



Edited by
Mary C. Lacity · Lynda Coon

Human Privacy in Virtual and Physical Worlds

Multidisciplinary Perspectives

OPEN ACCESS

palgrave
macmillan

Technology, Work and Globalization

Series Editors

Leslie P. Willcocks, Department of Management, London School of Economics and Political Science, London, UK

Mary C. Lacity, Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR, USA

The Technology, Work and Globalization series was developed to provide policy makers, workers, managers, academics and students with a deeper understanding of the complex interlinks and influences between technological developments, including information and communication technologies, work organizations and patterns of globalization. The mission of the series is to disseminate rich knowledge based on deep research about relevant issues surrounding the globalization of work that is spawned by technology.

Mary C. Lacity · Lynda Coon
Editors

Human Privacy in Virtual and Physical Worlds

Multidisciplinary Perspectives

palgrave
macmillan

Editors

Mary C. Lacity
Sam M. Walton College of Business
University of Arkansas
Fayetteville, AR, USA

Lynda Coon
Honors College
University of Arkansas
Fayetteville, AR, USA



ISSN 2730-6623

ISSN 2730-6631 (electronic)

Technology, Work and Globalization

ISBN 978-3-031-51062-5

ISBN 978-3-031-51063-2 (eBook)

<https://doi.org/10.1007/978-3-031-51063-2>

© The Editor(s) (if applicable) and The Author(s) 2024. This book is an open access publication.

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

ACKNOWLEDGMENTS

We were able to offer this book as open source with funding from our research chairs from the Honors College and the Sam M. Walton College of Business at the University of Arkansas. We thank the intrepid honors students who inspired us with their interdisciplinary zeal for understanding privacy in all its complexities.

The preparation of this manuscript was a team effort. We thank Shermer Shamara Sutton, Shelby Gill, and Jishan Mahmud for help with formatting, finding citations, drawing figures, and securing image permissions. We also thank the team at Palgrave Macmillan, including Alec Selwyn and Geetha Chockalingam.

CONTENTS

1	Introduction to Human Privacy in Virtual and Physical Worlds	1
	Mary C. Lacity and Lynda Coon	
Part I Foundations of Human Privacy		
2	Exploring Privacy from a Philosophical Perspective: Conceptual and Normative Dimensions	23
	Sharon Mason	
3	What's So Special About Private Parts? How Anthropology Questions the Public–Private Dichotomy	47
	Simon Hawkins	
Part II Technical Views of Privacy		
4	Privacy in the Digital Age: Navigating the Risks and Benefits of Cybersecurity Measures	71
	Christopher Farnell, Philip Huff, and William Cox	
5	Data Governance, Privacy, and Ethics	87
	Karl D. Schubert and David Barrett	
6	Web2 Versus Web3 Information Privacy: An Information Systems Discipline Perspective	111
	Mary C. Lacity and Erran Carmel	

7	Multi-party Computation: Privacy in Coopetition	141
	Daniel Conway and Kiran K. Garimella	
8	Zero-Knowledge Proofs and Privacy: A Technical Look at Privacy	157
	Kiran K. Garimella and Daniel Conway	
Part III Domain-Specific View of Privacy		
9	An Architect's View of Privacy	183
	Marlon Blackwell, Lynda Coon, and Mary C. Lacity	
10	Healthcare Privacy in an Electronic Data Age	193
	D. Micah Hester	
11	Privacy Considerations in Archival Practice and Research	205
	Katrina Windon and Joshua Youngblood	
12	Employee and Customer Information Privacy Concerns in Supply Chain Management	235
	Marc A. Scott, Matthew A. Waller, and Brian S. Fugate	
Index		269

NOTES ON CONTRIBUTORS

David Barrett is an instructor in the Department of Philosophy. He received his Ph.D. from the University in 2012 and has taught either as a graduate student or faculty member for 15 years. His teaching has covered a majority of courses routinely offered by the department, including all of the lower-level courses and a variety of upper-division courses (involving graduate students). His area of specialization is the philosophy of mind, with areas of competence in ethics and epistemology. His past research has revolved around mind, with publications on the nature of mental states, the relationship of consciousness to attention, the nature of psychological explanation, and self-deception. Recently he was Co-PI receiving the Chancellor's Fund for Humanities and Performative Arts for the 2020 academic year for *Reasoning in the Digital Age: Challenges and Implications of an Epistemic Crisis*. This funding has pushed him into research on the ethics of technology and artificial intelligence. He is now currently interested in the effects of social media on political behaviors and attitudes, the impact of causal reasoning on data analytics involving possible discrimination, and also, of course, the development of a data ethics course for the Data Science program.

Marlon Blackwell is the E. Fay Jones Chair in Architecture and a Distinguished Professor in the Fay Jones School of Architecture and Design at the University of Arkansas in Fayetteville. He's earned many awards, including the 2020 AIA Gold Medal, which is the highest honor awarded by the American Institute of Architects (AIA). In addition to being a

full time faculty member, he is also the founder and principal at Marlon Blackwell Architects (MBA), based in Fayetteville Arkansas.

Erran Carmel is a Professor of Information Technology at the Kogod School of Business at American University in Washington D.C. Carmel is known for his expertise on the globalization of technology work—especially global outsourcing. He wrote three books and well over one hundred articles. The pandemic—and the need for health credentials—brought him into the world of decentralized identity.

Daniel Conway is teaching professor in the Department of Information Systems at the University of Arkansas. He has previously held positions at Indiana, Notre Dame, Florida, and several other universities. He is active in cybersecurity and artificial intelligence and has worked with dozens of companies. Dr. Conway is a member of the think tank of Cognitive World and served as the first professor in residence at Cisco Systems.

Lynda Coon is Professor of History and Dean of the Honors College at the University of Arkansas. In 2023, she organized a cross-disciplinary course called *Privacy*, recruiting professors from architecture, political science, engineering, medicine, business, philosophy, data science, and library sciences to teach the course. Coon's research focuses on the history of Christianity from circa 300–900. Her first book, *Sacred Fictions: Holy Women and Hagiography in Late Antiquity*, explored the sacred biographies of holy women in late antiquity. Her second book, *Dark Age Bodies: Gender and Monastic Practice in the Early Medieval West*, focused on the ritual, spatial, and gendered worlds of monks in the Carolingian period (ca. 750–987). She is currently researching a book on imagining Jesus in the Dark Ages.

William Cox 223rd Cyberspace Operations Squadron Operations Superintendent. SMSgt Cox received his Master of Science degree in Cybersecurity from Liberty University in 2017. He has been in the military since 1998 where he has held many positions in cybersecurity. Most recently he has served as the Operations superintendent for the Arkansas Air National Guard's premier cyber unit. Bill is an Adjunct Faculty member at the University of Arkansas—Pulaski Technical College, where he teaches Cybersecurity and Information Technology courses.

Christopher Farnell is an Assistant Professor in the Electrical Engineering and Computer Science (EECS) Department at the University of

Arkansas. His research interests include Cybersecurity for Critical Infrastructure, Embedded System Design, FPGA Design, Advanced Control Algorithms, and Power Electronics. He is currently serving as an Associate Director for the National Center for Reliable Electric Power Transmission (NCREPT) located at the University of Arkansas. This 12,000 ft² laboratory provides the equipment, technical staff, and instrumentation to test and evaluate power electronic circuits and systems at realistic industrial and distribution voltage levels up to 6 MVA power ratings. Chris is the current chair for the IEEE Ozark Section, treasurer for the newly formed IEEE Computer Society Chapter, the CyberHogs Registered Student Organization (RSO) faculty mentor, and remains active in K-12 outreach activities.

Brian S. Fugate is the Chair of the Department of Supply Chain Management, and the Oren Harris Endowed Chair in Transportation at the University of Arkansas Sam M. Walton College of Business. He serves on the World Food Logistics Organization SAC and is a co-author of *The Blockchain Toolkit: A Supply Chain Manager's Guide to Understanding and Implementing Blockchain and Operations and Supply Chain Management: Enhancing Competitiveness and Customer Value*. Brian is a former MIT Fulbright Senior Research Scholar, Co-Editor-in-Chief of the *Journal of Supply Chain Management*, and recipient of multiple awards for innovations in teaching, including AACSB's Innovations That Inspire Award. Brian previously worked in supply chain management and industrial engineering in the airline, consumer packaged goods, and automotive industries.

Kiran K. Garimella is an assistant professor of instruction in the Muma College of Business, University of South Florida. His research interests include blockchain and machine learning, specifically on the integration of machine learning into distributed ledger technology (blockchain), functional security of blockchain applications, dynamic consensus mechanisms, dynamic allocation of multi-party blockchain channels in supply chains, and distributed ecosystem formation. He is also the co-founder and chief scientist at KoreChain, the world's first, fully compliant, SEC-qualified, permissioned blockchain for the global private capital markets, launched in 2019 in 23 countries. He is the principal author of two books on business process management and "AI+Blockchain: A Brief Guide for Gamechangers" (with foreword by Dr. Vint Cerf, co-founder of the Internet). He has a Ph.D. in machine learning from the University of

Florida's business school. He has numerous publications, including in Informs, IEEE, and WITS.

Simon Hawkins is Director of the Donaghey Scholars Honors Program and associate professor of anthropology at the University of Arkansas at Little Rock. As a Fulbright Scholar, he pursued his doctoral research on language learning and national identity in Tunisia. His later research in Tunisia tackled a range of topics, including conflict between language use inside and outside the academy, nationalist and ideological imagery in currency, gender and modernity, the state construction of religion, cosmopolitanism, and social media, and the origins of the Arab Spring. Prior to his anthropological work, he researched national and international STEM education with the National Center for Improving Science Education. In addition to his academic work, he is a graduate of Ringling Brothers, Barnum and Bailey Clown College.

D. Micah Hester Ph.D., is chair and professor in the Department of Medical Humanities & Bioethics at the University of Arkansas for Medical Sciences. He has published on the ethics of patient-provider relationships, end-of-life decision making, organ procurement, pediatric care, and more.

Philip Huff is an Assistant Professor in the Computer Science department at UA Little Rock and Director of Cybersecurity Research at the Emerging Analytics Center. He has a 15-year history of cybersecurity management in the electric sector and is the co-founder of Bastazo, a company specializing in cybersecurity AI for the electric sector. While at UA Little Rock, he has developed multiple degree and certificate programs in cybersecurity and directs the Department of Energy Emerging Threat Information Sharing and Analysis Center (ET-ISAC) and NSA National Cyber Teaching Academy. He is also a CISSP.

Mary C. Lacity is the David D. Glass Chair and Distinguished Professor of Information Systems in the Sam M. Walton College of Business at the University of Arkansas. She was previously Curators' Distinguished Professor at the University of Missouri. She has held visiting positions at MIT, the London School of Economics, Washington University, and Oxford University. She is founding co-editor of the Springer (Palgrave) Series on *Technology, Work, and Globalization*, helping the series since 2006. She has published 33 books on the topics related to technology, work, and globalization, including authoring/co-editing 9 books in the series. Her work has been cited over 24,000 times, with an h-index of 64.

Sharon Mason is an Associate Professor of Philosophy in the Department of Philosophy and Religious Studies at the University of Central Arkansas (UCA). Her research specialization is in contemporary epistemology, especially questions that concern reflection and perspective, epistemologies of ignorance, feminist standpoint theory, and science education. She has also published work in philosophical pedagogy on how to expand the early modern philosophical canon and on teaching philosophy as a way of life. She is a faculty associate in the STEM Residential College, a regular collaborator with the Norbert O. Schedler Honors College, and a supporting coach for the UCA Ethics Bowl team.

Karl D. Schubert is a Professor of Practice and serves as the Associate Director for the Data Science Program for the University of Arkansas College of Engineering, the Sam M. Walton College of Business, and the Fulbright College of Arts & Sciences. His research interests include data science and analytics, innovation, technology, and interdisciplinary project-based active learning methodologies. As part of his current role, Karl is leading a State-wide multi-college faculty and administration work-group, with the Arkansas Center for Data Science as the Education & Workforce Development Research Theme for the NSF EPSCoR grant, to develop a consistent and collaborative interdisciplinary multi-college B.S. and Associate degree, and certificate program in Data Science, and led a team to develop a State-wide High School path for Data Science for the Arkansas Department of Education officially adopted December 2020, and he is developing an interdisciplinary multi-college Innovation Curriculum.

Marc A. Scott is an Assistant Professor of Practice in the Department of Supply Chain Management in the Sam M. Walton College of Business at the University of Arkansas. His research focuses on supply chain fulfillment operations; supply chain service operations and design, specifically within the areas of logistics, transportation, and mobility; and well as fulfillment and mobility-related technologies in the supply chain. Additionally, Marc serves as a research consultant and advisor to various supply chain service, transportation, logistics, retail, and public sector companies and associations. Prior to a variety of academic roles, Marc led supply chain teams in the retail industry and has worked in the applied research and consulting, public transportation, development banking, investment banking, energy, and manufacturing industries.

Matthew A. Waller is Dean Emeritus of the Sam M. Walton College of Business at the University of Arkansas, where he also serves as Professor of Supply Chain Management. He was the recipient of the Council of Supply Chain Management Professionals' Distinguished Service Award in 2020 and is the former co-editor-in-chief of the *Journal of Business Logistics*. He also is co-author of *The Definitive Guide to Inventory Management*, *Purple on the Inside: How J.B. Hunt Transport Set Itself Apart in a Field Full of Brown Cows*, *Integrating Blockchain into Supply Chain Management: A Toolkit for Practical Implementation*, *Values-Driven Authentic Leadership*, and *The Dean's List: Leading a Modern Business School*.

Katrina Windon is the Collections Management and Processing Unit Head for the University of Arkansas Special Collections. She holds a Master of Science in Information Studies with a concentration in Archival Studies from the University of Texas at Austin, and is certified by the Academy of Certified Archivists. Windon is a former Chair and Steering Committee member of the Society of American Archivists Privacy and Confidentiality Section, and is the co-author, with Lydia Tang, of "Archival Discretion: A Survey on the Theory and Practice of Archival Restrictions" in the *Journal of Contemporary Archival Studies*.

Joshua Youngblood is the Instruction and Outreach Unit Head for the Special Collections Division in the University of Arkansas Libraries, where he also serves as the history and rare books librarian and the curator of the Arkansas Collection. Before joining Special Collections in 2011, he was a member of the Florida Memory Project of the State Archives of Florida, served as the information officer of the Florida Division of Cultural Affairs, and was a staff member of Florida Main Street in the Bureau of Historic Preservation. He has published on digital archival exhibiting and archival instruction programs, as well as on the history of Arkansas, lynching, and reform movements in the American South. A graduate of Florida State University, Youngblood is a certified archivist and a past president of the Society of Southwest Archivists.

LIST OF FIGURES

Fig. 3.1	“World Naked Bike Ride” Protestors Piccadilly Circus, London Athanasios Papadopoulos, Photographer Courtesy of Alamy	49
Fig. 3.2	Apartment block, Cairo, Egypt Petr Svarc, Photographer Courtesy of Alamy	54
Fig. 3.3	Scarfed woman selling sweets at the edge of the street, Egypt, Maadi, Cairo Blickwinkel, Photographer Courtesy of Alamy	56
Fig. 4.1	Denial-of-Service attack diagram (<i>Image credits</i> Iconfinder.com/Dmitry Mirolyubov, Maxicons, Z Studio, iStock.com/LeonidKos; Opal-RT Technologies; Stephan Green under CC BY-SA 3.0 Deed)	74
Fig. 4.2	Man-in-the-Middle attack diagram (<i>Image credits</i> Iconfinder.com/Dmitry Mirolyubov, Maxicons, Z Studio, iStock.com/LeonidKos; Opal-RT Technologies; Stephan Green under CC BY-SA 3.0 Deed)	75
Fig. 4.3	Spoofing attack diagram (<i>Image credits</i> Iconfinder.com/Dmitry Mirolyubov, Maxicons, Z Studio, iStock.com/LeonidKos; Opal-RT Technologies; Stephan Green under CC BY-SA 3.0 Deed)	76
Fig. 5.1	Data governance (Adapted by authors from Caserta, n.d.)	96
Fig. 6.1	An overview of Information Systems research on information privacy (<i>Image credit</i> The authors)	117
Fig. 6.2	Fundamentals of Web2 and Web3 (<i>Image credit</i> The authors)	121

Fig. 6.3	Web3 applications—Decentraland: a Location of British Blockchain Association (BBA) in Decentraland metaverse, located at (24,–28); b Mary Lacity’s avatar visits the BBA in Decentraland (<i>Image credit</i> The authors)	130
Fig. 9.1	Panorama of Shibam, Hadhramaut Province, Yemen (<i>Image credit</i> licensed from iStock.com/javarman3)	185
Fig. 9.2	Marygrove Early Education Center, designed by MBA (<i>Image Credit</i> With permission from Marlon Blackwell Architects)	187
Fig. 9.3	Lamplighter School Innovation Lab, designed by MBA (<i>Image Credit</i> With permission from Marlon Blackwell Architects)	188
Fig. 9.4	Saint Nicholas Eastern Orthodox Church, designed by MBA (<i>Image Credit</i> With permission from Marlon Blackwell Architects)	191
Fig. 11.1	Sample decision tree for evaluating archival collection privacy issues	219
Fig. 11.2	Updated PII and Access to Unprocessed Collections Policy, University of Arkansas Special Collections (<i>Image source</i> https://libraries.uark.edu/specialcollections/research/unprocessed.php)	228
Fig. 12.1	Supply chain, logistics, and order fulfillment activities	238
Fig. 12.2	Inward-facing camera monitors an employee (<i>Image credit</i> Alamy Stock Photo/Olaf Doering)	249
Fig. 12.3	Drone surveillance (<i>Image credit</i> Alamy Stock Photo/Wavebreak Media)	259

LIST OF TABLES

Table 4.1	An example of a k-anonymized dataset	79
Table 7.1	Faculty bonuses	145
Table 7.2	Three random numbers plus a calculated number to equal the bonus	146
Table 7.3	Faculty member's deviation from the mean bonus	147
Table 7.4	Three random numbers plus a calculated number to equal the deviation from the mean	147
Table 7.5	Nine random numbers and one calculated number for faculty votes	151
Table 7.6	Faculty bonuses represented in the binary numbering system	152
Table 12.1	Privacy implications of technology use in retail fulfillment	245
Table 12.2	Work environment privacy dimensions in retail fulfillment (Adapted from Bhave et al., 2020)	251



CHAPTER 1

Introduction to Human Privacy in Virtual and Physical Worlds

Mary C. Lacity and Lynda Coon

DEFINING PRIVACY

The title of this book is *Human privacy in virtual and physical worlds*. Although the title may appear straightforward, the concepts it explores are far from simple. Just defining human privacy is a challenging endeavor. Consider the range of definitions for privacy that appear in scholarly journals and books:

- *From an economics journal:* “Privacy is used today in at least three senses. First, it is used to mean the concealment of information; indeed, this is its most common meaning today. Second, it is used

M. C. Lacity (✉)

Sam M. Walton College of Business, University of Arkansas at Fayetteville,
Fayetteville, AR, USA

e-mail: mclacity@uark.edu

L. Coon

Honors College, University of Arkansas at Fayetteville, Fayetteville, AR, USA
e-mail: llcoon@uark.edu

to mean peace and quiet, as when someone complains that telephone solicitations are an invasion of his privacy. Third, it is used as a synonym for freedom and autonomy.” (Posner, 1981, p. 405).

