliva, E. Pérez Belleboni, E., and I. Pau de la Cruz. 2011. "Solving Identity Delegation Problem in the E-Government Environment." *International Journal of Information Security* 10, no. 6: 351–72. doi:10.1007/s10207-011-0140-7.

- SFUSD (San Francisco Unified School District). 2016. "Student and Family Handbook 2016–17." <https://www.sfusd.edu/en/assets/sfusd-staff/parent%20resources/files/2016–2017%20SH-%20FINAL%20English.pdf>.
- Sawers, Paul. 2016. "Amazon Launches Amazon Go, a Mind-Blowing Brick-and-Mortar Grocery Store with No Checkouts." *Venture Beat*, December 5, 2016. <https://venturebeat.com/2016/12/05/amazon-launches-amazon-go-a-brick-and-mortar-grocery-store-that-does-away-with-checkouts/>.
- Scahill, Jeremy, and Margot Williams. 2015. "STINGRAYS: A Secret Catalogue of Government Gear for Spying on Your Cellphone." *The Intercept*, December 17. <https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/>.
- Schmidt, Howard A. 2010. "The National Strategy for Trusted Identities in Cyberspace." June 25. <https://obamawhitehouse.archives.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace>.
- Secure Identity Alliance. 2015. *Civil Registry Consolidation through Digital Identity Management*. December. <https://secureidentityalliance.org/publications-docman/public/7-15-12-17-civil-registry-consolidation-digital-identity-sia-final/file>.
- Sheard, Nathan. 2017. "Oakland Privacy and the Fight for Community Control." *Electronic Frontier Foundation*, October 26. <https://www.eff.org/deeplinks/2017/10/oakland-privacy-and-fight-community-control>.
- Swann, W. B., Jr., and J. K. Bosson. 2010. "Self and Identity." In *Handbook of Social Psychology*, edited by S. T. Fiske, D.T. Gilbert, & G. Lindzey, 589–628. Hoboken, NJ: Wiley.
- Szreter, Simon. 2007. "The Right of Registration: Development, Identity Registration, and Social Security—A Historical Perspective." *World Development* 35, no. 1: 67–86. doi:10.1016/j.worlddev.2006.09.004.
- Tham, Irene. 2017a. "All SingPass Users to Be Auto Enrolled in Digital Data Vault MyInfo by Year End." *Straits Times*, September 26. <https://www.straitstimes.com/tech/all-singpass-users-to-be-auto-enrolled-in-digital-data-vault-myinfo-by-year-end>.
- . 2017b. "Watchdog Seeks Stricter Protection of NRIC Data." *Straits Times*, November 8. <https://www.straitstimes.com/tech/watchdog-seeks-stricter-protection-of-nric-data>.
- ThreatMetrix. 2017. <https://www.threatmetrix.com>.
- Tizor. 2006. "Privileged User Monitoring for SOX Compliance." https://web.archive.org/web/20160910074615/https://www.computerworlduk.com/cmsdata/whitepapers/3592/tizor_sox_comp_wp.pdf.