- *From a philosophy encyclopedia:* “We can see that there is no single definition, analysis or meaning of the term ‘privacy’, either in ordinary language or in philosophical, political and legal discourse. The concept of privacy has broad historical roots in legal, ethical, socio-logical and anthropological discourses.” (Roessler & DeCrew, 2023, p.1)
- *From an information systems journal:* “Privacy is a commodity that can be exchanged for perceived net benefits” (Zhu et al., 2023, p. 295).
- *From a sociology journal:* “Privacy is the ability of individuals to control the terms under which their personal information is acquired and used ” (Culnan & Bies, 2003, p. 326).
- *From an architecture journal:* “ Privacy is a process whereby a person sometimes wants to be separated and at other times wants to be in contact with other people.” (Shah & Kesan, 2007, p. 353).

From these five definitions, readers may observe varied interpretations of privacy across academic disciplines. Some authors provide very narrow views of privacy while other authors acknowledge that even within a discipline, there is no common definition. One major contribution of this book is its ability to confront readers with both familiar and unfamiliar readings of privacy in all its complexity.

The term “virtual world” featured in the book’s title refers to digital spaces that depend on computer technologies. In these spaces, privacy is commonly understood in terms of information privacy or communication privacy. Conversely, the term “physical world” points to analog spaces where individuals are not connected to computing devices. In this realm, privacy is often thought of in terms of bodily or territorial privacy.

While the distinction between the virtual and physical worlds serves as a helpful framework for introducing the book’s comprehensive aims, this dichotomy is ultimately misleading. This ambiguity stems from the increasing interaction between the virtual and physical realms in today’s world.

Communications privacy, for example, can relate to preventing unauthorized eavesdropping in the physical world or deterring similar invasions

in online communications. To illustrate the *interaction* between the physical and virtual worlds, consider a face-to-face conversation in the physical realm that is digitally recorded without knowledge or consent. This recording could then be stored or disseminated in the virtual world, highlighting the complex interplay between physical and virtual realms.

In addition to grappling with the tension between the virtual and physical worlds, readers will explore a variety of other dichotomies in this book. These dichotomies include distinctions between public and private, descriptive and prescriptive approaches to privacy, the intrinsic versus instrumental value of privacy, and between privacy and security. More broadly, the book examines the tension between the best interests, rights, and preferences of the individual as compared to those of the group.

VIEWING PRIVACY FROM MULTIPLE DISCIPLINES

Addressing privacy in the modern context is what is often termed a “wicked problem.” Coined by Rittel and Weber in 1973, this concept refers to a problem that is socially complex, involving multiple stakeholders with differing perceptions, preferences, and levels of power. This book aims to expand scholars’ understanding of privacy by introducing perspectives on human privacy from humanistic, social scientific, design, and STEM (science, technology, engineering, and math) disciplines.

Most of the authors of these chapters initially collaborated to teach an interdisciplinary course on privacy to honors students from across the State of Arkansas and the Netherlands in the summer of 2023. One of us, Lynda Coon, who is the Dean of the Honors College, along with Noah Pittman, the Associate Dean, conceived and organized the course. They recruited faculty from diverse disciplines to each teach a module. As the course unfolded, we quickly realized that faculty members themselves gained valuable insights from interdisciplinary engagement. Eager to share this collective wisdom more broadly, we invited scholars from different departments to offer academic overviews that elucidate how their respective fields conceptualize, investigate, and recommend strategies to protect human privacy.

We guided the authors to make their work accessible to academics outside their own discipline. This meant clarifying terms and concepts that are often taken for granted within their own fields. Each chapter, therefore, begins with an overview of how the author’s discipline approaches

the study of privacy before diving into specialized topics. Our aim is to inspire other academics to broaden their research perspectives on privacy, moving beyond the limitations of a single disciplinary lens.

This introductory chapter sets up the tripartite structure for the entire book: foundations of human privacy, technical views on privacy, and domain-specific views of privacy. Both philosophy and anthropology underpin our understanding of human privacy as a construct deeply embedded in culture, psychology, and society, encompassing norms and values. Philosophy further delves into the ethics of privacy, shifting the discussion from merely defining privacy to what it ought to be. Technical perspectives on this subject aim to protect human privacy in an era where technologies increasingly intrude upon our lives, such as surveilling behaviors, collecting data, and monetizing information—often unbeknownst to us and without our explicit consent (Zuboff, 2019). The domain-specific views of privacy include perspectives from the fields of architecture, healthcare, archival, and supply chain disciplines.

Foundations of Human Privacy

Chapter 2, “Exploring Privacy from a Philosophical Perspective,” provides this volume with its intellectual and ethical anchor. Philosopher Sharon Mason deliberates historical definitions of privacy expressing tensions between the public and the private, in which the public and its utilitarian “good” often outweigh the importance of privacy to the individual. Surveying various philosophical paradigms swirling around the notion of privacy from Greek antiquity through the artificial intelligence revolution of the present day, Mason notes that what we moderns may privilege as a fundamental right of humans—the right to privacy—is a relative latecomer on the historical stage.

For ancient Greek philosophers, most famously Plato (d. 348 BCE) and Aristotle (d. 322 BCE), the concept of the public good thoroughly overshadowed thoughts about protecting one’s personal space, physical or mental. Public service in the world of the Greek *polis* or city-state triumphed over the pursuit of one’s own interests. In fact, the Greek term *idios*, referring to “one’s own,” represents the origin of the modern English word “idiot” because ancient Athenian citizens believed that those who stuck to their own or inhabited marginal spaces to the one side of civic government had more in common with animals and monsters than they did with their compatriots—clearly a negative register of selfhood.

Philosophical stars from the eighteenth century ran with classicizing comprehensions of the private. For David Hume (d. 1776), the private was the reserve of personal interest, existing outside the scope of governmental control. Mason rightly notes that the industrial revolution and its technological interventions sparked the first major Western rewriting of the role of privacy in society. In the nineteenth century, theorists of the private-public divide introduced the concept of the “inviolate personality,” that is, the “right to one’s personality” as free from external pressures. This shift in the cultural reading of privacy partially stemmed from advancements in print culture, bringing to the broad population gossip tracts and pamphlet diatribes against well-known persons, thereby foregrounding the idea that privacy exists as a kind of reified, natural human right.

This historical trajectory shot western constructions of privacy into the realm of inalienable rights, where it joined the company of other nebulous products of the Enlightenment, such as “liberty” and “equality.” From there, philosophers added conversations about the intrinsic value of privacy into the intellectual mix, debates about the degree to which privacy inhabits the space of an inalienable right. Mason transfers abstract, philosophical discussion about the intrinsic nature of philosophy to the critical themes covered in this book: security, transparency, and democracy, thereby offering an exceptional theoretical framework for the chapters that address artificial intelligence (AI), Web 3, blockchain, supply chain, health care, big data, and more. Here, ethical dilemmas complexify notions of privacy, especially since privacy has become increasingly a commodity of exchange in which wealthier players can buy and sell at higher rates than those with fewer resources. Overall, Mason stands back from reading privacy purely as a commodity by offering a provocative interpretation of privacy as a key component in Western constructions of the self, an ability to claim one’s existence as a human in an era disrupted by technological surveillance of personhood in its most intimate details.

Chapter 3, “What’s so special about private parts,” is a tour-de-force through global readings of privacy within the shifting landscape of what it means to be “public.” Cultural Anthropologist Simon Hawkins centers his reading of privacy strongly on different political and cultural spaces: North Africa, the Middle East, the United Kingdom (U.K.), and Eastern Europe. His analysis problematizes a progressive reading of privacy; that is, privacy as the litmus test of more developed and sophisticated cultures, a kind of *natural* right for citizens in those spaces. Rather, in Hawkins’

capable hands, privacy becomes a moving target influenced by vectors of class, race, ethnicity, gender, political persuasion, and the positioning of the body in space. Three objects glue this thick analysis together: bike, door, and toilet.

Bike. Hawkins begins his tour with an event taking place in central London—*World Naked Bike Day*—in which cohorts of nude bicyclists disrupt western notions of privacy by exhibiting their private parts within the full gaze of urban city-dwellers. Shielded by a battalion of bikes, these protesters draw attention to what should be more shocking than a penis or a vagina: environmental devastation on a global scale. The bikers' collective presence, however, safeguards their own nudity from intense surveillance, thus complexifying further the idea of privacy in the very public space of a bustling city.

Door. Moving from the affluent ranks of nude bikers, Hawkins turns his attention to a working-class neighborhood of Cairo, Egypt, al-Zawiya al-Hamra, the brainchild of modernizing President Anwar el-Sadat (d. 1981). Here, newly constructed doors leading into apartments mark the intrusion of western notions of privacy onto spaces where these ideas sit uncomfortably with the historical rhythms of communal practice. What in the United States (U.S.) might comfort a viewer—the door as indicator of intimate, familial space—transmutes into a darker presence et al.-Zawiya al-Hamra. Here, the door functions as a roadblock to the kind of communal intimacy shared among extended families, who previously circulated in and out of each other's abodes. The fallout opens a window onto the negative side of universalizing concepts of privacy.

Toilet. Door *cum* signifier of privacy does not hold up to the test of time. Ancient cultures, like that of Classical Athens, possessed (seemingly) strict divides between the public and the private, the latter being heavily associated with elite, urban female bodies. Yet this same culture embraced the material reality of the communal toilet, a practice shared by ancient Romans. What a modern reader might consider the ultimate marker of privacy—defecating in spaces off limits to an audience—evaporates in the gap between the ancient and the contemporary, another indication that notions of privacy remain historically unstable.

Hawkins' chapter sets the theoretical agenda for this volume. He locates places, where shifting political structures, such as the communist regimes of Eastern Europe, compel women into the public and men into the private. He contests the American “white-picket fence” as an icon of privacy. Finally, Hawkins so successfully problematizes the very idea

of privacy that readers walk away challenged to rethink the map of the fictional divide between the private and the public.

Technical Views of Privacy

The authors of Chapters 4 through 8 are experts in technology-related fields, including computer science, data science, electrical engineering, industrial engineering, and information systems. These chapters provide a comprehensive analysis of both the threats to, and potential solutions for, online privacy. The authors of Chapter 4 note that maintaining privacy on the Internet is challenging due to the lack of defined boundaries and varying laws across countries that personal data may traverse. Unlike the physical world where entering a new jurisdiction is clearly marked, online data in virtual worlds can flow through multiple countries and be subject to different regulations and surveillance levels, often without the user's awareness.

The five technology chapters focus upon *information privacy*, which can be defined as “the ability of individuals to control the terms under which their personal information is acquired and used” (Culnan & Bies, 2003, p. 326). Specializing in technology-related disciplines, these chapters explore the safeguarding of *personally identifiable information* (PII), which encompasses data that can identify or verify an individual or a group of people (AICPA/CICA, 2020). Examples of PII range from basic details like name and home address to more sensitive information such as criminal or healthcare records, and extend to online activity data like IP addresses, email accounts, and website cookies.

How can PII be protected better? Chapters 4 and 5 focus on the human aspect of privacy protection, including government regulations, industry standards, organizational practices, and individual behaviors to safeguard privacy. Chapters 6 through 8 interrogate new technical approaches to privacy protection, including Web3, multi-party computation, and zero-knowledge proofs. Both human and technical solutions are needed to better protect PII.

Chapter 4, titled “Privacy in the Digital Age: Navigating the Risks and Benefits of Cybersecurity Measures,” is authored by Chris Farnell, Philip Huff, and William Cox. The chapter opens with a definition of *cybersecurity* as “the protective actions taken to safeguard digital information and processes that an organization deems necessary for its successful operations.” The authors outline the most common threats to cybersecurity,

categorizing them as attack vectors: Denial of Service (DoS), Man in the Middle (MitM), and Spoofing Attacks.

A DoS attack inundates a computer server with numerous fake requests, thereby denying legitimate users access. A MitM assault occurs when an external attacker intercepts, modifies, or suppresses information traveling over the network, deceiving both the sending and receiving computers into believing they are communicating normally. In the case of spoofing attacks, an illegitimate actor masquerades as a legitimate one, tricking an unsuspecting individual into revealing PII. Robust cybersecurity practices are essential for defending against these types of attacks.

The authors delve into ways organizations and individuals can protect PII. For organizations, they recommend following the Privacy Control Catalog provided by the National Institute of Standards and Technology (NIST). This standard offers guidance on administrative, technical, and physical controls. For individuals, the authors suggest using non-attributable networks like The Onion Router (TOR), privacy-enhancing operating systems such as the Debian Linux-based Tails OS, and adopting protective social behaviors, including the deployment of multiple online personas.

Chapter 5, “Data Governance, Privacy, and Ethics,” written by Karl Schubert and David Barrett, expands on the theme of how organizations should safeguard privacy. While the preceding chapter surveyed various types of cybersecurity attacks, this chapter commences by discussing the repercussions of data breaches for both individuals and organizations. The financial implications outlined are staggering, highlighting the need for governments and organizations to improve their practices.

On the government front, the authors explore key legal and regulatory frameworks that direct data privacy and ethics. These include the European Union’s General Data Protection Regulation (GDPR) and several U.S. federal and State laws. The authors observe that European actions, particularly through the GDPR, are far more advanced than those in the rest of the world.

Given the weaker regulatory landscape in the U.S., the onus falls on organizations to self-govern when it comes to data. To assist in this effort, the authors present a comprehensive framework for data governance aimed at protecting PII and ensuring the ethical use of data. Importantly, they also acknowledge the organizational challenges involved in adopting data governance and offer advice for overcoming resistance.

Chapter 6, titled “Web2 versus Web3 information privacy: an Information Systems discipline perspective” by Mary Lacity and Erran Carmel, also centers on protecting PII, but with a technical solution called Web3. The authors begin by summarizing the Information Systems (IS) research on information privacy. First, they note that IS scholars primarily examine online information privacy in the context of Web2, which is the dominant version of Internet. With Web2, individuals rely on centralized platform providers to access online services using accounts and passwords; individuals also submit other PII as required by the centralized platform providers. Second, the authors explain how IS scholars have conceptualized and scrutinized information privacy in terms of an individual’s information *privacy concerns* and have examined why these concerns do not prevent individuals from *disclosing personal information* with centralized platform providers; the phenomenon is called the *privacy paradox*.

The authors mine four theoretical explanations for the privacy paradox: (1) *privacy calculus*, where individuals assess the trade-offs between the risks and benefits of disclosing PII; (2) *privacy fatigue*, characterized by emotional exhaustion from continuous efforts to protect PII; (3) *trust in centralized platform providers*, which encourages users to share PII; and (4) *lack of user choice*, where PII disclosure is mandated by centralized platforms to access their services. Together, the four theories show how difficult it is to protect PII in Web2.

Introducing the concept of Web3, the authors present a revolutionary approach to enhancing online privacy. Web3 represents the next era of the Internet, founded on decentralized technologies and applications such as Bitcoin and Ethereum. In contrast to Web2, Web3 allows individuals to access services without revealing PII to a central authority. This improved privacy is technically facilitated through the integration of digital wallets, cryptography, and distributed ledgers, commonly known as blockchain. Although Web3 is still a new idea comprising emerging technologies, education plays a crucial role in accelerating its adoption.

Chapter 7, titled “Multi-party Computation: Privacy in Cooperation,” is authored by Daniel Conway and Kiran Garimella. The authors present an innovative approach to calculating information among trusted parties without revealing anyone’s confidential data. The chapter elucidates the methodology through easily understandable examples, such as, “How does my annual salary bonus compare with others?” and “Who is everyone going to vote for as leader?” In these scenarios, all parties are

interested in the answers but do not want to disclose their actual bonuses or votes.

The method involves each participant generating random numbers and a calculated number that sums to their bonus (in the first example) or indicates their vote (in the second example). The ingenious aspect of this method is that it does not just aim to protect private data—it avoids sharing private data altogether! The authors note that multi-party computation is computationally intense, which means it will consume significant computer resources if the number of parties is large. Moreover, this approach does necessitate trust among the parties involved. Hence, the chapter incorporates the term “coopetition,” which denotes trusted collaboration among traditional competitors to answer questions of mutual interest, such as “Am I paying the same for materials?” or “Does anyone else see suspicious cybersecurity activity on their networks?” The authors demonstrate the wide range of contexts in which this method can be useful, including auctions, voting, financial transactions, supply chains, fraud detection, genomic data sharing, and user authentication.

Dan Conway and Kiran Garimella are also the authors of Chapter 8, titled “Zero-knowledge proofs and privacy: A technical look at privacy.” In this chapter, the authors explore another kind of privacy-enhancing algorithm known as the zero-knowledge proof (ZKP). They define ZKP as a method by which one party can prove to another that they possess a particular identity, item, or piece of knowledge without revealing the specifics of what that identity, item, or knowledge is. Like the previous chapter, the authors provide illustrative examples to help non-technical readers grasp the core concepts and the myriad applications, such as digital verification, secure messaging, voting, healthcare privacy, location privacy, and many others. Readers with a more technical background will appreciate the detailed discussions on specific ZKPs and their advantages and drawbacks, including Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK), Zero-Knowledge Scalable Transparent Argument of Knowledge (zkSTARK), commitment schemes, and homomorphic encryption.

All ZKPs strive for completeness and convincingness. They are sound, preventing dishonest actors from proving false statements, and they enhance privacy by ensuring that no private data is revealed. While multi-party computation requires a certain level of trust among the participants and becomes computationally intensive as it scales, some forms of zero-knowledge proofs are computationally efficient. These proofs eliminate

the need for parties to trust one another, as they can instead place their trust in the proofs themselves.

Domain-Specific Views of Privacy

Chapters 9 through 12 dive into the exploration of privacy across diverse domains including architecture, healthcare, library sciences (archival), and supply chains. Each field offers a unique perspective and set of challenges concerning privacy. Architects bring the nuanced interplay between spaces and privacy; architectural scholars analyze how design can both enhance and inhibit the privacy of individuals within different environments. In the realm of healthcare, scholars grapple with the delicate balance between the laws and ethics of safeguarding individual information privacy while ensuring public welfare. Turning to library sciences, scholars in this field explore the ethical considerations and best practices for archiving and providing access to information, ensuring a balance between accessibility and confidentiality. Lastly, in the context of supply chains, the emphasis is on balancing the collection of data on employees and customers to enhance service delivery against the obligations to safeguard employee and customer privacy. Supply chain scholars investigate strategies and frameworks to ensure that the pursuit of operational efficiency does not compromise individual privacy rights. As the chapter descriptions will show, these chapters provide a multifaceted exploration of privacy across different disciplines, highlighting the commonalities, differences, and unique challenges each field faces in protecting individual privacy while meeting broader objectives,

In Chapter 9, titled “An Architect’s View of Privacy,” we, the editors, engaged in a thought-provoking interview with Marlon Blackwell, the E. Fay Jones Chair in Architecture and a Distinguished Professor at the Fay Jones School of Architecture and Design, University of Arkansas, Fayetteville. In addition to his academic role, he is the founder and principal of Marlon Blackwell Architects (MBA).

This conversation concentrated on the design philosophy of Blackwell, an esteemed American Institute of Architects (AIA) award recipient, focusing on his approach to privacy. Several themes pivotal to architectural privacy were explored. Initially, he considered the influence of culture on the interconnection between privacy and comfort, observing that individualistic societies tend to prioritize privacy more than their collective counterparts. Subsequently, he deliberated how primary, secondary, and

tertiary spaces can cultivate private moments within public environments, illustrated by examples from MBA's portfolio such as an alcove in a church, a recessed wall in a school, and a solitary bench in a garden.

Moreover, Blackwell examined the dual role of light and sound as both disruptors and facilitators of privacy, illustrated through various projects by MBA. A central theme emerged that encapsulates Blackwell's design ethos: *ennobling the prosaic*. For him, architecture ennobles the prosaic by imbuing ordinary, everyday things with a sense of nobility and significance. This chapter features a vivid example of this philosophy in action, showcasing the transformation of a simple welding shed into a sacred space for the congregation of Saint Nicholas Eastern Orthodox Church.

Chapter 10 is titled "Healthcare Privacy in an Electronic Data Age" by D. Micah Hester. The principle of confidentiality of patient information in healthcare, which has been integral since the days of Hippocrates, signifies patients' right to control personal details of their life. This obligation, falling on healthcare professionals, is challenged by the fact that multiple entities and people, including diagnosticians, therapists, social workers, chaplains, medical transcriptionists, medical records clerks, and insurance providers access the information. With the advancement in technology, digitization of healthcare records, and the rise of telemedicine, maintaining confidentiality has become more challenging.

Hester discusses the complex interplay between patient privacy and the need for information sharing in healthcare, outlining the various ethical and legal challenges that arise. Medical confidentiality is not absolute; it is guided by laws such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), which provide protective frameworks and conditions for permissible breaches. These breaches include reporting communicable diseases, cases indicating imminent harm, legal mandates like court orders, and certain safety and protection factors like suspicions of abuse or criminal activity.

This chapter concludes by arguing that healthcare organizations must foster a culture of confidentiality, even if absolute guarantees of privacy are not feasible. By promoting and adhering to such a culture, both institutions and healthcare providers can adopt practices that intentionally and proficiently mitigate the tangible risks to the privacy of patients, participants, and the broader community they serve.

Chapter 11, "Privacy Considerations in Archival Practice and Research," details the delicate dance among invested parties—donors, estates, the dead, archivists, administrators, the public—who negotiate the

line between opening access to sensitive materials and shutting that access down. Following the lead of previous chapters, authors Katrina Windon and Joshua Youngblood clarify that there is no one approach to archival privacy in North America; nor is there a single international legal system. The fact that archival collections often represent a snapshot of history frozen in time, determining when or if to grant access to the public is a very dicey political game.

Windon and Youngblood give a series of fascinating cases where archival behavior went astray. They cite the infamous example of author Franz Kafka (d. 1924), who had requested that his executor burn his papers after his death. The executor of Kafka's estate, Max Bord, not only refused to honor Kafka's wishes, but he also went on to publish the writer's papers, which eventually found their way from Europe to the National Library of Israel, a journey underscoring the disconnect between an individual's personal preference and an institution's decision to open access based on the idea of the common good.

Archivists are also sensitive to the fact that authoritarian regimes have silenced the voices of at-risk populations. A disturbing case involves the Stasi Records Archive in Berlin, where 111,000 meters of documents contain a wealth of data retrieved through unrelenting, clandestine surveillance of citizens living in the Eastern Bloc. Given the manner of how they were collected, should these documents be open to the public?

Archival collections offer their users a "shot in time," a recording of historical events, such as political protests, in which the participants may or may not know that photographic and videographic technology has recorded their physical involvement in controversial movements, storing this visual information in archival repositories. Such "ephemeral" data, that is, information not taken with an eye toward recording stories in perpetuity but merely capturing them in a moment in time, presents yet another set of archival challenges in an age when law enforcement officials are combing archives searching for potential terrorists, insurrectionists, and anarchists.

What is fascinating here is the authors' focus on the person of the archivist, that impresario of access to sensitive material. What role in archival ethics does the archivist play? How much power does the archivist have to open and close access? In answering these questions, Windon and Youngblood draw on "best practices" available for archival access, noting that these guidelines are in no way consistent across the globe.

They share the regulatory framework of their own institution, the University of Arkansas Special Collections, where the demands of a Land-Grant university necessitate unrestricted access but the realities of the history of this state often make impossible—or extremely thorny—that mandate.

Our final chapter, “Employee and customer information privacy concerns in supply chain management,” is written by Marc Scott, Matthew Waller, and Brian Fugate. Retailers and their logistics partners, in their pursuit of enhanced competitiveness, harness sophisticated technologies that gather PII data, aiming to elevate customer service and bolster employee efficiency. However, employees and customers often raise privacy concerns.

While earlier chapters turned to customer and user privacy concerns, this chapter uniquely addresses the concerns of employees. Today, there’s a growing trend of employees being watched through surveillance cameras and wearable sensors that track their health, emotions, and behaviors. Such monitoring has led many employees to believe that their privacy rights are being violated, making them vulnerable to potential mistreatment or bias. Striking the right balance between the organization’s need for data—related to safety, efficiency, and compliance—and respecting employees’ privacy is a complex issue.

This chapter highlights individual and cultural variances regarding employee data collection acceptance. The research summarized indicates varying perceptions based on personality traits and workplace type. For instance, individuals with higher neuroticism and extroversion levels expressed fewer privacy concerns than their counterparts with lower levels of these traits. Job nature also plays a role: manual laborers expressed greater surveillance concerns than those in non-manual roles. Furthermore, an organization’s culture has a significant impact: employees in companies with a nurturing culture showed less resistance to monitoring compared to those in more bureaucratic settings.

The analysis also focuses on work environment privacy, defined as the ability of the employee to control sensory stimuli in the work environment. Organizations should craft workspaces that consider visual, acoustic, spatial, and even olfactory aspects. As highlighted by insights from both our supply chain and architectural experts: no one wants to work in an exposed, cramped, loud, and stinky environment.

THEMES ACROSS CHAPTERS

As a complex social construct, academics approach the study and conceptualization of privacy differently across disciplines. One unanticipated yet intriguing discovery was that we often share more common ground than initially presumed, even if we sometimes employed different terminology. Four recurring themes emerge across the chapters in this book:

1. **Privacy is best understood as a multifaceted, contextual, and temporal concept.** Our collective efforts did not yield a singular, all-encompassing definition of privacy, which seems fitting given its complexity. Throughout the chapters, authors excavate various facets of privacy, including acoustic, bodily, communication, data, information, olfactory, spatial, territorial, and visual privacy. They also examine privacy from the perspectives of different entities, from individual consumers, decision-makers, employees, and patients to larger units like families, groups, organizations, and societies. Attempting to condense privacy into a singular definition would inevitably diminish the depth and nuance of understanding, as would trying to imagine certain “universal” truths about privacy operating globally.
2. **Individuals’ rights to privacy are often in conflict with the group’s desire or right to know.** Many authors delve into the tension between the rights and interests of the individual and those of the collective. Technologists, for example, weigh the protection of individual user data against the broader demands to authenticate users to enhance cybersecurity. Healthcare professionals strive to shield patient information while also safeguarding society at large. Archivists grapple with the duality of defending individual data in archives and fulfilling their duty to disseminate information to students, researchers, and the public. Similarly, supply chain experts navigate the delicate balance between an organization’s data collection imperatives and the privacy concerns of employees and customers. These tensions signify the complexity of privacy considerations.

The concept of *power* plays a pivotal role in determining which stakeholders ultimately hold sway. Given that governments typically wield more influence than organizations, and organizations hold more power than individuals, it becomes imperative

to establish robust governmental regulations to safeguard individuals from potential infringements of their privacy by organizations. Overall, several authors mentioned complying with privacy laws as a minimum requirement for striking the balance between individual and group needs.

3. **Privacy law is pervasive.** While no legal scholars contributed to the chapters in this book, privacy law permeates many discussions because professionals in every field must adhere to restrictions relevant to their jurisdiction. Although American scholars wrote this book, four chapters cover the European Union (E.U.)'s General Data Protection Regulation (GDPR). GDPR applies to all companies processing the personal data of E.U. residents, regardless of the company's location. American companies must adhere to GDPR if they offer goods or services to, monitor the behavior of, or have business operations concerning E.U. citizens. Non-compliance can result in hefty fines and reputational damage. Several U.S. federal laws are discussed in this book, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA), along with state-specific laws in the U.S. Most authors advocate privacy-enhancing policies and practices beyond mere legal compliance.
4. **Privacy prescription.** The chapters written by the philosopher and the anthropologist caution against assuming that individual privacy is universally valued and should invariably be safeguarded. In contrast, the authors of the technology and domain-specific chapters predominantly advocate for the valuation and protection of individual privacy, emphasizing that such protection should exceed privacy laws.

The authors discussing technology recommend various measures to bolster individual privacy. These measures include administrative, technical, and physical controls; data governance; embracing technology decentralization (Web 3.0); and employing algorithms like multi-party computation and zero-knowledge proofs. The authors of the domain-specific chapters interrogate privacy-enhancing solutions within distinct fields:

- In architecture, by creating avenues for private moments within public spaces.
- In healthcare, by fostering a pervasive culture of privacy.
- In archiving, by adhering to a decision tree approach.
- In supply chains, by striking a balance among organizational, employee, and consumer needs.

Across the diverse disciplines and perspectives presented, it is evident that privacy remains a dynamic, multifaceted realm necessitating nuanced understanding and approach. Clearly, privacy is a *moving target* when dropped into various contexts and spaces across the globe.

Ultimately, readers must determine how insights from various disciplines might influence their own research and teaching. In our concluding remarks, we each reflect on how learning from fellow scholars has influenced our work.

Mary, as we noted, is an information systems scholar who examines technical solutions for protecting personally identifiable information. This book broadened her perspective on privacy. Mary is less inclined to think that technologies alone will protect online privacy. The chapters on philosophy, cultural anthropology, and the domain-specific chapters illuminated the historic and contextual understanding needed to solve the “wicked” problem of online privacy, assuming of course, that privacy protection is deemed valuable by individuals within a specific context.

More specifically, one of Mary’s current research and teaching interests are metaverses, which are three-dimensional, computer-generated virtual worlds one visits with an avatar. Marlon Blackwell’s chapter on architectural privacy in physical spaces has had a profound effect on her thinking about designing virtual spaces. Most virtual worlds are designed to be expansive, open public spaces. So far in metaverses’ development, the virtual worlds are rather barren unless a particular event like a fashion show or concert are announced, so she had never thought about spatial privacy. As metaverse adoption grows, she now thinks about designing virtual spaces where an avatar might have a private moment.

Mary’s co-editor, Lynda, is a historian of early medieval era Europe (ca. 600–900) with a special focus on gender, visual culture, and religion (Coon, 2011). For Lynda, two things stand out here. First, an appreciation for the historical rhythms of the subject of privacy, from classicizing discourses of what belongs to the individual in contrast to the hegemony of the city-state and empire. The notion that the private existed

as a reified, inalienable right simply did not appear in the West before the advent of the Industrial Age. Rather, premodern cultures in the West blurred the line between the private and the public in ways that seem either off-putting or even illogical to contemporary societies. The classical communal toilet—be it located in ancient Athens or Rome—represents a case in point as does the fact that Roman elites often conducted political business in their bedrooms. Marlon Blackwell notes the shared space of the familial bed in later medieval England surprises us moderns; monasteries too preferred corporate living—in the bedroom, in the toilet, in the garden, in the basilica—due to the dangers of sin which could penetrate monastic bodies seeking solitary spaces outside of the watchful gaze of the abbot.

The era of the Enlightenment and the Victorian era in Britain polarized the notion of the private vs. the public, bringing us to the second key point about this volume. What may be read as positive outcomes of philosophical discourse in the eighteenth century materialized into a darker legacy of surveillance and discipline designed to produce “good” citizens and to reform those falling into abyss of crime and immorality. What struck her most in the chapters devoted to modern-day privacy, technology, poverty, and labor is that certain themes are strangely haunted by the Victorian past. Nowhere is this haunting clearer than in how the control of bodies in supply chain workspaces eerily echoes the disciplinary techniques of the Victorian prison and factory, where docile bodies endured relentless surveillance, embodied by the all-seeing eye of the Panopticon, the ultimate shadowing system designed to make workers or inmates feel as if they were being watched at every moment even if they were not.

Perfected by Utilitarian philosopher, Jeremy Bentham (d. 1832), the Panopticon took the physical presence of the jailor or factory floor-manager and inscribed it onto the impersonal architecture of prison and industrial workspace. Whereas in the medieval monastery, monks went through their daily paces conscious of the watchful gaze of the omnipotent Deity, Victorian laborers and inmates operated under a regimen in which they could be observed at any moment by those in control of their lives, but they could not see their controller, whose presence was obfuscated behind a system of blinds and spotlights emanating from the warden’s box. The prisoner and the factory laborer were to

become the masters of their own productive habits due to the fear of all-encompassing, punitive supervision. In Bentham and other nineteenth-century reformers' view the endgame was self-evident: the moral reform of those now had lapsed and the improved efficiency of those toiling under dire circumstances in the Victorian workhouse. These reforms then, theoretically speaking, led to an overall improvement of the common good and its overall happiness.

Taking the philosophical paradigm of the Panopticon on a road trip to the modern workplace of truck or supply chain warehouse, it is possible to detect strains of Utilitarian philosophy in the present era. Cameras installed inside of truck cabs monitor the driving behaviors of truckers, Smartwatches worn on employee wrists to gage the efficiency of their movements, and ultrasonic bracelets monitoring laborers' engagement high-tech equipment prove that we have entered a new era of the Panopticon, where the coercive power of jailor and faculty floor-supervisor no longer merely transfers to the architecture of the prison or factory. Now that surveillance-regime is miniaturized. It can be worn, carried, or installed in proximity to its user.

As the chapters in this book have argued, the technological Panopticon of the contemporary world infringes on privacy and private space, often under the guise of the public good and capitalist efficiency, in ways that demand a second volume on *Human Privacy* devoted to this subject alone.

REFERENCES

- AICPA/CICA. (2020). *Privacy Management Framework. Issued by the Information Management and Technology Assurance Executive Committee*. Retrieved June 3, 2023 from <https://www.aicpa-cima.com/resources/download/privacy-management-framework>
- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company.
- Coon, L. (2011). *Dark Age Bodies: Gender and Monastic Practice in the Early Medieval West*. University of Pennsylvania Press.
- Culnan, M., & Bies, R. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), 323–342.
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-commerce Transactions. *Information Systems Research*, 17(1), 61–80.
- Foucault, M. (1977). *Discipline and Punishment: The Birth of the Prison*. Vintage Books New York.

- Posner, R. A. (1981). The Economics of Privacy. *The American Economic Review*, 71(2), 405–409.
- Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, 4(2), 155–169.
- Roessler, B., & DeCew, J. (2023). Privacy. In E. N. Zalta & U. Nodelman (Eds.), *The Stanford Encyclopedia of Philosophy* (Winter 2023 ed).
- Shah, R., & Kesan, J. (2007). How Architecture Regulates. *Journal of Architecture and Planning Research*, 24(4), 350–359.
- Zhu, Y., Kanjanamekanant, K., & Chiu, Y. (2023). Reconciling the Personalization-Privacy Paradox: Exploring Privacy Boundaries in Online Personalized Advertising. *Journal of the Association for Information Systems*, 24(1), 294–316. <https://doi.org/10.17705/1jais.00775>.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Public Affairs.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



PART I

Foundations of Human Privacy



CHAPTER 2

Exploring Privacy from a Philosophical Perspective: Conceptual and Normative Dimensions

Sharon Mason

Extended Abstract

Philosophical approaches to privacy focus on clarifying its many dimensions, providing a conceptual foundation for thinking about privacy in deep and fruitful ways. The modern concept of privacy developed as new technologies, such as print media and photography, made new types of exploitation possible. In response to the possibility of these new harms, legal and philosophical theorists began to develop analyses of privacy, including the concept of privacy rights and justifications for protecting privacy. Some philosophers have noted that there is no single concept of privacy. Instead, privacy can refer to a variety of different things, such

S. Mason (✉)

University of Central Arkansas, Conway, AR, USA

e-mail: smason@uca.edu

as access to information; ownership or control of information, physical spaces, or particular objects; a private domain contrasted with the “public” domain; or appropriateness in what may be viewed by others. This chapter explores some of these concepts of privacy, examining how pluralism about the many different dimensions of privacy reflects ongoing technological change.

Philosophical inquiry also explores the normative and ethical dimensions of privacy, including questions about why privacy is valuable and how it is related to other values. Some of these areas of focus include the relation between privacy and security, privacy and ownership, privacy and the conditions for democratic society, privacy as a means of commodifying the self, and the role of privacy in the possibility of intimacy with others. Another area of focus involves understanding how privacy is related to fundamental moral principles, such as preventing harm, preserving individual freedom, protecting human rights, and promoting justice. Overall, normative inquiry aims to develop a moral framework for when and why privacy should be protected, and when and why it should not.

INTRODUCTION

The philosophical study of privacy focuses on its conceptual and normative dimensions. One key area of analysis involves clarifying the many concepts of privacy that are in use, focusing on evaluating definitions and key distinctions. These analyses are partly aimed at the clarification of various notions of privacy, but they are also often targeted at the development of new insights into privacy. The goal is to develop a coherent, rationally supported conceptual framework for thinking and talking about privacy.

A second key area of philosophical analysis deals with normative questions. Normative questions ask what ought or should be, in contrast to descriptive questions, which focus on identifying how things are. The normative study of privacy considers questions about the value of privacy and the moral dimensions of privacy, including the examination of privacy rights. Some examples of normative questions about privacy include: What sorts of privacy should be protected, and why? When is it morally acceptable to violate someone’s privacy, and for what reasons? Is a particular privacy protection good or bad, and why? What are our current goals

and values, and how should we change current privacy laws, attitudes, and practices to align better with those goals and values?

As is perhaps already apparent, the conceptual and normative dimensions of philosophical inquiry are intertwined. There is a normative dimension to conceptual inquiry, for in addition to its clarificatory aims, conceptual inquiry generally has a prescriptive aspect. Some ways of thinking about privacy may be better than others, perhaps because they are more coherent, shed light on important adjacent concepts, or in some other way serve as more useful conceptual tools for thinking about privacy. So, too, our concepts of privacy influence normative inquiry, providing the language of thought with which values and ethics are expressed and explored.