- Tracy, S. J., and A. Trethewey. 2005. "Fracturing the Real-Self↔Fake-Self Dichotomy: Moving toward 'Crystallized' Organizational Discourses and Identities." *Communication Theory* 15: 168–95. doi:10.1111/j.1468-2885.2005.tb00331.x.
- Turack, D. C. 1972. *The Passport in International Law*. Lexington, MA: Lexington Books.
- UNICEF (United Nations Children's Fund). 2013. *Every Child's Birth Right: Inequities and Trends in Birth Registration*. New York: Data and Analytics Section, Division of Policy and Strategy. https://www.un.org/ruleoflaw/files/Embargoed_11_Dec_Birth_Registration_report_low_res.pdf.
- US Fed News Service. 2017. "Office of Information Technology Shares Details of Equifax Data Breach." September 13.
- USA Water Polo. 2017. "FAQ - Birth Date Verification." <https://web.archive.org/web/20180702045937/http://www.usawaterpolo.org/membership/faq-birthdate-verification-faqs.html>.
- US Government Publishing Office. 2015. *What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Thirteenth Congress, First Session, December 18, 2013*. Washington, DC: U.S. Government Publishing Office. <https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf>.
- US General Services Administration. "Login.gov." <https://login.gov>.
- Valinsky, Jordan. 2017. "Whole Foods Is Stealing Walmart and Trader Joe's Customers with Its Low Prices." *CNN Money*, October 3. <http://money.cnn.com/2017/10/03/news/companies/whole-foods-competition/index.html>.
- Verble, Joseph. 2014. "The NSA and Edward Snowden: Surveillance in the 21st Century." *ACM SIGCAS Computers and Society* 44, no. 3: 14–20. doi:10.1145/2684097.2684101.
- Verma, Ashish Kumar. 2016. "Public Transportation and Verification by Aadhar Card." *i-manager's Journal on Information Technology* 5, no. 4: 11–19. doi: 10.26634/jit.5.4.10333.
- Wagner, Kurt. 2016. "Facebook's New Ads Will Track Which Stores You Visit: Facebook Wants to Prove That Its Ads Lead to Actual Purchases." *ReCode*, June 14. <https://www.recode.net/2016/6/14/11926124/facebook-ads-track-store-visits-retail-sales>.
- Watkins, Peter. 2007. "Trust and Identity Management: Experience and Perspective from the Province of British Columbia, Canada." Trust Conference: e-Government

- Identity Management Initiatives, The Hague, Netherlands, November 21. <http://www.lbbc.leg.bc.ca/public/PubDocs/bccdocs/437299/BCPaperTrustandIdentityManagement.pdf>.
- WEF (World Economic Forum). 2011. *Personal Data: The Emergence of a New Asset Class*. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.
- . 2012. *Rethinking Personal Data: Strengthening Trust*. <https://identitywoman.net/wp-content/uploads/WEF2.pdf>.
- . 2016. *A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity*. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.
- Wermüller, Ben. 2016. "Stop Writing Specs, Start Finding Needs – What I've Learned Working on Known." February 22. <https://werd.io/2016/stop-writing-specs-start-finding-needs---what-ive-learned>.
- Wilson, Amy Blank. 2009. "It Takes ID to Get ID: The New Identity Politics in Services." *Social Service Review* 83, no. 1: 111–32. doi:10.1086/599025.
- WiSER (Wits Institute for Social and Economic Research). 2017. "FutureID2: Johannesburg Agenda." *Implications of New Technology for Civil Registration and Identification: Research and Policy*, University of the Witwatersrand, Johannesburg, February 14–16, 2017. <http://wiser.wits.ac.za/future-identity>.
- Wolf, Gary. 2010. "The Data Driven Life." *New York Times*, April 28. <https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html>.
- Wood, David M., and Kirstie Ball. 2013. "Brandscapes of Control? Surveillance, Marketing and the Co-Construction of Subjectivity and Space in Neo-Liberal Capitalism." *Marketing Theory* 13, no. 1: 47–67. doi:10.1177/1470593112467264.
- World Bank Group. 2016. *Identification for Development: Strategic Framework*. January 25. <http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf>.
- Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Wadhwa, and Didier Bigo. 2010. "Sorting Out Smart Surveillance." *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 4: 343–54. doi:10.1016/j.clsr.2010.05.007.
- Yang, Bian, Christoph Busch, Julien Bringer, Els Kindt, Willem Ronald Belser, Uwe Seidel, Edward Springmann, Uwe Rabelre, and Magnar Aukrust. 2013. "Towards Standardizing Trusted Evidence of Identity," in *DIM '13: Proceedings of the 2013*

ACM Workshop on Digital Identity Management, edited by Thomas Groß and Marit Hansen, 63–72. New York: Association for Computing Machinery. doi:10.1145/2517881.2517890.

Yoti. 2017. <http://www.yoti.com>.