The first section of this chapter focuses on conceptual dimensions of privacy, centering on the development of the concept of privacy in Anglo-American legal and philosophical traditions. The chapter then addresses the question of why numerous philosophers assert that there is no single concept of privacy, arguing that there is an expected pluralism in a concept that has evolved largely in response to extensive technological innovation. The second section explores some normative questions about privacy, concentrating on why privacy is valuable, if indeed it is, as well as on how privacy interacts with other values. Some of these other values are widely recognized, such as the interplay between privacy and security, or privacy and ownership. Some of them are more subtle, such as the role of privacy in enabling democratic society, the construction of the self, and our management of relationships with others.

CONCEPTS OF PRIVACY

What is privacy? What makes something in the domain of the private, instead of the public? When one values privacy, what is it that one cares about? These are questions about the concept of privacy, insofar as they explore what privacy is and is not, as well as how it is related to other concepts. The aim of this section is to explore the concept of privacy, starting by identifying some common notions of privacy in current use. This section also traces some older philosophical analyses of privacy, considering why a single definition of privacy has been elusive and arguing that pluralism in various concepts of privacy is not a problem to eliminate, but rather a feature of a concept whose development has been deeply intertwined with changing technologies and social interests.

In response to the question, “What is privacy?” many philosophers have noted that the term “privacy” is used in a variety of contexts, and no single definition of privacy applies to *all* the uses to which the term is put in our ordinary conversations about privacy. Also, it is not always clear how varying notions of privacy relate to one another. For example, information privacy often emphasizes the idea of *control over access to information*. In a classic paper, Alan Westin (1967) describes privacy as “the ability to determine for ourselves when, how, and to what extent information about us is communicated to others” (cited in DeCew, 2018). Control over access to information is often viewed as essential to managing risk and mitigating harm, especially in relation to decision-making processes (Anglim et al., 2015). For example, medical information (see Hester chapter in this volume) informs decisions about life insurance and health care premiums, and credit records can affect employment decisions. Information is powerful, and privacy protections are often aimed at keeping information from harming people.

Privacy can also mean *control over access* to both physical spaces and to experiences. Privacy as control over access often involves notions of *ownership* more generally and frequently appeals to notions of personal property and individual rights. A beach is private when access is limited, perhaps to the owner or to a private resort. A person’s private residence may not be entered by others without permission: police officers must obtain warrants; trespassers may be prosecuted. Ownership rights apply regardless of any additional harm that might result from unsanctioned access. If someone accesses private information without permission, one might object that they have violated a person’s privacy rights, even if no further damage resulted. It is also possible to have control over access to experiences. For example, a person’s inner thoughts and feelings are private in the sense that they occur only to one’s own conscious experience. It is a stretch to think of inner experience as one’s personal property, yet much of a person’s inner life is private unless and until that person decides to share it.

Another notion of privacy references a *domain*, where the “private” domain may be contrasted with the “public” domain. Things in the public domain are open to use by anyone, while things in the private domain are restricted to the concern of particular individuals. Privacy is often cited in arguments for reproductive rights and gender-related medical care, which view medical treatment as private in the sense that it should be exempt from government interference. Calling a person’s property, affairs, and

beliefs “private” can indicate that they are *outside the scope of relevance*. Other examples include religious beliefs, which are considered a private matter in many contexts, and thus outside the purview of the things that the state should be concerned with in its oversight of the activities of its citizens. So too, some types of private beliefs are protected from being relevant in hiring decisions, college applications, loan applications, and more.

Privacy also sometimes refers to *what is appropriate for the viewing of others*, especially in relation to cultural norms of politeness, but also as it relates to the experience of being unobserved. One example comes from Annabelle Lever (2012), who explores privacy as it relates to “interests in anonymity, seclusion, confidentiality, and solitude” rather than privacy as it relates to ownership or a private domain. Privacy can designate a category in which unseemly things are hidden, things often having to do with bodily care. Children are taught privacy and modesty in order to know which sorts of behaviors are appropriate in front of others and which are not. For example, trimming one’s toenails should be done in private, not because it is important to limit access to one’s toenails or protect ownership rights to one’s toenails, but rather because cultural manners dictate keeping certain grooming activities to oneself.

In a now-classic article on privacy, Judith Jarvis Thomson (1975) remarks that “The most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.” She was not claiming that there are no definitions of privacy, but rather that there are many different uses of privacy, with no single definition that fits all the possible uses. This view has persisted, as Alastair Macleod (2018) recently argued that “The uses to which the notion of privacy is put in contexts of different sorts are so diverse that no unifying definition is available.” Despite the resignation that is apparent in both Thomson’s and Macleod’s observations, the lack of cohesiveness among the various concepts of privacy is itself interesting and worthy of further exploration. It also reveals something important about the way that the concept of privacy has developed, as well as how philosophical work on privacy proceeds. Exploring both those claims is the focus of the remainder of this section.

The main idea is that among the many changes that are driven by technological innovation, one fluctuation involves the concepts and theory underpinning our legal and moral thinking. The philosophical analysis of privacy is a primary means by which it is possible to, as Herman Cappelen

(2018) puts it, actively participate in “the project of assessing and developing improvements of our representational devices,” which in this case are our representational devices for thinking about privacy.

Concepts are a primary tool through which human beings think about the world. They are, as Cappelen observes, a core representational device that enables thought about external reality, from mundane objects such as tables and chairs to complex, abstract ideas such as privacy. These concepts form the basis for understanding various parts of our experience, including what we can notice, describe, and communicate to others. Philosophers have many goals, including lofty aims such as the pursuit of truth, wisdom, and understanding, or perhaps more modestly, the aim to discover what it is reasonable to believe. But one thing that many philosophers also do is analyze and engineer concepts, which is—as the name suggests—the “project of designing, evaluating, and implementing concepts” (Chalmers, 2020). Concepts develop and change according to the various needs and interests of the people who use them to understand and describe various aspects of their world.

Consider a brief historical sketch of the development of the concept of privacy in philosophical use. Go far enough back in history, and for many philosophers the problem of how to live well together was much more pressing than any problems that concerned privacy. For instance, Plato’s discussion of privacy is quite sparse. He explores the consequences of invisibility on moral behavior in a famous thought experiment about the Ring of Gyges in Book 2 of *The Republic* (Cooper, 1997). There, he focuses on the effects of observation and the consequences, including social approval, of acting justly. Socrates argues that few, if any, would act justly if there were no consequences for injustice, but that a truly just person’s behavior would be unaffected by invisibility because their justice would be motivated by a genuine concern for the good. Yet again, Plato’s concern was not about privacy as a right or as a good that contributes to a person’s well-being. His focus was on illuminating the demanding standards that are met by a truly just person and showing the relation between justice and a happy life.

Aristotle distinguished between the *polis*, or city, and the *oikos*, or home/domestic spheres, as two distinctive domains with distinct virtues, or excellences. He viewed excellence in public life as requiring a different set of virtues than excellence in private life (Embler, 2015b; Lord, 2013). Aristotle’s account is also an example of a deeply gendered division in conceptualizing privacy, where men belonged in the public sphere,

women in the private, especially those in the upper-classes. Even so, his theorizing about privacy is minimal. His attention was not focused on developing a notion of the *private*, but on developing a robust notion of the *public*, including attention to the possibility of citizenship, the obligations we have toward others, and the structure of a just society.

Moving forward over a millennium, the notion of privacy receives limited attention from Enlightenment philosophers, even those particularly interested in social, political, economic, and psychological affairs. David Hume, for example, uses the term “privacy” to mark a distinction between what concerns the goals or good of all members of society (public interests) versus what concerns the goals or good of a particular person (private interests). Hume’s use of the word “private” is essentially equivalent to what benefits the individual, and his usage is consistent across various references to private interest, private education, and private benevolence. (See Hume’s *A Treatise of Human Nature* especially Book 3; *Enquiry Concerning Morals*, Section 5 for examples.) In Hume’s work, the notion of privacy marks the distinction between a public domain and a private domain, but privacy is still not conceptualized as a robust individual right.

To find a more contemporary notion of privacy, we must look to a more recent source. In a well-known essay by Louis Brandeis and Samuel Warren titled “The Right to Privacy” (1890), Brandeis and Warren identified a need to develop legal protections based on what they called a “right to be let alone,” calling this “the next step which must be taken for the protection of the person.” Interestingly, they cite a variety of technological advancements as the impetus for the development of both the notion of a right to privacy and its subsequent legal protection. While by this point print media had existed for centuries, late nineteenth-century society saw an increase in the publication of gossip columns and pamphlets. As their production and dissemination increased, so too did the damage to the reputations of their unfortunate subjects. A second problem was the relatively new capability of photography to capture images, as well as “any other modern device for recording or reproducing scenes or sounds.” These new technologies created the possibility for new types of harm.

Warren and Brandeis argued that there was a need for the development of legal protections for privacy in light of new technological advancement that made these new harms possible. Their argument used protections for personal property as a model. However, they articulated the value

of privacy as extending beyond ownership and property rights, maintaining that privacy itself was a good associated with free flourishing as a human person: “Urging that they were not attempting to protect the items produced, or intellectual property, but rather the peace of mind attained with such protection, they said the right to privacy was based on a principle of ‘inviolate personality’ which was part of a general right of immunity of the person, ‘the right to one’s personality’” (DeCew, 2018; citing Warren & Brandeis, 1890). Their arguments began a discussion in US law, political theory, and ethics about the value of privacy protections, laying the groundwork for thinking about privacy as a fundamental human right and as essential to human flourishing. (For a more detailed summary of this history, see Anglim et al., 2015.)

This brief overview suggests a way to think about the pluralism that many philosophers have encountered in the various concepts of privacy that are in use. The standard in philosophical conceptual analysis has for some time been to articulate a single definition of a concept that captures what is distinctive about the thing one is trying to define. These definitions give clarity about the concept and provide a basis for sorting out borderline cases. Some concepts do not, however, have that unity. Privacy seems instead to have several interrelated meanings, without it being possible to identify a single core concept that applies in all cases. Lever (2012) suggests that the various overlapping concepts of privacy may be due to the fact that privacy is intertwined with other notions whose edges overlap with privacy: “The main reason why it is hard to define privacy--the absence of a set of necessary and sufficient conditions which would enable us to identify privacy and to distinguish it from allied concepts--suggests that the fuzziness of our concepts of liberty, equality and rights may, themselves, explain why the boundaries of privacy are hard to fix.” Some concepts have fuzzy edges, which means they overlap with closely related concepts to the point that there is not a sharp distinction between where one concept ends another begins.

Lever’s analysis may be correct, but it is not complete, for there is more to the story of why there seems to be an ineliminable pluralism in the concept of privacy. It seems likely that privacy is a concept that has a structure referred to by Ludwig Wittgenstein (1953) as a *family resemblance concept*. When careful analysis does not reveal a core notion, Wittgenstein recommends that “We should, instead, travel with the word’s uses through ‘a complicated network of similarities overlapping and criss-crossing’” (PI 66, cited in Biletzki & Matar, 2023). The philosophical

work of understanding privacy involves precisely this sort of traveling through the various uses of privacy that have been developed as people create and tweak conceptual tools for thinking and talking about their experiences.

In the late nineteenth century, Warren and Brandeis were arguing for a new extension of the law, but they were also developing a new concept of privacy rights that had not yet existed in quite that form. Perhaps there are various concepts of privacy because the idea of privacy has been in constant reconsideration, revision, and expansion. As the world changes, so does the need for ongoing innovation in our laws and moral principles, but also in our concepts. The need to develop privacy law spurred the development of philosophical accounts of privacy aimed at gaining a better understanding of privacy's value, the specific ways in which privacy was under threat, the harms that might result from failing to protect privacy, and a clearer articulation of what was to be gained by developing a robust theory of privacy rights. In particular, technological and social change drive this development. It seems all but certain that the future will continue to see innovations that make new kinds of exploitation possible, and that our current understanding of privacy will need to continue to develop in response.

While acknowledging the need for flexibility in our thinking about privacy, we can also provisionally define different types of privacy as they are relevant to specific contexts. An operational definition need not apply to *all* possible contexts in which privacy is relevant. Rather, those who work on issues related to privacy ought to specify what is relevant to the inquiry at hand, keeping in mind the possible need for future revision. Working to illuminate different conceptions of privacy and show their significance can help clarify and refine our thinking, as well as suggest new ways of thinking about privacy in the future.

NORMATIVE DIMENSIONS OF PRIVACY

In addition to exploring the conceptual dimensions of privacy, philosophers also try to answer normative questions about privacy. Normative questions ask not what is, but what should or ought to be. Ethics is normative in the sense that ethical principles aim to guide action, moving beyond the way things actually are to examine how people should act, given a broader context of values and moral principles. Part of the normative study of privacy involves understanding the value of

privacy, especially why privacy is valuable and how it interacts with other values. For instance, does privacy have intrinsic value which should be protected for its own sake? Or is the value of privacy instrumental, derived from its relation to other goods that it makes possible? The normative study of privacy also involves developing various moral arguments for when and why privacy should be protected, given various goals such as promoting justice, protecting privacy rights, and contributing to a flourishing life. Finally, the normative study of privacy includes feminist analyses of privacy, which focus on exploring how privacy is entangled with various forms of gender discrimination and how privacy relates to efforts to promote justice, equality, and human dignity (e.g., Allen, 2011; DeCew, 2015; Mackinnon, 1989; Williams, 1991).

Notably, the normative study of privacy should not be thought of as isolated from descriptive inquiry, which focuses on inquiry about what is the case. In the same way that the concept of privacy has developed in response to social and technological change, new ethical challenges arise as changes in technology create new ways of collecting and sharing information, thus creating new possibilities for harm. As Catherine Wilson (2019) puts it, "...societies evolve new forms of organisation and new technologies. Morality has to play catch-up as clever humans discover new ways to deceive, use, coerce and rob one another that were not previously available.... New moral norms have to be worked out through discussion and debate by the public, including philosophers and journalists, and new forms of conscience instilled by educators. These norms, too, are subject to revision in the light of changing circumstances." Responding to technological change requires careful attention to the many ways in which privacy may be threatened, as a matter of clear description of the current circumstances and challenges to privacy. These descriptions motivate extending normative analyses to new contexts, identifying where established moral values apply, and identifying when a new development prompts revision in our moral ideals.

Warren and Brandeis could scarcely have imagined all the ways in which it is now possible to collect and use information in harmful ways. There is an ongoing need to extend the application of normative standards in response to new technologies in order to manage technological innovation in a way that coheres with other values such as the protection of individual rights, the prevention of harm, and the promotion of security. This section explores some of these areas of ongoing normative inquiry about privacy.

The Value of Privacy

A foundational distinction in value theory distinguishes between value that is intrinsic vs. value that is instrumental. *Intrinsic value* is value that is internal to a thing. If privacy has intrinsic value, then privacy has value in and of itself, regardless of its relation to other goods. Those who take privacy to have intrinsic value sometimes view privacy as a basic human right or as a fundamental good, worth protecting and preserving in its own right. Many who view privacy as an intrinsic good also claim that there is something distinctive about privacy, arguing that the value of privacy cannot be fully reduced to the value of something else, such as property ownership or personal security.

If privacy has *instrumental value*, then its value is derived from the contribution it makes to some other valuable end. Instrumental value is derivative, meaning that the value of a thing comes from its usefulness as a tool, or instrument, for achieving something else. This view is sometimes described as a type of *reductionism*, the claim that the value of privacy can be fully explained by describing the other valuable ends to which privacy contributes. Also, the value of privacy then depends on whether privacy does, in fact, help achieve those goals, rather than existing as something to be pursued for its own sake.

These types of values are not mutually exclusive. Something might have both intrinsic and instrumental value, if it is both valuable for its own sake, and valuable insofar as it leads to other, desirable ends. Thus, it is possible that privacy has intrinsic value as a basic human good *and* that privacy also has instrumental value because it supports other goods, such as preserving personal security and enabling democratic society. In addition, although accounts differ about the sorts of goods that privacy enables and their relative importance, there is general agreement about the fact that privacy has instrumental value.

In contrast, there is disagreement about whether privacy has intrinsic value. One significant challenge comes from the fact that there is cultural variation in viewpoints about the importance of privacy. If something has intrinsic value, there is a sense in which its value is self-evident. After all, one cannot show that something has intrinsic value by appealing to its importance in achieving some other valuable end. That would show that the thing has instrumental value, not intrinsic value. Simply put, it does not seem that the value of privacy is self-evident. Rather, it appears to be culturally specific. Although some scholars argue that there are some

cross-cultural similarities in privacy protections (Embler, 2015a), it is far from obvious that privacy is universally recognized as having intrinsic value (see Hawkins chapter in this volume).

Privacy need not be intrinsically valuable to be instrumentally valuable, however. The question about intrinsic vs. instrumental value focuses on how to best understand why we value privacy, not whether privacy is valuable at all. Even if there is nothing distinctive about privacy that makes it valuable for its own sake, privacy might still be important and worthy of protection. An instrumental value can still be “something in the enjoyment of which all human beings have a defensible personal stake” (Macleod, 2018). Exploring privacy as an instrumental good has been quite interesting and fruitful, for it involves examining the ways in which privacy is related to other values. Clarity about the values that support the protection of privacy is essential for understanding why privacy should be protected. These analyses can also provide a basis for evaluating particular privacy protections.

Even so, there is no guarantee that an account of the value of privacy will be simple or straightforward. On the contrary, there are layers of complexity and overlapping values in our lives. Sometimes our values mutually support one another, but sometimes they are in tension with each other. Our values come into conflict with the values of others, and we cannot assume that we are even aware of all the nuanced layering of our motivational structures (Nguyen, 2022). Thus, even if there is no single answer to the question of why privacy is important to us (Rachels, 1975), we might find instead a constellation of values that privacy supports.

Furthermore, we have already seen that the development of the idea of privacy as a fundamental right in the Western philosophical and legal tradition was a relative latecomer to the discussion of natural rights that began several centuries before. The idea of natural human rights is an idea with a particular historical development. It is also an idea that has had significant political, moral, and legal influence, providing guidance for how people should treat one another and what we can reasonably expect from our political system. As such, questions about whether privacy has intrinsic value might be more useful if transformed into questions such as “Are there good reasons to include privacy as one of the things that we choose to treat as a fundamental value?” and “What happens if morally and legally we extend to privacy the status of a fundamental right?”

The remainder of this chapter explores some of the constellation of values that philosophers have identified as being related to privacy. Some of these are values that privacy promotes and supports, while others are in tension with protecting privacy. This discussion is not exhaustive, but will emphasize particular areas of recent interest: (1) privacy and security, (2) privacy and transparency, (3) privacy and democratic society, (4) privacy rights, (5) privacy and the self, and (6) privacy and commodification.

Privacy and Security

Privacy has a close relationship to security. Privacy supports certain types of security, thereby protecting against harms such as identity theft and voyeurism. We limit access to some personal information, such as social security numbers or credit card numbers, to protect people from identity theft. Facial recognition software surveys thousands of faces at airports, an invasion of privacy that some say will make air travel more secure (Gentilo & Santana, 2023). Privacy protections can also prevent public embarrassment that leaves a person feeling exposed.

At the same time, privacy can enable harm when it is used as a shelter to hide harmful behavior. As DeCew explains, “privacy appears to be something we value to provide a sphere within which we can be free from interference by others, and yet it also appears to function negatively, as the cloak under which one can hide domination, degradation, or physical harm to women and others” (2018). Many feminist scholars have documented various ways in which appealing to the value of privacy has provided legal protection for various types of gendered violence (Allen, 2011).

The notion of privacy also designates some aspects of life as being outside governmental control, exempt from certain kinds of interference in domestic affairs. As a result, protections for privacy of personal dwellings and family relationships have historically been a source of support and protection for abusers. Privacy protects domestic life from unauthorized observation, but also plays a role in enabling domestic abuse (Allen, 2011). In fact, some feminist authors have argued that the private/public distinction is itself problematic, suggesting a rethinking of the distinction between public and private domains (for example, see Landes, 1998).

Privacy and Transparency

Transparency provides a balance to privacy, as it deals with the legitimate disclosure of certain types of information in certain contexts. Transparency is a tool against the misuse of privacy to hide problematic behavior, and it is often cited in cases where things such as reasoning, justification, bureaucratic processes, and decision-making should be available for review to interested parties or to the general public. For example, when decisions affect others, transparency about decision-making processes gives some assurance of fair treatment in contexts such as the allocation of funds, selection of job candidates, or calculating a student's grades. Transparency promotes trust.

At the same time, transparency can be a double-edged sword. In a recent paper, C. Thi Nguyen (2022) argues that transparency can be deeply opposed to trust, especially when expertise is involved. The demands of public transparency are often aimed at reducing corruption. However, transparency can also require that experts "act within the range of public understanding." Nguyen articulates a number of problems that can result from this requirement, including the pressure to articulate reasons in non-expert language which distorts the description of the actual reasoning process, the preference for metrics of evaluation that are simple and easy to understand over those that may be more accurate or that reflect a plurality of values, and the erosion of the implicit knowledge that is characteristic of expertise. Nguyen views the tension between public transparency and expertise as ineliminable: "Transparency works to eliminate the non-explicit and the private. That is where corruption and bias live -- but also sensitivity, expertise, and intimacy. There is no getting around this tension" (Nguyen, 2022). Sometimes this cost will be worth paying, but it is good to know what exactly one is trading when pursuing transparency, especially when experts are expected to provide justification that is accessible to the general public.

Privacy and Democratic Society

Many discussions of privacy assume some version of *liberalism*, a theory that takes the preservation of individual freedom and individual rights as fundamental in political and social theorizing (Bell, 2014). The term "liberal" traces its origins back to "liber," a Latin adjective that means "free." It is also the word from which the English term "liberty" is derived.

Roughly, a liberalist perspective on privacy emphasizes the protection of privacy insofar as it promotes and protects individual liberties, while opposing privacy laws that interfere with individual liberty. Privacy is often taken to be essential in contributing to “the right to the enjoyment of opportunities for the living of a satisfying and fulfilling life” (Macleod, 2018).

Recently, Annabelle Lever (2012, 2015a, 2015b) has also developed a democratic justification for the protection of privacy, emphasizing the importance of some forms of privacy for democratic society. As she explains:

The point of protecting privacy from a democratic perspective is not that privacy is some preeminent individual good because of its connection to human dignity, intimate and familial relationships or to property ownership—as it would be from liberal perspectives. Privacy may or may not be justified on these grounds. The point, rather, is that protection for anonymity, confidentiality, seclusion, and intimacy—to name a few characteristics of privacy—helps to foster the freedom and equality necessary for democratic politics by structuring and limiting competition for power in ways that enable people to see and treat each other as equal despite incompatible beliefs, interests, and identities.

Lever argues that some forms of privacy are required for democratic governments to function. On the one hand, voter privacy allows individuals to vote according to their conscience, without fear of repercussions. Without voter privacy, things such as voter intimidation or retaliation can exert significant sway over voters, thereby threatening democratic elections. On the other hand, making legislative voting records of elected officials public contributes to their accountability as representatives of their constituents.

The distinction between Lever’s democratic defense of privacy and justifications for privacy rooted in liberalism is not entirely clear. To the extent that the justification for democratic government is based on liberal ideals such as the value of self-governance, the role of consent in legitimating governmental authority, and the protection of unalienable rights, a democratic justification for protecting privacy might itself rely on liberal arguments that give support for valuing democratic governance. Even so, Lever’s analysis provides a helpful detail of many of the specific ways in which democracy and privacy are intertwined.

Privacy Rights

While we have already discussed the development of the concept of privacy as a fundamental right, the notion of privacy rights is also important in normative explorations of privacy. Rights come with both entitlements and obligations. For instance, if a person has a right to privacy, then they are entitled to privacy of some sort, and others are obligated not to violate their privacy. Legal privacy rights create entitlements and obligations that are codified and protected by law, as are the legal consequences of being caught violating these rights. Fundamental or natural rights are entitlements and obligations that apply to all human beings and there is a moral obligation to protect them. Ideally, a legal system will recognize and protect fundamental human rights, although the existence of those rights does not rely on such recognition or protection. An appeal to fundamental human rights can provide arguments for changing the law to bring it into alignment with moral imperatives.

A robust notion of privacy as a fundamental human right plays another important role in moral thinking about privacy. Privacy protections that focus on preventing possible harm, such as those discussed in the section on privacy and security, treat privacy as instrumental to other goals, such as security or general well-being. These approaches are *consequentialist*, in the sense that they emphasize the consequences of protecting or not protecting privacy. Privacy should be protected when its protection leads to a good outcome; privacy should not be protected when its protection leads to a bad outcome. If privacy is a fundamental human right, however, then it should be protected independently of any further harm that might result.

It is sometimes said that surveillance is not a problem if one has nothing to hide, or that privacy is unnecessary in the absence of personal guilt. If privacy is a fundamental right, then it is important to protect privacy for its own sake, even if one has nothing to hide. Perhaps privacy is important not just because of its role in avoiding negative consequences such as financial loss or public embarrassment, but perhaps it is also important because it is somehow fundamental to human dignity. The next section explores this possibility, considering how privacy might occupy a special role in the development and ongoing construction of the self, as well as in our ability to develop intimacy with others.

Privacy and the Self

In a now-classic essay, Jeffrey Reiman (1976) emphasizes the role of privacy in fully developed personhood, arguing that privacy is “a social ritual by means of which an individual’s moral title to his existence is conferred.” Reiman’s analysis places privacy among the basic rights and obligations that are essential to recognizing and interacting with someone as a co-person, rather than as an object or as a less autonomous being. According to this view, there are certain fundamental abilities and expectations that are morally basic to full personhood. Reiman claims that the right to privacy “is the right to the existence of a social practice which makes it possible for me to think of this existence as mine. This means that it is the right to conditions necessary for me to think of myself as the kind of entity for whom it would be meaningful and important to claim personal and property rights.” Viewing oneself as entitled to certain kinds of privacy requires viewing oneself as a subject capable of making decisions about one’s own experiences and how those experiences are shared with others. Privacy is an expression of autonomy, and the absence of any control over one’s own privacy threatens the conception of oneself as an individual self at all.

Furthermore, just as the ability to conceptualize certain aspects of experience as one’s own is an expression of autonomy, so too is the ability to decide which aspects of one’s experience one wishes to share with others or to hide from others. The ability to control privacy is central to the cultivation of intimacy insofar as intimacy is fostered in part by the willing disclosure of private details about oneself. Close friends and family often have access to various aspects of each other’s lives that indicate varying levels of intimacy in those relationships, and the decision to share personal details with someone is an important way of building trust. Sometimes trust also motivates the protection of privacy. Preserving the privacy of a loved one can be an expression of care and respect, such as the respect shown by allowing a person to disclose personal details if and when they wish. A loss of privacy can undermine a person’s ability to regulate their own interactions with others, and a sustained inability to have any say in what remains private in one’s own life signals that one’s life is not, in fact, much of one’s own. It is for this reason that the loss of control over one’s own privacy can be experienced as a significant personal violation, as evidenced by the experience of exposure and helplessness that sometimes results from invasions of privacy.

Reiman's analysis has also played an important role in many analyses of privacy. For instance, Lever (2012) considers a sense of privacy that is tied to our sense of ourselves as moral agents. Her argument is worth quoting at length:

Just as our willingness to grant privacy to others can reflect respect and trust—and be valued and desired for that reason—our willingness to act anonymously, confidentially, or discreetly can reflect a mature and considered decision to avoid burdening others with our problems, or to avoid forcing them to confront features of the world with which they may be unwilling or unable to cope...This is partly because our interests in privacy are not purely instrumental but seem sometimes to be ways of affirming, even constituting, ourselves as people to be trusted, respected, and deserving of liberty, equality, and happiness. Indeed, while privacy can be necessary to our security and be desired for that reason, people are sometimes willing to risk their lives and health in order to maintain anonymity, seclusion, and confidentiality.

By recognizing privacy as a way of “affirming, and even constituting, ourselves,” Lever is highlighting the relevance of privacy to the development and management of certain types of character. Privacy might be preserved out of respect for another person, but it also might be motivated by the desire to be a trustworthy, discreet, and reliable person. Being motivated by genuine respect for others and being motivated by the desire to develop one’s own character in certain ways are often mutually reinforcing goals.

Similarly, Iris Marion Young (2004) notes that “An important aspect of the value of privacy is the ability to have a dwelling space of one’s own...in which one lives among the things that help support the narrative of one’s life.” Young’s observation is particularly relevant for views about personal identity that suggest that persons are narrative selves, authors of their own stories, and interpreters of experiences and their significance (Rea, 2022). Without a (literal or metaphorical) place of one’s own, it is difficult to play a significant role in determining the trajectory and meaning of one’s own life.

Anita Allen (2011) likewise emphasizes the importance of privacy to the self, although her view goes further than Reiman’s insofar as she argues that some types of privacy are so fundamental to the self that a person should not be permitted to give away privacy rights in certain contexts, even if they willingly consent to do so. One concern is aimed at

preserving “the experience of privacy and the habits of respect for privacy it constitutes.” Another concern is that giving away some privacy rights results in harms that are worse than the paternalism she is suggesting. Her suggestions are tentative but striking in a context where privacy protection is often intertwined with the value of personal autonomy. As she puts it, “If people are completely morally and legally free to pick and choose the privacy they will experience, such as deferential civility, appropriateness and limited data flow, they are potentially deprived of highly valued states that promote their vital interests, and those of fellow human beings with whom they associate. We need to restrain choice—if not by law, then somehow” (2011). If she is correct, then some privacy rights are inviolable, resistant even to a person’s own desire to relinquish them.

Privacy and Commodification

A final area of focus concerns the ways in which privacy has been increasingly commodified. Privacy can be traded for access to goods and services, some of which are essential to participating in the modern world. We let our internet browsers track our search history in exchange for access to the internet. Our phones can now broadcast our location at any given moment, enabling friends to find each other quickly and targeted messages to be sent when close to a restaurant or event. Sometimes we are informed about the surveillance of our lives, but often the language with which we indicate consent is buried in the fine print and it is easier to simply click “I Agree” than to read through all the details. Anglim et al. (2015) refer to this as a paradox of privacy: “On the one hand, we benefit from the easy exchange of personal information through digital communications. On the other, we give up some degree of control over what happens to that information. Is that an appropriate trade off? Is it worth it?”

A further complication is that it is not always apparent what, exactly, is being traded. Privacy that can be bought and sold is another way of turning ourselves into commodities, along with our time, attention, and labor. Privacy can be viewed as a type of capital which can be used to purchase goods and services. For instance, “free” access to social media is in fact “purchased” in part by the disclosure of information that can be turned into a profit by selling it to advertisers.

Patricia Williams (1991) highlights this dimension of privacy, considering “the degree to which it might be that public and private are

economic notions, i.e., that the right to privacy might be a function of wealth.” As with other forms of capital, the amount of control one has over privacy now often depends on the money one is able to spend. A particularly high-profile example of the ability to buy privacy occurred in 2013 when Mark Zuckerberg famously purchased four homes that surrounded his own home in Palo Alto, CA. The purchases were reportedly in response to the fact that “a developer wanted to purchase one of his neighbor’s homes and use the fact that Zuckerberg lived close by as a marketing tactic” (Shontell, 2013). Zuckerberg’s privacy had a price tag of around \$30 million. Perhaps it is for good reason that Williams refers to privacy as a “bargained freedom.”

The increased commodification of privacy raises concerns about equal access to privacy, as social and economic disparities result in significant disparities in privacy protections. When privacy is the commodity being bought and sold, there is concern about a significant incongruity between those who have the resources to protect their privacy and those who do not. This disparity exists in terms of both wealth and education, as both provide increased access to the means for protecting one’s own privacy.

LOOKING AHEAD AT FUTURE CHALLENGES

Technological development will almost certainly continue to drive conceptual and moral thinking in the future. This chapter concludes by briefly considering a current area of emerging concern: developing robust moral and legal guidelines for privacy protections in response to the possibilities of big data and AI generated content. While individual action is still meaningful, a person’s privacy is increasingly affected by decisions at levels far beyond their individual control. Furthermore, even if individuals want to protect their own privacy, the barriers can be overwhelming. Simply becoming aware of the various ways in which privacy may be breached can require a significant investment of time into understanding technologies such as social media, smartphones, facial recognition, AI, and more. The challenge of protecting one’s own privacy grows as the knowledge and time investment required to even understand possible threats to privacy become prohibitively large for a person who does not have specialized knowledge in the field.

Furthermore, knowledge does not always lead to the ability to take meaningful action to protect privacy. Almost three decades ago, Priscilla Regan (1995) noted that “Privacy is rapidly becoming a collective value

in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy." Achieving meaningful privacy protection requires collective action, cooperation from large corporations, and government regulation, given the large scale of influence necessary for effective change.

Regan's observation rings all the more true in our world of increasing technological interdependence. The responsibility to protect privacy will increasingly be unable to be borne by the individual, and those concerned with protecting privacy must insist that privacy be protected within the various systems and structures that affect our lives.

REFERENCES

- Allen, A. (2011). *Unpopular Privacy: What Must We Hide?* Oxford University Press.
- Anglim, C., Kirtley, J. E., & Nobahar, G. (Eds.). (2015). *Privacy Rights in the Digital Age*. Grey House Publishing.
- Bell, D. (2014). What Is liberalism? *Political Theory*, 42(6), 682–715.
- Biletzki, A., & Matar, A. (2023). Ludwig Wittgenstein. *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition), E. N. Zalta & U. Nodelman (Eds.), forthcoming, <https://plato.stanford.edu/archives/fall2023/entries/wittgenstein/>.
- Brandeis, L., & Warren, S. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220.
- Cappelen, H. (2018). *Fixing Language: An Essay on Conceptual Engineering*. Oxford University Press.
- Chalmers, D. (2020). What Is Conceptual Engineering and What Should It Be? *Inquiry*, 1–18.
- Cooper, J. M. (Ed.). (1997). *Plato: Complete Works*. Hackett.
- DeCew, J. (2015). The Feminist Critique of Privacy: Past Arguments and New Social Understandings. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 85–103). Cambridge University Press. <https://doi.org/10.1017/CBO9781107280557.006>
- DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition). <https://plato.stanford.edu/archives/spr2018/entries/privacy/>
- Embler, J. A. (2015a). Cross-Cultural Perspectives on Privacy. In Anglim, C., Kirtley, J. E., & Nobahar, G. (Eds.). *Privacy Rights in the Digital Age* (pp. xxvii–xxxiv). Grey House Publishing.

- Embler, J. A. (2015b). Philosophical Basis of Privacy. In C. Anglim, J. E. Kirtley, & G. Nobahar (Eds.), *Privacy Rights in the Digital Age* (pp. 404–411). Grey House Publishing.
- Gentilo, R., & Santana, R. (2023, May 15). *TSA Is Testing Facial Recognition at More Airports, Raising Privacy Concerns*. AP News. <https://apnews.com/article/facial-recognition-airport-screening-tsa-d8b6397c02afe16602c8d34409d1451f>
- Hume, D. (2000). *A Treatise of Human Nature* (D. F. Norton & M. J. Norton, Eds.). Oxford University Press.
- Landes, J. B. (1998). *Feminism, the Public and the Private*. Oxford University Press.
- Lever, A. (2012). *On Privacy*. Routledge.
- Lever, A. (2015a). Democracy, Privacy and Security. In A. Moore (Ed.), *Privacy, Security, Accountability: Ethics, Law and Policy* (pp. 101–116). Rowman & Littlefield.
- Lever, A. (2015b). Privacy, Democracy and Freedom of Expression. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 162–180). Cambridge University Press. <https://doi.org/10.1017/CBO9781107280557.010>
- Lord, C. (Ed.). (2013). *Aristotle's Politics*. University of Chicago Press.
- MacKinnon, C. A. (1989). *Toward a Feminist Theory of the State*. Harvard University Press.
- Macleod, A. (2018). Privacy: Concept, Value, Right? In M. Navin & A. Cudd (Eds.), *Core Concepts and Contemporary Issues in Privacy*. Springer Verlag.
- Nguyen, C. T. (2022). Transparency Is Surveillance. *Philosophy and Phenomenological Research*, 105(2), 331–361.
- Rachels, J. (1975). Why Privacy Is Important. *Philosophy and Public Affairs*, 4, 323–333.
- Rea, M. (2022). The Metaphysics of the Narrative Self. *Journal of the American Philosophical Association*, 8(4), 586–603.
- Regan, P. (1995). *Legislating Privacy*. University of North Carolina Press.
- Reiman, J. H. (1976). Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 6(1), 26–44. <http://www.jstor.org/stable/2265060>
- Shontell, A. (2013, October 11). Mark Zuckerberg Just Spent More Than \$30 Million Buying 4 Neighboring Houses for Privacy. *Business Insider*. Retrieved August 21, 2023, from <https://www.businessinsider.com/mark-zuckerberg-buys-4-homes-for-privacy-2013-10>
- Thomson, J. J. (1975). The Right to Privacy. *Philosophical Dimensions of Privacy*, 272–289. <https://doi.org/10.1017/cbo9780511625138.012>
- Westin, A. F. (1967). *Privacy and freedom* (1st edition). Atheneum.
- Williams, P. J. (1991). *The Alchemy of Race and Rights*. Harvard University Press.

- Wilson, C. (2019). *How to Be an Epicurean: The Ancient Art of Living Well.* HarperCollins.
- Wittgenstein, L. (1953). *Philosophical Investigations* (G. E. M. Anscombe & R. Rhees, Eds. and G. E. M. Anscombe, Trans.). Blackwell.
- Young, I. M. (2004). A Room of One's Own: Old Age, Extended Care, and Privacy. In B. Rössler (Ed.), *Privacies: Philosophical Evaluations*. Stanford University Press.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 3

What's So Special About Private Parts? How Anthropology Questions the Public–Private Dichotomy

Simon Hawkins

INTRODUCTION

In so much of the conversation about privacy, people take the value and nature of privacy for granted. Of course, everyone wants privacy. Of course, privacy is fundamental to a well-functioning and just society. Indeed, the meaning of privacy appears so obvious that there often seems little need to define it. It is a simple term that we all use and understand. And yet, as is often the case with self-evident terms, the concept is trickier than it appears. The general definitions do not hold up terribly well. The standard dictionary definitions tend to emphasize being alone, being free from observation, or keeping personal information confidential. That sounds reasonable on its face, but upon reflection, there are far too many exceptions. One can certainly carve out a private moment even in a crowded or observed setting. Defining privacy in terms of personal

S. Hawkins (✉)

University of Arkansas at Little Rock, Little Rock, AR, USA

e-mail: sxhawkins@ualr.edu

information is still less useful, as it rests on a tautology. What constitutes personal information is that which we desire to keep private. Further complicating any definition is the fact that conceptions of privacy vary enormously from group to group, person to person, or even setting to setting.