Young, Kaliya. 2019. "Key Differences between the U.S. Social Security System and India's Aadhaar System." *The Promise of Public Interest Technology: In India and the United States*, *New America*. <https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/key-differences-between-the-us-social-security-system-and-indias-aadhaar-system-kaliya-young/>.

Yubico. 2017. "Why Yubico for Individuals." <https://www.yubico.com/why-yubico-for-individuals/>.

Zengerle, P., and M. Cassella. 2015. "Estimate of Americans Hit by Government Personnel Data Hack Skyrockets". *Reuters*. Retrieved July 9, 2015. <https://www.vox.com/2015/7/9/11614608/estimate-of-americans-hit-by-government-personnel-data-hack-skyrockets>.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1: 75–89. doi:10.1057/jit.2015.5.

Index

- Aadhaar system, Indian 28, 52
- ABAC. *See* attribute-based access control
- American Indians status 18
- anima 11
- Anthem 105
- anti-money laundering (AML) regulations 58
- applicant surveillance 84
- artificial intelligence (AI) 23
- attribute-based access control (ABAC) 88
- authentication 46–47
 - vs. enrollment 3233
 - factors 64
- Balkan, Aral 14
- “beacon” technology 80
- Big Data 64, 81
- biometrics, in government registration 31–32
 - acquisition stage of 31
 - definition 31
 - enrollment stage of 31
 - matching stage of 32
 - storage stage of 31
- birth certificates 27–28, 30–31, 34, 51
- birth registration 26–28
 - origins of 40–41
 - universal 41–42
- Blakley, Bob 22
- breeder document. *See* birth certificates
- Brown, Simone 68
- Canadian Tire Dollars 58
- Castells, Manuel 10
- CCTV cameras 74, 79
- Chango, Mawaki 37
- child labor laws 41
- civil society registration 6, 34, 49–52
 - delegation 52
 - enrollment, process of 50–51
 - examples of 49
 - vs. government registration 51
 - identity proofing for individuals 51–52
 - PII 50
 - relationship to other domains 50
 - roles of 49, 52
- civil society surveillance 7, 73–75
 - conduct 75
 - description and relevant literature 74–75
 - examples 73
 - PII 73
 - relationship to other domains 73
 - roles/actors 73
- civil society transactions 6, 53–56
 - data, collection and management of 55
 - digital management 55
 - initial registration and ongoing interaction, relationship between 54
 - membership in organization, prove of 55–56
 - PII 53
 - relationship to other domains 54
 - roles 53
 - technology of paper in 54
 - types 53
- Clarke, Roger 11, 69
- commercial registration 6, 57–61
 - enrollment
 - online, process of 59
 - in person, process of 58–59
 - second stage of 59–60
 - examples of 57
 - explicit 60
 - implicit 60–61
 - vs. government registration 60
 - PII 57
 - relationship to other domains 57–58
 - roles 57
 - un-enroll 61
- commercial surveillance 7, 77–81
 - in enterprises 78–79
 - examples 77
 - grey zone 81
 - kinds 79
 - known involuntary surveillance 79–80
 - unknown involuntary surveillance 80–81
 - voluntary surveillance 79
 - PII 77
 - relationship to other domains 77–78
 - roles 77
- commercial transactions 6, 63–65
 - data 64
 - examples 63
 - individuals use identifier from registration for 64

commercial transactions (*cont.*)

- PII 63
- records 64
- regulation in Europe 65
- relationship to other domains 64
- roles 63

corporations 38

credential 30

Cromwell, Thomas 40

customer oriented infomediaries 22

Dark Matters: On the Surveillance of Blackness 68

data breaches/thefts 100–101, 104–5

data broker industry 8, 95–102

- consumer score 101
- data 98–100
 - access, consumers rights to 102
 - breaches, risk of 100–101
 - civil society sources 99
 - commercial sector sources 98–99
 - state and local governments sources 98
- description 96–97
- examples 95
- numbers of 99
- PII 96
- relationship to other domains 96
- roles 95
- types of 97–98