The point here is not to undermine the idea of privacy so much as to demonstrate that the concept exists within social contexts rather than on an objective scale. Privacy is a shifting—not fixed—attribute. Under the right conditions, the public metamorphoses into the private and the private translates into the public. Beyond this, our very experience of privacy is itself cultural, and as such, privacy inhabits the socio-economic structure of our society. While some of the chapters in this book celebrate the liberatory power of privacy, privacy can also play a role in the oppression of marginalized groups. The anthropological examinations of privacy draw on the experiences of various groups of people in other times and places to question assumptions about the presumed nature, value, and ubiquity of privacy.

PUBLIC/PRIVATE DICHOTOMIES OF THE HUMAN BODY

The starting point for this discussion must be the lack of any inherent quality of privateness found in any act or object. To lead with the cliched example, in the contemporary US, one's body is a symbol of privacy. To intrude upon someone when they were clad only in their underwear would be a gross violation of their privacy, yet at beaches and pools that standard disappears. One can go further, and discuss World Naked Bike Ride Day, in which hundreds of naked cyclists ride en masse through the streets of major cities like London (Fig. 3.1).

Here, the private transmutes into the public. The body is not inherently private, but the social and individual contexts make it so...except when they make it more public. Even this simplifies the issue, because it assumes that with regard to privacy, all bodies are the same. In reality, age, sex, race, size, and other factors all play a role in society's view of whether a body should be made public or kept private. One could go further still along the contemporary scale of privacy and discuss bodily elimination. So privatized are urination and defecation that modern houses have specific, lockable rooms for these activities, yet here too, this standard can be



Fig. 3.1 “World Naked Bike Ride” Protestors Piccadilly Circus, London
Athanasios Papadopoulos, Photographer Courtesy of Alamy

flipped. Long troughs for men’s urination exist in a variety of large institutions and military barracks at various times have had communal toilets grouped together without any partitions (Hartzler et al., 2014).

To demonstrate that privacy is not an inherent objective quality is not to question its importance or power, but to begin to explore how societies create and use the idea of privacy. The fact that privacy is so malleable is part of its power. It can be a force of liberation and a force of oppression. To understand these dynamics, it is necessary to understand how the concept operates, or rather, how the private and public function. Privacy does not exist by itself; it is always in a comparative dichotomy with the concept of public. We use this distinction to categorize information, activities, and space itself. We cannot discuss privacy by itself, as the very nature of what is considered private depends upon a contrast with what is deemed public.

Beyond this malleable nature of privacy within a society, the underlying principles that guide the distinction between private and public are culturally determined. Even a superficial experience with cultures different

from one's own yields different perspectives on privacy. Travel guides thrive on discussing these different expectations. Visitors are told that the French don't like questions about their lives (Thyebaut, 2018), that taking photos of women in Jordan is an invasion of privacy (Rough Guide), and that Americans "appreciate their privacy, especially when it comes to matters of money" (Penn State Harrisburg) and "can be very protective of their privacy and safety" (immihelp). But while this relativization is important, its explanatory power is limited. To simply say that the sense of privacy is determined by culture is to put it into a black box and avoids looking at the specific history of privacy within a community, the socio-economic forces that played a role in its development, and its intersection with other ideological dichotomies in the community.

PUBLIC/PRIVATE DICHOTOMIES OF SPACES

For example, the current particular character of the distinction between (private) home and (public) work in the US depends on the move from an agrarian society in which production was part of the home and both men and women were regarded as instrumental to economic production, to the physical separation of homes from wage earning workplaces and the association of men with work and women with home. This shift is itself linked to the rise of the suburbs and the creation of the home as a female space, a sanctuary of nature and serenity protected and buffered by a garden and a white picket fence. The workplace, by contrast, becomes masculine space, a constructed realm of rationality and competition. Clearly the conceptions of privacy stack with conceptions of gender, both of which are part of structural economic changes. Unsurprisingly, changes to understandings of gender roles have affected perceptions of privacy. The feminist slogan that "the personal is political" is based on the idea of making what had been considered private a subject of public debate. Domestic abuse had long been ignored because it was considered private, but increasing public outcry shifted that perspective (Kelly, 2003).

What these political struggles also illustrate is that while definitions of private versus public are socially determined, they are not universal within a society. Certainly, there is individual variation, but more importantly for social change, distinct groups within a society have different perspectives, which are in turn linked to their position within that society. The broad definitions of privacy support certain communities and hurt

others. The suburban American dream of the house with a white picket fence is not just connected to gender, but also to class and race. The rise of the suburbs in the US was closely linked to the white flight of middle-class residents fleeing the cities (Jackson, 1987). The sanctuary and refuge of the suburban home was white and middle class, presuming the economic resources for a stay-at-home mother. We may experience private and public realms viscerally, but those emotions are rooted in the structures of our society.

PUBLIC/PRIVATE DICHOTOMIES OF INFORMATION

At the risk of over simplifying, in the US, the distinction between public and private is based on the individual. The connection is so self-evident that the linkage appears inevitable, even natural. As this chapter will go on to illustrate, this naturalness is an illusion. Societies can create separate realms of private and public that focus on units other than the individual. If that is the case, then one must ask what drives the US prioritization of the individual in privacy. It was not ever thus. One of the most cherished private acts, the individual's right to cast a secret ballot, is of recent origin. Early attempts to move toward privacy in voting were condemned by an old guard who proclaimed that they would "make any nation a nation of scoundrels" (Lepore, 2012, p. 247). Not coincidentally the move to secret ballots grew in the mid-nineteenth century as the population expanded and industrial and economic development leapt forward. The values of the emerging populist democracy matched those of the emerging economy, privileging the sanctity of individual choice free from community interference. The free market depends on individual autonomy and selection as much as broad-based democracy does. One cannot separate US prioritization of free individual choice from the economic or political system. The specific forms that privacy takes are certainly cultural, but not random or arbitrary. They are connected to larger ideological and material forces.

PUBLIC/PRIVATE DICHOTOMIES PROVIDE MEANING TO SYMBOLIC ACTS

Because the categories of private and public are flexible, they can be a powerful tool for constructing and defining relationships or giving weight to a symbolic act. To return to the example of bodily elimination, grouping toilets together without dividers in a military barracks is not merely about efficiency. By making that most private act (in the contemporary US) shared with others, it breaks down the boundaries with those others. As much as the private act becomes public, so too does the public group of individuals become private. It creates a bond among them. As to the other example, the symbolic power of World Naked Bike Ride Day stemmed directly from the shock of exposing the private body in the public space. The ideological and political focus of the event was on reducing the reliance on fossil fuels, not something that is inherently linked to public nudity. The disruptive power of the mass violation of social privacy norms becomes linked to the massive changes needed for environmental protection. As with the previous example, this group activity becomes simultaneously public and private. Because it is a large group of people doing something together (and in this case, on public streets) it is public. However, for those viewing this from afar, it is still the inappropriate display of the private in a public setting. This ability for an act to be definable as both public and private is an underlying component of the dichotomy.

PRIVATE/PUBLIC DICHOTOMIES: AN EXAMPLE FROM EGYPT

In trying to understand privacy, however, one must examine the idea in other cultures. Because any individual's experience of privacy is quite visceral, it is easy to presume that it is natural and inherent. Looking at other cultural practices can shatter that sense of universality. It can also provide examples that better help individuals understand their own experiences through the various contrasts and similarities they find when engaging with the practices of people of different places and times. While it can be tempting to hop from one exotic example to another, any attempt to understand the structures of privacy must be rooted in their specific contexts. The parts can only be understood in relation to other parts.

The extended example below is taken from Farha Ghannam's (2002, 2013) ongoing research in a working-class neighborhood in Cairo, al-Zawiya al-Hamra. Its center is a series of large apartment blocks built in the late twentieth century as part of a modernization scheme by then President Anwar Sadat. The negotiation over private and public space and its shifting definition has been an ongoing theme for residents as they adapted to their new surroundings. Figure 3.2 shows an apartment complex in Cairo parallel to the one et al.-Zawiya.

On the face of it, life in al-Zawiya has a clear and strongly enforced distinction between private and public and this pattern would seem to match patterns in the US. Apartments are private and the streets are public, with that private domestic space coded as female and the streets and institutions beyond coded as male. There are even explicit markers of this status. Women must wear hijab, covering their hair, when they go out into those public spaces and must behave in a very constrained fashion. In the domestic spaces, however, there is far more freedom of behavior and clothing.

And yet, on a closer look, this firm binary distinction becomes shifting and unstable, defying easy expectations. The family unit drives the categorization of space and the activities housed there. All the members of a family (mothers, fathers, brothers, sisters, aunts, uncles, cousins) are judged by the actions of any member, giving all family members both a license and obligation to intervene and participate in the lives of other family members. This intrusion includes economic resources (money and labor), social resources (matchmaking, conflict resolution, networking), and moral resources (correcting poor behavior and extolling good behavior). It is effectively impossible for any given individual, male or female, to get married and become a functioning adult member of society without the active support of all their family. While individual actions matter a great deal, any individual will always be judged, for better or worse, by the reputation of their family in addition to their own actions and every individual will require the aid of their family.

This strong focus on family plays out in constructions of privacy, or more specifically, who is or is not included in private space and what are the boundaries between public and private realms. The domesticity of the home is the most private space, and yet to a US eye, there is extremely little privacy. Children of all ages may enter their parents' bedroom without knocking, unless of course, they are already there, as children typically sleep with their parents. The front door to the apartment is



Fig. 3.2 Apartment block, Cairo, Egypt Petr Svarc, Photographer Courtesy of Alamy

generally kept open, as to close it is an aggressively rude act to one's neighbors. When relations are good, it is common for neighbors to casually walk into the main room of each other's apartments unannounced. Indeed, with the constant possibility of visitors, whether next-door neighbors or more removed guests, women and men may observe the modest standards of dress when in their own main room.

To describe the home as inherently private clearly does not work, as it takes on both public and private qualities. This is not merely a question about the nature of space, but the relations of people. The realm of the private includes family and the realm of family has flexibility itself and can include close community members. If privacy centers around the individual in the US, in this community, the family is at the center. Anyone who must spend an extended period by themselves is to be pitied, and both men and women live with their parents until they move into a home with their spouse. The family is not simply an economic unit, but also an emotional one, and that status is woven into the standards of privacy in the home.

If the category of the home as private space is more complicated than it might first appear, so too is the category of the street as a public space. Buildings orient toward a central square, an open space that would seem to be the epitome of public, and yet the social norms regarding it and the immediately adjacent streets are more nuanced. Society generally frowns upon married women working outside the home, but many women may set up small stalls in these exterior spaces, selling small dry goods, prepared foods, and candies (Fig. 3.3).

The rules of decorum for young women in public are quite strict, with modesty always demanded. But at the wedding celebrations held in these courtyards (there is no other space large enough to accommodate these big events), the norms are quite different. Young women must display their beauty in their clothing, makeup, and dancing. This seemingly public space can lose its association with masculine formal restraint. Because long work hours and commuting times to work keep men out of the home for long stretches, women interact with the local public institutions, such as the school and the police. The use of the central square for a wedding, particularly getting the electricity needed for all the lights, generally violates the formal regulations, and it is the women who build the relations with the local authorities and provide the small bribes to get them to look the other way. The police are a quintessential public masculine institution, but the relationships with individuals who are responsible



Fig. 3.3 Scarfed woman selling sweets at the edge of the street, Egypt, Maadi, Cairo Blickwinkel, Photographer Courtesy of Alamy

for specific decisions could be seen as more private. Categorization is not merely unclear, it is shifting.

In short, just as the seemingly private nature of the home is much more complicated, so too is the public nature of the street. The flips and ambiguities are not arbitrary but stem from underlying social and economic structures. The central square simultaneously exists as a public space or an extension of the familial private space. A wedding celebration is a family event, regardless of its location, and therefore at least semi-private. The community itself takes on a nebulous quality. In this tightly packed urban environment where residents may have originally come from different neighborhoods, no one trusts all their neighbors, but at the same time, it is a community and is distinct from the more alien world beyond the boundaries of the neighborhood. Community can take on aspects of family, in which members support each other. This responsibility is most apparent in the norms for dealing with domestic conflicts.

If a community member hears a fight or a similar disturbance in a neighbor's home, they should intervene. Not only is intervention encouraged, but lack of getting involved is censured. A family will roundly condemn an individual who hears them fighting but does nothing. People are expected to be in each other's affairs.

If the descriptions above show how the categorization of private and public can flip depending on context, the distinctions between public and private standards and behavior remain strong. While the specific nature of the distinctions and contexts may be different from western perspectives, the basic underlying structure is similar. It would be easy to assume then, that the emotional experiences and desires associated with the private and public would also be similar.

PRIVACY CROSS-CULTURALLY: THE NOTION OF SOLITUDE

In the US, there is a strong belief in the individual's emotional need for privacy, that is, time spent alone. Indeed, it becomes hard to disentangle concepts of "private" and "privacy." In the working-class Cairene example, however, there is no such conflation. There is no cultural idea of time spent alone as desirable or positive. On the contrary, being alone is actively seen as unpleasant and even threatening. No one speaks of a desire to be alone and one who experiences it is to be pitied. This anxiety about solitude plays out in multiple forms in daily life, whether it be in organization of living space, or what is the appropriate and comfortable distance for standing next to someone. In my own research with salesmen at tourist oriented stalls in the medina of Tunis, the salesmen worked hard to understand the different perspectives on bodily separation among their customers (Hawkins, 2010). Their income depended on making customers feel comfortable, and they quickly learned that Americans preferred a much wider sphere of bodily separation than did Tunisians, with various European nationalities on a continuum between them. What could be seen as an act of general and polite friendliness in one culture could be seen as invasive and threatening in another. (Popular US culture branded those who violated these norms as "close talkers" and the internet is replete with guidance on how to deal them).

Using generalizations about US culture and privacy is at least partially misleading, given the incredible diversity within the country. The point is not so much to typify US culture (or Arab culture, for that matter) as to illustrate again that while an individual's emotional experiences may feel

so deeply rooted as to be inherent in the experiences themselves, this sense is often misleading. As a discipline anthropology holds that what we take to be natural and universal may well not be, and this is certainly the case for a desire for privacy. An underlying goal of anthropology is to show how behaviors and patterns that may seem exotic or foreign can be experienced as “normal” and common sensical while contrastingly revealing how “natural” behaviors are contingent and constructed. The experience of needing privacy can feel so central and powerful that it seems as if it must be inherent, almost biological. When popular culture in the US recognizes different experiences of privacy, it attributes them to innate characteristics of the individual. Being an introvert or extrovert is part of one’s identity. Self-help books and personality quizzes present these as essential realities that vary from person to person in a quasi-genetic manner. Focusing on differences as arising within each individual obscures the role of larger socio-cultural forces that foster different relations to the experiences and expectations of privacy.

WEAVING DICHOTOMIES TOGETHER

Given an essentializing dichotomy that portrays cultural categories as natural, it is unsurprising that much of the critiques of the assumed nature of private and public came from feminist scholars who were questioning essentialized visions of gender (Gavison, 2017; Landes, 2003; Pateman, 1989). That the dichotomous pair of public and private mapped so neatly onto the matching pair of male and female is no coincidence. Critics demonstrated the ideological nature of the construction of these categories and how they obscured understandings of cultural practices. Societal definitions of private and public affected how members of that society perceived activities within those areas. Because women were presumptively absent from public spaces, for example, the multiple instances of women who were present in these spaces were ignored or erased. To shift from Egypt to Lebanon, Joseph describes working-class women in Beirut forming complex visiting networks that established community norms, brokered access to social services and employment, and created a sense of community for men and women (1983). Such work would seem to be public, yet policy makers (and academics) have typically not seen them as such. The linked ideological pairs of gender and public/private supported each other, making them feel more natural.

This sense of obviousness and ubiquity obscured the existence of individuals and groups that did not “fit,” the so-called normal order. Erasing deviations from the norm masked the real complexity of these categories and behavioral patterns.

If the categories of public and private are shifting and multifaceted, gender is famously equally complex, affected by multiple variables such as class, education, race, age, and the position of the body in space. Linking these pairs not only naturalizes them by drawing on seemingly inherent qualities, but linkage also homogenizes them, smoothing the complexity away. This means not only ignoring the presence of people in places where they theoretically should not be, but also activities that are not in keeping with the presumed nature of the sphere. The home is the epitome of the private space, separate from the world of work, and yet it is also a workplace for nannies and cleaning services. The division of private and public depends upon a timeless vision of society which ignores the specific history of contemporary practices. Hughes describes how an economic move in twentieth-century Jordan from subsistence agriculture to wage labor pulled men out of the “household economics” while increasingly limiting women to a domestic sphere that was not connected to economic production (2021, p. 42). Prior to the shift, there was no meaningful distinction between home and work. However, after the shift, society viewed this new distinction as not only one of long standing, but as essentially traditional.

TRADITIONAL/MODERN DICHOTOMIES

The invocation of “tradition” in this instance is not incidental, as its binary relationship with “modernity” also maps onto the public/private, male/female dichotomies. Constructing the public realm as one of rationality, economic production, and efficiency links it to conceptions of modernity and masculinity. Conversely, the private world’s emphasis on emotions and nurturing with no regard for efficiency places it in opposition to modernity and in the realm of the feminine and traditional. As one starts clustering these spheres, the moral judgments of, and the presumed value systems within, them become more apparent. To label a sphere as private, feminine, and traditional is not an act of neutral description. It may be viewed positively or negatively, but it is always a moral evaluation. Thus, modernizing reform efforts place a particular emphasis on women, who are understood to be the most traditional, the most restricted to

the private realm, and the most in need of reform. This focus is a main-stay of western development projects (Abu-Lughod, 2002), but is in no way limited to them. Deeb describes Hezbollah activists in Lebanon who wanted to modernize Shi'a Islam and lead it away from tradition and ignorance. The activists placed particular importance on the role of women who were seen as the most traditional and the most backward, trapped in the private domestic world, "Especially for women, making piety visible has become an imperative, as public piety has become part of the normative model of morality" (Deeb, 2011, p. 36).