dataveillance 69, 79

delegation 55

- entity-to-person 5
- person-to-entity 5
- person-to-person 5

digital human rights 14

digital identity/persona 11–12

- control 13–15
 - digital human rights 14
 - Indie Web Camp 14
 - Quantified Self 14
 - self-sovereign identity 15
 - user-centric identity 13–14
- definition 11–12
- ownership 12–13

digital signatures 45–46

Dissent Magazine 69

Dixon, Pam 28

document signing management, digital systems 19–20

DocuSign company 23

drivers licenses 29–30

Earnst, Johannes 13–14

e-authentication solution 47

EBT. *See* electronic benefit transfer

EdTech platforms 56

electronic benefit transfer (EBT) 52

electronic identity (eID) systems 19–20, 52

employment registration 7, 83–86

- description 84
- digital identity management system
 - for 85–86
- employees deprovisioning/termination, identity management in 84
- examples 83
- vs. government registration 86
- identity proofing and credential verification 84–85
- PII 83
- pre-enrollment processes 84
- relationship to other domains 84
- roles/actors 83

employment surveillance 8, 91–94

- description 92–93
- examples 91
- PII 91
- relationship to other domains 91–92
- roles 91
- self-tracking and 93–94

employment transactions 7, 87–89

- description 88–89
- examples 87
- vs. government transactions 89
- PII 87
- relationship to other domains 88
- roles 87

enrollment vs. authentication 32–33

enterprise identity and access management (EIAM) 7

entity-to-person delegation 5, 17

- gaps with 23

EOI. *See* evidence of identity

e-Residents 52

evidence of identity (EOI) 30

face-recognition technology 79–80

Fair Credit Reporting Act (FCRA) 8, 97

FCRA. *See* Fair Credit Reporting Act

feudalism 37–38

Fordism 92

General Data Protection Regulation, Europe 61, 65

Goffman, Erving 10

Google 56

Google Docs 56

government registration, identity 5, 25–36

- alternatives to 35–36
- biometrics role in 31–32
- birth registration 26–28
- citizens registration with state 26
- vs. civil society registration, identity 51

- vs. commercial registration 60
- for development and birth registration
 - challenges 33–35
- digital technologies for 29–30
- vs. employment registration 86
- enrollment vs. authentication 32–33
- to get identity documents 30–31
- identification numbers 28–29
- Identity for Development (ID4D) program 33
- need for 27
- origins 37
- relationship to other domains 26
- self-sovereign identity systems 36
- states 38–39
- government surveillance, identity 7, 67–72
 - description 68
 - examples 67
 - kinds
 - involuntary known 70–71
 - involuntary unknown 70, 72
 - semi-known involuntary 71–72
 - voluntary known 70
 - PII 67
 - power dynamics of 68–69
 - relationship to other domains 68
 - roles/actors 67
 - technology 69
- government transactions 6, 43–47
 - vs. agencies 45
 - authentication, role of 46–47
 - description and relevant literature 44
 - vs. employment transactions 89
 - examples of 43, 45
 - PII 43
 - relationship to other domains 44
 - roles 43
 - sign documents in 45–46
 - SSN in 46–47
- Gramm-Leach-Bliley Act 88