In this instance, public piety explicitly required using "rationality to understand the authenticated meanings of religious texts and practices" (Deeb, 2011, p. 35). The moral valance of tradition can just as easily be flipped, however. As Hodgson pointed out, women often "figure as repositories of 'tradition' and 'culture' in nationalist rhetoric," invoking conflicts over women's clothing in Afghanistan and the complicated debates over hijab in the Muslim world more generally (2001, p. 9). The same nation, indeed, the same person may both laud and condemn tradition. For example, the anti-colonial resistance leader Habib Bourguiba championed hijab as a symbol of Tunisian national identity, but when he became the first president of an independent Tunisia, he spoke out against hijab as one of the fetters of traditional religion that retarded modernization (Hawkins, 2011, p. 39). Viewed negatively, tradition and privacy can be an obstacle to progress, while viewed positively they preserve morals and purity.

Hijab itself is a perfect example of how a cultural act can be either public or private, depending on the framing context. In its shielding of a woman from the public gaze, hijab can be seen as a form of privacy that the wearer takes with her into the world (Gilsenan, 1990). Conversely, as a symbol of religious observance worn when among non-intimates, the hijab can also function as a meaningful public act. Indeed, in 2004 the French parliament passed a law banning ostentatious religious symbols in public schools, with hijab as the chief focus. It would be misleading to argue about which is the correct interpretation, as there are no objective criteria inherent in any act or space that mark it as private or public. One might argue that the reading of something as private or public is in the eye of the beholder, and that groups in power will simply define practices according to their own interests. On its face this makes some sense, as western male analysts certainly did classify the wearing of hijab as removing women from the public sphere in accord with stereotypes about

Muslim society (Gilsenan, 1990), and many would argue that the French government really was pushing to homogenize the Muslim population into French society. The shifting categorization of the hijab, however, was not simply made by outside observers. For differing female activists, both putting on hijab, or taking it off, were assertive public stances. Conversely, for hijab wearers, taking off the garment often marks a context as being private.

These flips and shifts abound. The focus on rationality and efficiency of modernity marks it as public and yet modernizing reformers often critique traditional cultural practices as lacking privacy. It is common to condemn the lack of defined spaces for specific activities, such as sleeping, cooking, and bathing. The construction of a modern public redefines what is private, prioritizing the privacy of the individual and separating activities into discrete (in both senses) spaces (Foucault, 1977). The reforms shift the basic unit of privacy from the family to the individual. The construction of a modern public sphere requires the construction of modernized private spaces where traditional values and practices can continue. The distinction between private and public is not a new one and changes over time. In western culture, the ancient Greeks focused a great deal of thought on the distinction between private and public realms, and while certain classical theories seem familiar today—the emphasis on the public realm being masculine and rational—others are less so. Toilets, for example, were communal, with no sense of elimination being a particularly private act. This is not simply to note again that diverse cultures have different understandings of private and public, although that is certainly true, but that these understandings point to larger structures of belief about the nature of society, the individual, and community and that the changing privacy standards reflect changes in those larger structures. A self-consciously modern focus on the distinction between private and public actively distinguishes itself from previous models. The “modern” Cairene apartments Ghannam describes were touted by the government as increasing physical and moral hygiene by creating separate areas for food preparation, sleeping, and washing, part of a long tradition of urban reformers throughout the world creating modern housing that would have proper privacy (2002, pp. 32–34). It is a standard strategy to demonstrate the inadequacy of housing by listing the large number of people sleeping together in a room.

The example of urban reform efforts also demonstrates how claims about privacy can be used to justify potentially oppressive practices. In

the US, the push for more modern housing with proper privacy adopted the comparatively benign name Urban Renewal, but this practice was sometimes more accurately referred to as Slum Clearance (Vale, 2013). Eliminating the neighborhoods of substandard housing moved an undesirable population of marginalized people out of downtown urban areas that were highly desirable to developers (Pattillo, 2010). Thousands of people were displaced, and communities broken apart, all in the name of helping the residents, bringing them into the “modern” world. Insisting on proper forms of privacy delegitimizes all other models. Those living in such conditions are portrayed as not merely suffering, but as less civilized. If one does not follow the appropriate standards for privacy, one is backward, traditional, not properly developed. This, in turn, is used to justify “reforming” them.

INVOKING PRIVACY TO DEFINE RELATIONSHIPS

Heretofore the chapter has discussed privacy regarding spaces, events, and objects, but it is equally a categorizer of people and relationships. Who is included in the private realm and who is not? Certain relationships are socially structured, so that family are part of the private realm (although how family is defined may vary immensely) and strangers are not. Privacy is not limited to intimates, however. Because it is a sign of trust, aspects of it may appear in professional or therapeutic settings. Thus, a work conversation might well be private, as might a therapy session. While the nature of these interactions would be importantly different—mutual sharing for friends, one-way sharing in therapeutic settings—they both are predicated upon participants having a shared sense of trust. The sharing of private information indicates something about the nature of the relationship and the attendant rights and responsibilities. Acquaintances do not share confidential information, but close friends do.

Beginning to include private details does not simply mark the transition from one phase to another, so much as it accomplishes it, or at least attempts to. If the offered private information is warmly accepted, it marks a change in the relationship, but not all such offers are taken up. Someone who too readily provides personal information is condemned as an “over-sharer.” Hearing these private details that symbolize intimacy can be extremely uncomfortable, leading the surprised recipient to complain that that is too much information, or just “TMI.” If an offer

of private personal information is successful, it must be met with reciprocity, maybe not in the moment, but at some later point. The trust and accompanying vulnerability must be shared. The sharing, or not sharing, of the ability to control the dissemination of information constructs one as an independent individual in western society. Unlike an adult, a child has little privacy, and the process of becoming an adult requires claiming privacy, hence the social cliché of a teen's insistence on privacy, with shut doors and sullen responses. It doesn't merely mark the transition to existence as an independent subject in society, it is part of creating it.

If the social intimacy of friendship requires reciprocal private sharing, it is because non-reciprocal sharing marks an imbalance of power and is found in formal therapeutic relationships, such as with a doctor or social worker. In these, the private information flows in one direction and is driven by the questions of the participant with power and socially recognized authority. While some of these relationships may be voluntary, the power imbalance can be formally coercive, as when state powers require engagement with a licensed medical/mental health professional. The unequal power distribution is so fundamental to the relationship that to move into a relationship of mutual friendship violates professional ethical standards. If a close friend must share details of their private life a therapist must not. Reciprocity would flatten the hierarchy.

Separating worlds into neatly defined categories is an ideological action, asserting a purity that does not exist. It is not simply the case that there is some leakage between the categories of private and public, that there is some gray area around the edges, but that there is a constant flow between them and that any space that is categorized in one way can be flipped to be categorized in the opposite manner. That such discrepancies and flow are ignored and unreported is not random. As Irvine and Gal discuss, erasure is a key tool in ideological construction (2000). That which does not fit the model is unseen, allowing the continued belief in the ideological structure. It is akin to a societal level confirmation bias, with observers at all levels ignoring examples that do not fit the model or explaining them away with a tortuous rationalization as to why those examples did not count. We believe in a steady, clear distinction between private and public that is inherent in contexts or activities themselves. If the idea that these deeply held and personal perceptions are not only contingent, but driven by ideological forces, is disturbing, still more so is the realization that these same forces can shift our categorizations and even our experiences.

Labeling a context or behavior as private or public is not so much descriptive as making a claim about that behavior and context, linking it to larger social patterns accepted as private or public (or challenging those patterns). It is, as Gal puts it, “making an argument about and in the world” (2002, p. 79). If there is no inherent quality of private or public, then in using the terms we are constantly (re)establishing what they are and are not. As mutually constitutive concepts, establishing one defines the other in opposition. But the process goes farther than this. Any given thing that is defined as private or public can itself be subdivided into private and public components. The classic house with a white picket fence is an icon of the private, but within that space, the front yard is public while the house itself is private. Within the house, the entrance hall is public, but the rest is private. Within the rest, the dining and living rooms are public, but the bedrooms are private. This pattern of self-similar repetition, in which a distinction can separate a group into a set of sub-groups, and then any of those sub-groups can be divided in the same way, and then any of those can be divided, and so on is fractal recursivity, a pattern that Irvine and Gal (2000) present as a crucial building block of ideology. Specifically, Gal (2002) argues that this is central to understanding the use of the dichotomy of private and public. Because anything contains within it the possibility of being labeled as public or private, applying one label or the other points to the attributes that are held to be relevant in the moment. In theoretical terms, these are “indexical signs that are always relative” (Gal, 2002, p. 80). That is, they point to a particular attribute, highlighting it as the relevant component in that instance, rather than some other attribute or component. Privacy or publicness only ever exists in comparison to something else. Relative to the house, the yard is public. Relative to the street it is private. We all invoke the markers of privacy or publicness to indicate what aspects of a relationship or interaction are relevant in any given instance. An open-door policy in an office is a statement of public availability, but for discussion about certain topics, the door will be closed, marking a change in categorization. Indeed, one participant or another may ask “is this a closed-door meeting or open?” What frame is being invoked?

The changing frames occur not only in individual instances, but also at the larger scale over time. Gal gives the example of women in East Central Europe before the end of the Cold War (2002). During that era women were grouped in the public realm of the communist state, which, when communism was rejected, could have discredited them. Reality,

however, was more complicated. Within the socialist state itself, women were associated with “redistributive and social support aspects” which were comparatively more private than some state functions, allowing them to distance themselves from the state. Men, by contrast, were linked not to all the private realm, but to the “anti-politics” that was occurring within the private realm (the more public aspect). The existing ideological frames could be used to change categorizations over time. Importantly, because the dichotomies themselves remain constant even as the referents change, they can create an illusion of continuity even through large social changes.

PATHS FORWARD

As noted above anthropology teaches us that not all cultures have a need for privacy. This extends further than simply saying that the desire for privacy is a cultural construct, as it implies that what is being desired (or not) in various cultures is the same thing, which is not true. Indeed, it is inadequate to state that diverse cultures have different standards for privacy. As this chapter has shown, the statement is true, but obscures the fact that within a culture anything can be categorized as private or public depending on the context. Focusing on the differences among cultures masks the differences within a culture. More importantly, these differences within a culture are not inconsistencies or slippages within an otherwise stable system, but rather, are the ideological underpinnings of the system itself. Assertions of privacy are always ideological and as such can well be liberatory, but also oppressive, hiding information that could challenge existing power structures. Information about an individual’s salary, for example has long been held in the US as a very private matter, but marginalized groups have challenged this stance, arguing that it allows organizations to pay individuals from those groups less than those from the dominant group. Reformers have pushed for regulations that would make this previously private information public, leveling the negotiating playing field. The concept of privacy is inextricably bound up with power, as it affects not just what information is available and circulated, but whose information. As the French theorist, Foucault (1977) noted, the institutional surveillance on the individual increases the farther that individual differs from the established norms. Those on the margins, who encounter the police and social services the most, have far less control over their privacy than those comfortably in the center.

The point about privacy is not simply that it is malleable and changing. Change does not just happen on its own, but change is the result of social forces. Privacy is not an independent quality that changes on its own; people modify it, shift it, and flip it. In this regard, privacy is no different from other aspects of culture, or indeed, culture itself. Cultures may superficially appear static, but a core component of anthropology is that all cultures are always changing and that the changes do not follow a straightforward or inevitable path. The changes to privacy do not follow a mechanistic or predetermined pattern but are emergent, resulting from complex interactions of internal and external forces, some the result of deliberate pushing from concerned groups (the shift away from seeing domestic violence as a private affair), some the unintended consequence of other changes (the presence of social media leading to more individuals sharing previously private information in public settings). Privacy (or the lack thereof) is not an end in and of itself but is a tool for ordering and making sense of society and the world. While a society's invocation of privacy is driven by values, there is not a specific correspondence between any value and privacy. One might argue that an emphasis on the value of individual freedom would link to privacy, but it can just as easily be flipped ideologically, so that for an individual to exercise their freedom, information must be publicly available. Rather, the forms that the distinctions between private and public take are driven by the sets of values within a society. In working to change definitions of private and public, activists are addressing those underlying values. Likewise, changing the values changes the understandings and experiences of privacy. Because of this linkage, examining privacy in any given context is a particularly useful path for illuminating underlying values and for making comparisons among different societies or groups within societies.

REFERENCES

- Abu-Lughod, L. (2002). Do Muslim Women Really Need Saving? Anthropological Reflections on Cultural Relativism and Its Others. *American Anthropologist*, 104, 783–790.
- Deeb, L. (2011). *An Enchanted Modern: Gender and Public Piety in Shi'i Lebanon*. Princeton University Press.
- Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Vintage Books.

- Gal, S. (2002). A Semiotics of the Public/Private Distinction. *Differences: A Journal of Feminist Cultural Studies*, 13, 77–95.
- Gavison, R. (2017). *Feminism and the Public/Private Distinction, Privacy* (pp. 217–261). Routledge.
- Khannam, F. (2002). *Remaking the Modern: Space, Relocation, and the Politics of Identity in a Global Cairo*. University of California Press.
- Khannam, F. (2013). *Live and Die Like a Man: Gender Dynamics in Urban Egypt*. Stanford University Press.
- Gilsenan, M. (1990). *Recognizing Islam: Religion and Society in the Modern Middle East*. Tauris.
- Hartzler, R. B., Walker, L. E., Gatewood, R., Grandine, K., Kuranda, K. M., Goodwin, R. C., Associates. (2014). *Leading the Way: The History of Air Force Civil Engineers, 1907–2012*. Department of the Air Force.
- Hawkins, S. (2010). Cosmopolitan Hagglers or Haggling Locals? Salesmen, Tourists, and Cosmopolitan Discourses in Tunis. *City & Society*, 22, 1–24.
- Hawkins, S. (2011). Who Wears Hijab with the President: Constructing a Modern Islam in Tunisia. *Journal of Religion in Africa*, 35–58.
- Hodgson, D. L. (2001). Introduction: Of Modernity/Modernities, Gender, and Ethnography. In *Gendered Modernities: Ethnographic Perspectives* (pp. 1–23). Springer.
- Hughes, G. F. (2021). *Kinship, Islam, and the Politics of Marriage in Jordan: Affection and Mercy*. Indiana University Press.
- immihelp. *A Guide to Social Etiquette in the U.S.*
- Irvine, J., & Gal, S. (2000). Language Ideology and Linguistic Differentiation. In P. Kroskrity (Ed.), *Regimes of Language: Ideologies, Politics, and Identities*. School of American Research Press.
- Jackson, K. T. (1987). *Crabgrass Frontier: The Suburbanization of the United States*. Oxford University Press.
- Joseph, S. (1983). Working-Class Women's Networks in a Sectarian State: A Political Paradox. *American Ethnologist*, 10, 1–22.
- Kelly, K. A. (2003). *Domestic Violence and the Politics of Privacy*. Cornell University Press.
- Landes, J. B. (2003). Further Thoughts on the Public/Private Distinction. *Journal of Women's History*, 15, 28–39.
- Lepore, J. (2012). *The Story of America: Essays on Origins*. Princeton University Press.
- Pateman, C. (1989). *The Disorder of Women: Democracy, Feminism, and Political Theory*. Stanford University Press.
- Pattillo, M. (2010). *Black on the Block: The Politics of Race and Class in the City*. University of Chicago Press.
- Penn State Harrisburg. *Guide to American Culture and Etiquette*.
- Rough Guide. *Culture and Etiquette in Jordan*.

- Thyebaut, E. (2018). *14 Rules You Should Follow in France So the Locals Don't Hate you.*
- Vale, L. J. (2013). *Purging the Poorest: Public Housing and the Design Politics of Twice-Cleared Communities*. University of Chicago Press.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



PART II

Technical Views of Privacy



CHAPTER 4

Privacy in the Digital Age: Navigating the Risks and Benefits of Cybersecurity Measures

Christopher Farnell, Philip Huff, and William Cox

INTRODUCTION

The discipline of cybersecurity is still in its infancy, which leads to different interpretations of common terminology and concepts. Before we can discuss privacy concerns in cybersecurity, one must define cybersecurity. Cybersecurity, in essence, is the protective actions taken to safeguard digital information and processes an organization deems necessary for its successful operations. In practice, cybersecurity professionals will use many techniques to reduce the risk of systems being compromised against all types of threats. Not only do cybersecurity practitioners need to protect against adversarial threats; but they also need to be concerned with natural disaster events. The range of threats and the sophistication of methods

C. Farnell (✉)
University of Arkansas, Fayetteville, AR, USA
e-mail: cfarnell@uark.edu

P. Huff · W. Cox
University of Arkansas at Little Rock, Little Rock, AR, USA

used to attack networks, called “attack vectors,” make this field change at an exponential rate. Merriam-Webster dictionary (2023) defines privacy as “the quality or state of being apart from company or observation.” In cyberspace, this state translates to being protected from observation over a digital connection. To refine further the definition of privacy relating to cybersecurity, privacy is keeping personal information safe from unauthorized disclosure, or someone’s network traffic protected from surveillance. Privacy concerns have become an essential element of cybersecurity due to the vast amount of information that has become available over the Internet.

A person’s privacy is hard to preserve over the Internet for many reasons. The Internet does not have predefined boundaries like those which are present in the real world. If someone were to drive from the United States to Canada, they would go through a border entry point, which in turn, lets them know that they are leaving the laws and regulations of the United States and will now be under the laws of the Canadian government. In cyberspace, a user’s network traffic may start in one country but may go through many countries before ending at its destination. A computer programming tool called “traceroute” can be used to show how network traffic flows over the Internet. For example, if someone in central Arkansas were to traceroute to the University of Arkansas at Little Rock’s website from their home network, they could get an output that starts on their home network router and traverses through many Internet Service Provider (ISP) networks, then through the university system’s network until it reaches the final location. Internet traffic does not take physical locations as a metric for data flow but deploys a variety of technologies like the speed of the network or the predefined path set by the telecommunication company. Furthermore, the website servers could be distributed around the world to reduce latency or to provide security from attacks. Every country has its ideas about its citizens’ rights to privacy and as such an individual’s traffic may be collected if the data flows through a country that is considered a surveillance state.

Another area of privacy concern is the preservation of Personally Identifiable Information (PII) collected by organizations. PII is any information that can be used to ascertain who a person is and any data about that individual. (See more information in Chapter 4 on PII.) Before the boom of the Internet, PII was collected primarily at physical access points, for example, showing a passport to board an airplane. Now public and

private entities have transitioned to a more online presence where applications, forms, and e-commerce can be accomplished. By doing this a person's information may be collected and stored on servers that have access to the Internet. This action complexifies the safeguarding of this data. Data breaches are occurring relatively regularly and according to an article in the *Healthcare Journal*, the number of people affected by reported hacking events has risen in the healthcare field from 15.3 million between 2005 through 2014 to 145.7 million between 2015 and 2019 (Seh et al., 2020). This trend does not seem to be slowing, especially as new technologies are connected to the Internet and requirements for personal information are still necessary. The need for cybersecurity is becoming more prevalent in the defense of privacy data.