- Hagel, John, III 22
- health care card 29–30

- ID2020 35
- identification numbers 28–29
- identity
 - corporations 38
 - domains 2–8
 - civil society registration 6, 34, 49–52
 - civil society surveillance 7, 73–75
 - civil society transactions 6, 53–56
 - commercial registration 6, 57–61
 - commercial surveillance 7, 77–81
 - commercial transactions 6, 63–5
 - data broker industry 8, 95–102
 - employment registration 7, 83–86
 - employment surveillance 8, 91–4
 - employment transactions 7, 87–89
 - government registration 5, 25–36
 - government surveillance 7, 67–72
 - government transaction 6, 43–47
 - illicit market 8, 103–5
 - me and my 5, 9–16
 - surveillance 6
 - you and my 5, 17–23
 - feudalism to church, transition from 37–38
 - management 1
 - citizen to government 1–2
 - consumer to merchant 1–2
 - domains 2–8
 - employee to employer 1–2
 - origins 37
 - papers, origins of 39–40
 - register record 30
- Identity for Development (ID4D) program 33
- illicit market 8, 103–5
 - description 104–5
 - examples of 103
 - PII 104
 - relationship to other domains 104
 - roles/actors 103
- Indian Aadhaar system 28, 52
- Indian Citizenship Act of 1924 18
- Indie Web Camp 14
- International Civil Aviation Organization (ICAO) 30–31
- International Commission on Civil Status (ICCS) 31
- Internet Protocol (IP) address 60–61

- KBA. *See* knowledge-based authentication
- Kelly, Kevin 14
- knowledge-based authentication (KBA) 52
- known involuntary surveillance
 - by commercially entities 79–80
 - by government 70–71
- know your customer (KYC) 52
- KYC. *See* know your customer

- legal identity 34–35
- Login.gov service 47
- Lupton, Deborah 14

- machine-readable travel document (MRTD) 30
- Mann, Steve 75
- Marx, Gary 69
- me and my identity 5, 9–16
 - collection of 16
 - delegation management 16
 - digital identifiers for 16
 - digital identity 11–12

me and my identity (*cont.*)

- control 13–15
- definition 11–12
- ownership 12–13
- management of 16
- meaning 10–11
- and state, private actors, and organizations, relationship between 15–16

membership card 51

monitoring 93

National Center for Health Statistics (NCHS) 27

National Vital Statistics System 27

natural person 18

Oakland Privacy group 75

Open Authorization (OAuth) 20–22

passports 39–40

PayPal 60

persona 11

personal identification number (PIN) 64

personally identifiable information (PII) 2

person-to-entity delegation 5, 17

- gaps with 22–23
- pre-digital world, management in 22

person-to-person delegation 5, 17, 19

- document signing management, digital systems 19–20
- gaps delegation management 20–21
- management 19

PII. *See* personally identifiable information

Policy for a Common Identification Standard for Federal Employees and Contractors 85

preemployment surveillance practices 92

The Presentation of Self in Everyday Life 10

privacy policies 81

privileged account management (PAM) 22, 89

privileged identity management (PIM) 89

Quantified Self 14

role-based access control (RBAC) 88

SAML (Security Assertion Markup Language) 86, 89

Sarbanes–Oxley Act of 2002 22, 88

School Loop, online tool 21

self-sovereign identity systems 15, 36

self-tracking 11, 14, 93–94

semi-known involuntary surveillance, government 71–72

S&H Green Stamps 58

sign documents 45–46

simulacrum 12

Social Security Administration (SSA) 28

Social Security Numbers (SSNs) 28, 46–47

states government registration 38–39

surveillance 6, 68, 75, 78

- applicant 84
- civil society 7, 73–75
- commercial 7, 77–81
- employment 8, 91–94
- government 7, 67–72
- workplace 92–93

Szreter, Simon 40–41

Taylorism 92

tracking cookies, websites 80

Tracy, S. J. 10

Trethewey, A. 10

UK Verify 47, 52

Under Observation: The Interplay between eHealth and Surveillance 74

universal birth registration 41–42

unknown involuntary surveillance

- by commercially entities 80–81
- by government 72

user-centric digital identity 13–14

user-managed access (UMA) 22

voluntary surveillance

- by commercially entities 79
- by government 70

“what you know” factor of authentication 51

Wolff, Gary 14

workplace surveillance 92–93

you and my identity 5, 17–23

- entity-to-person delegation 17
- gaps with 23
- natural person 18
- person-to-entity delegation 17
- gaps with 22–23
- pre-digital world, management in 22
- person-to-person delegation 17, 19
- document signing management, digital systems 19–20
- gaps delegation management 20–21
- management 19
- relationship to other domains 18

Yubikey, hardware token 51