BRIEF INTRODUCTION TO THE INTERNET OF THINGS (IoT)

As embedded systems become more feature-rich and cost-effective their integration into household appliances, smart consumer devices, and even the nation's critical infrastructure has become more prevalent. This increased integration provides users with unprecedented situational awareness but also creates a privacy concern that must be acknowledged and mitigated. For instance, power utilities can now collect power quality data across large geographic regions in real-time which allows them to balance generation resources more effectively and mitigate potential outage events before they cause an interruption in service to their customers. Field devices such as Real-Time Automation Controllers (RTACs), Protection Relays, Solar Inverters, Battery Energy Storage Systems (BESSs), and Phasor Measurement Units (PMUs) with integrated communication channels for monitoring and control are becoming more widespread. These devices transmit critical real-time information to grid operators which provides them with additional situational awareness as well as a means to resolve issues before they progress to a critical level. However, these devices also increase the overall attack surface and may be connected through insecure external networks. As such, the control layer that manages, monitors, and provides mitigations for these systems must be protected using state-of-the-art cybersecurity techniques. A bad actor could intercept this data and malform it to cause the service provider to take a non-optimal action. Bad actors, or companies, could also collect personal user data from connected smart devices or develop consumer patterns from internet-connected smart appliances such as thermostats,

refrigerators, or fitness trackers. One noteworthy incident, as reported by *Wired* in January 2018, involved American bases and soldiers' patrol patterns overseas being revealed due to military personnel's usage of fitness trackers while jogging and patrolling the perimeter of the bases (Hsu, 2018). It is important for users to fully review the terms of service and understand what data is being collected and how it will be used, stored, and in some cases, sold to third parties to develop customer profiles for targeted advertisements.

OVERVIEW OF COMMON ATTACK VECTORS

In this section, we discuss three common cyber-attack vectors, as well as effective mitigations: Denial of Service (DoS), Man in the Middle (MitM), and Spoofing Attacks.

A DoS attack can render a service unavailable either through a direct or indirect attack (see Fig. 4.1). It also refers to physical attacks on communication infrastructure, such as the cutting of wires or wireless jamming. DoS attacks typically send multiple requests in rapid succession to overload a server's ability to respond to any other requests. More advanced DoS attacks are executed using BotNets which consist of many previously compromised computers. These attacks are typically characterized as Distributed Denial of Service (DDoS) attacks and require more advanced tactics and coordination to execute. Typical mitigation for this attack vector is to install software that identifies multiple rapid requests from a single computer or network of computers and blocks any future request for a specified time.

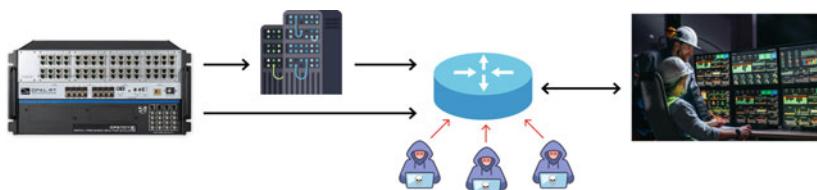


Fig. 4.1 Denial-of-Service attack diagram

(Image credits Iconfinder.com/Dmitry Mirolyubov, Maxicons, Z Studio, iStock.com/LeonidKos; Opal-RT Technologies; Stephan Green under CC BY-SA 3.0 Deed)

A MitM attack occurs when an external attacker is capable of intercepting, modifying, suppressing, or replaying network packets undetected by tricking two communication nodes into believing they are still communicating normally (see Fig. 4.2). This attack can enable the collection of PII data from a system or allow a bad actor to show corrupted information to operators and managers which would in turn make incorrect decisions based on the compromised data. A typical mitigation for this type of attack is to use up-to-date encryption and validation protocols. A Zero-Trust architecture is also an effective mitigation for this attack vector. Zero-Trust is a concept that involves taking additional measures to verify the authenticity of all devices and users on a network regardless of their physical location or privilege levels.

A spoofing is an attack where an illegitimate actor pretends to be a legitimate actor (see Fig. 4.3). There are many methods of spoofing in the cybersecurity domain. A bad actor could spoof a webserver, WiFi Access Point, or even a signal from the Global Positioning System (GPS). The act of causing Global Navigation Satellite System (GNSS) receivers to lock onto simulated or replayed satellite signals instead of real ones, effectively causing the receiver to locate itself at the wrong position and/or time. This class of attack is a major threat to PMU and synchrophasor systems, which are heavily reliant on time synchronization. To mitigate this class of attack, a zero-trust architecture along with a Public Key Infrastructure (PKI) is recommended. PKI is a framework that uses a combination of public and private keys to encrypt and verify data transmitted between users and servers. Regular site surveys are also recommended to help ensure rogue equipment may be identified and removed.

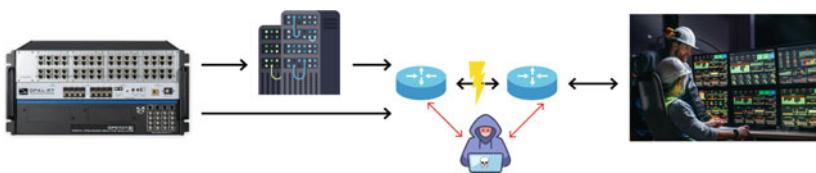


Fig. 4.2 Man-in-the-Middle attack diagram
(Image credits Iconfinder.com/Dmitry Mirolyubov, Maxicons, Z Studio, iStock.com/LeonidKos; Opal-RT Technologies; Stephan Green under CC BY-SA 3.0 Deed)

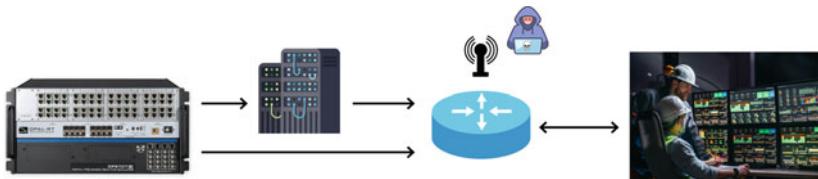


Fig. 4.3 Spoofing attack diagram

(Image credits Iconfinder.com/Dmitry Mirolyubov, Maxicons, Z Studio, iStock.com/LeonidKos; Opal-RT Technologies; Stephan Green under CC BY-SA 3.0 Deed)

THE DYNAMIC PROTECTIONS OF PRIVACY IN AN ORGANIZATION

The only true way to protect privacy in cyberspace is to use dynamic protective measures that adapt to the current threat landscape. Dynamic protection is a process of continuously reviewing and changing an entity's defensive controls. For an organization, this process can be through administrative or technical means. Organizations will need to build robust security plans that consider privacy.

User consent management. User consent is an essential aspect of users' privacy. User consent will need to adapt over time as the information needs of the organization change along with the techniques attackers will use to subvert security measures. User consent should be in the form of a contract between the individual and the organization and be displayed in any location being monitored, be it physical or digital. By getting consent from all users, everyone understands their rights within an organization, which allows users to make a conscious decision on what activities they will partake in while on the organization's network.

Access management. Another protection mechanism an organization can take is to apply access management to data. Access management is a way to regulate the data users can access. The concept is to develop markings for information based on importance to the organization or pertinent privacy laws. Several types of access management control can be implemented on a variety of factors. One access control model uses a person's role within an organization to approve or disapprove access to data. Another model may use predefined classification marking to control data like how the United States Federal Government assigns unclassified,

confidential, and secret classification markings to information. The organization will need to determine which access control model suits their needs.

Choosing the wrong access control model could have adverse effects on privacy. For instance, if an organization was protecting the social security numbers of their customers, only employees with a need to access this information should be able to view relevant details but not be able to modify this data. The model for this example should use a person's role or a set of predefined rules within the organization to determine the level of access. If a model that uses criticality of data was used, then people without a need to access that data may inadvertently have access rights.

Both user consent and access management are holistic approaches to privacy protection. What if PII data is needed by others but specifics about a person's identity need to be obfuscated? Think of medical research or census data. (See Chapter 10, "Healthcare Privacy in an Electronic Data Age" for a deeper dive on healthcare privacy.) Other people may need particular information like the age or location of an individual in a study, but they do not need the person's name or the social security number associated with the data. Here, anonymity techniques protect an individual's privacy but still allow the relevant data to be accessed by anyone.

ANONYMITY IN CYBERSECURITY

In the cybersecurity discipline, three main tenets are sought: confidentiality, availability, and integrity, known as the CIA model of cybersecurity. Privacy is a crucial aspect of trying to achieve the confidentiality of data. Maintaining confidentiality can be a daunting task that requires many techniques to ensure the privacy of data. One area of interest, anonymity, manipulates data in a way that obfuscates the identity of individuals but still allows others to view the applicable data. Keeping data private can be accomplished through a procedure known as k-anonymity.

K-anonymity: The idea behind K-anonymity has been around since 1986 when Tore Dalenius wrote a paper describing how to identify personal information from census data. The theory behind k-anonymity is that people's personal information can be anonymized, which preserves privacy but still allows pertinent data to be shared for scientific studies. For example, if a survey for the cure of cancer was conducted by a

major university, the data would undoubtedly contain personally identifiable information and cause privacy concerns for the subjects. K-anonymity allows for specific data to be shared while preserving the subject's privacy.

K-anonymity is accomplished by first categorizing information into three classes: non-identifier, identifier, or quasi-identifier (Samarati & Sweeney, 1998). Identifiable information is any data that would quickly ascertain a person's identity in the data. Non-identifiers are data that have no relation to a particular person unless directly correlated with an individual. Lastly, quasi-identifiable information is an attribute that can be associated with multiple people but when used with other quasi-identifiable information can eventually allow for the identification of an individual. Once the data is categorized, one can apply one of two methods to the data to anonymize the dataset.

The first method is to generalize the data. This strategy can be done by looking through all the data in a particular column and finding commonalities. If one category is age, the data can be grouped into five- or ten-year increments. The objective here would allow only pertinent information to be shown while preserving key characteristics of the subject. The other method is to sanitize the information from the released data. There will be times when the data cannot be generalized or is not needed for a different study or research. In these situations, the data should not be included in the released dataset. Examples of this are the person's name, street address, and even the person's religion. This type of information can be used to identify a person relatively easily.

The key feature behind k-anonymity is to have anonymity set to at least $k-1$, where k is a person's identifiable data (Samarati & Sweeney, 1998). This constraint means that there should be two or more matching records in each column. Table 4.1 shows how information should be presented if the dataset is to be considered k-anonymized.

When looking at the table, one can see all the characteristics of k-anonymity are applied. Each column is either sanitized with an asterisk or data is grouped. Each column has at least two rows with the same data to hide the identity of the person. K-anonymity is not impervious to attacks and should not be used for all datasets.

One area in which k-anonymity fails is with small group studies or small datasets. When there is not a substantial amount of data in each column, obscuring the identity of a person becomes difficult when trying to preserve the crucial pieces of information for a particular study. For

Table 4.1 An example of a k-anonymized dataset

<i>Name</i>	<i>Age</i>	<i>Sex</i>	<i>Religion</i>	<i>State</i>	<i>Medication</i>
*	18–24	M	*	Arkansas	Placebo
*	30–34	M	*	California	Anastrozole
*	18–24	F	*	Arkansas	Anastrozole
*	30–34	F	*	Delaware	Placebo
*	35–39	M	*	Vermont	Placebo
*	30–34	M	*	Delaware	Anastrozole
*	35–39	F	*	Vermont	Anastrozole
*	30–34	F	*	California	Anastrozole

example, if there are only ten subjects in a study then the commonalities are reduced, which can hinder the generalization of data and thus not lessen the amount of releasable information. When datasets are small, other data science methods for preserving identity would need to be used in conjunction with k-anonymity. The reality is preserving 100% data loss or privacy is very difficult and with the advancement of technology and the amount of data accessible by the public, privacy will only become harder to preserve.

Several techniques can be used to attack k-anonymity and must be understood to implement this privacy control. One method that can be used for re-identification is known as a linkage attack. This type of attack uses anonymized data along with a dataset that is known to the attacker. The attacker then looks for all overlapping information in the datasets and once enough overlap is found the identity of the individual can be ascertained. Now that structured and unstructured datasets are being sold and distributed regularly, this type of attack is becoming more and more effective. Furthermore, neural network models like OpenAI's GPT-4 and Google's BERT can expedite this process by taking available information and quickly isolating any common parameters. As artificial intelligence and publicly available information increase the protection of privacy will certainly decrease unless new measures are developed or defense in depth is followed.

THE PRIVACY CONTROL CATALOG IN NIST 800-53, REVISION 5

One sure way to make sure an organization is using defense in depth is to follow a well-developed and reviewed standard. Before we dive into one of these standards, let's discuss defense in depth.

Defense in depth. Defense in depth is nothing more than adding layers to cybersecurity defense. The quintessential analogy for defense in depth is picturing a castle. If the castle is open and there are no protections like locked doors, curtain walls, a moat, or security guards, then the castle can be easily conquered by adversaries. Defense in depth is where the castle is built on top of a mountain and there is a moat and drawbridge, archers on the high walls. Each layer of security added aids in the overall defense of the castle or, in our case, network security and ultimately privacy. Now that defense in depth has been explained, we can use a standard to help guide in implementing defense in depth also known as layered defense.

The National Institute of Standards and Technology (NIST) is an organization that develops standards for U.S. Federal Agencies. One such standard, NIST Special Publication 800-53 revision 5, published in 2020, outlines how to implement security and privacy controls within an organization. This publication was developed for the U.S. Federal government but can be applied to any organization. NIST SP 800-53r5 uses three categories of controls; administrative, technical, and physical, to guide privacy safeguards. Each category identifies how a control will be implemented.

Administrative controls. An administrative control is nontechnical in nature. This type of control is typically developed by cybersecurity professionals and management within an organization. Policies, training, and other types of plans encompass much of this control category. Administrative controls outline how an organization will operate and define the rules that employees must follow. This control category implements the procedures used in defending personal information or other privacy concerns. Management is heavily involved in this category of controls, which in turn allows for the enforcement of policies and procedures. The enforcement of these controls is regarded as the most critical aspect of this category. If administrative controls are not enforced, then users may decide to not follow the policies or procedures which puts data at risk of compromise.

Technical controls. Technical controls are applied to computer systems, networking equipment, or other information systems. As the

name implies, these controls are developed to harden equipment or add boundary protection to the organization's network. Technical controls are usually applied by skilled information technology professionals and overseen by cybersecurity practitioners. An administrative control would define the password policy of the organization, whereas technical control would apply the settings to the systems. Cybersecurity personnel would audit the control to verify that the control was implemented properly.

Physical controls. A physical control is a category that protects employees and data in the real world. This category of controls implements security through tangible means. A lock on a door would be considered a physical control. Another physical control would be an access control system that only allows authorized people into a particular room or area of the building. Physical controls are usually implemented by many divisions of an organization but can still be monitored by the cybersecurity team. Cybersecurity personnel monitor these controls because physical access to equipment can easily subvert any of the other control categories and allow attackers the ability to execute malicious code locally on the computer systems.

NIST SP 800-53r5 takes these three major categories and segments them into smaller areas, which allows the organization to focus on specific controls. If the key concern for the organization is privacy, the organization can quickly scan the control catalog and individually select the areas that are labeled as identifiable information or privacy. This streamlines and allows for prioritization of the implementation of each control. All the control categories rely on each other to preserve privacy within an organization.

The NIST control catalog is organized into twenty functional areas, where each group of controls is classified by requirements stemming from governmental requirements or organizational needs. Controls are developed to combat many attack vectors and as the landscape of attacks increases, NIST develops new controls and provides updates to SP 800-53 on a consistent basis. Controls are placed in alphabetical order and labeled with the abbreviation of the control area with a corresponding number; AC-1 for the Access Control area's first subsequent control. Furthermore, a description of the control is documented which streamlines the learning curve for the implementation of the control. Privacy-specific controls are easily located within the catalog due to NIST's approach to documenting controls.

PII Processing and Transparency, labeled as PT in the catalog, is one control group that is exclusively written for privacy. This control first outlines the need for the organization to create policies and procedures in relation to handling personal information, then aids the organization in finding and documenting the authority to process personal information. This control also outlines the need to allow only authorized personnel to access PII and explicitly restricts access to all others. Additionally, this control group has organizations detailing the purpose of collecting PII, getting consent from their users, and providing privacy statements when privacy is not provided on a system. This allows users some transparency on their privacy within the organization and allows them to make their own informed privacy decisions. SP 800-53 has additional privacy-related controls, which ultimately support the cybersecurity posture of the organization.

Individual's Privacy Relating to Cybersecurity (Three Ways to Protect Your Privacy)

Organizations have resources to provide security to their customers and employees including protecting privacy. What about the average person? How do they protect their privacy using cybersecurity principles and techniques? Using NIST standards may not be feasible for every person due to the lack of equipment, time, and effort gained from applying each control area. Privacy can be enhanced using cybersecurity best practices and using Free and Open-Source Software (FOSS).

1. **Use non-attributable networks.** One technique that can be very effective is the use of non-attributable networks. These networks are developed to obscure network traffic with the purpose of evading monitoring. One such network, The Onion Router (TOR) network, uses encryption, proxy devices, and tunneling techniques to make the user's network traffic ambiguous. One way to use TOR is to download and install the TOR web browser. When someone opens the TOR browser and surfs the Internet, the browser will set up an encrypted tunnel and pass traffic through multiple TOR relays. These relays are how an individual user's traffic becomes anonymous and virtually untraceable back to the original sending device. Once the traffic has gone through the TOR relays it will pass through an exit node and send the traffic back to the public Internet. Using

TOR will give some privacy on the Internet but as with anything in cyberspace, one method is not enough to give full anonymity.

2. **Use a privacy-specific Operating System (OS).** Another way to add layers to privacy on the web is to use a privacy-specific operating system (OS) like the Debian Linux-based Tails OS. When one uses Apple's MacOS or Microsoft's Windows, network traffic and browsing history can become compromised thus lessening one's privacy on the web. There are a few OSs that were developed with privacy as the primary purpose. Everything users do on an operating system leaves a trace on their hard drive. Digital Forensic tools can be used to look through each cluster on hard drives and find files that have previously been deleted from computers. This process stems from the fact that operating systems do not typically delete data. When one deletes a piece of data, the operating system just marks that is available to write on again. This is where privacy operating systems come in. These operating systems will run from a disk or USB drive and operate 100 percent in memory without writing anything to the actual hard drive. Once users reboot their computers, all traces of the operating system disappear. Only this process grants its users a much-needed layer of privacy protection, but the method must be used as prescribed by the vendor and proven best practices.
3. **Use social behaviors.** The last cybersecurity defensive technique in this category is not technical in nature. If an individual uses an anonymizing network and privacy-related operating systems, she or he may also want to utilize social behaviors to preserve privacy. One tactic would be to have many online personas and not log into systems that are associated with user accounts. Think about it this way; a user goes through all the trouble to obfuscate traffic and make it untraceable but then they log into social media accounts. Game over, they just compromised their privacy by associating the login with the network traffic. Never do anything that would trace the traffic back to the originator. Create a few online personalities. Users from the United Kingdom should deploy TOR and only surf traffic with .com and not.uk domains. This results from the fact that .com is generic and can be attributed around the world whereas .uk domains are specific to the United Kingdom. Moreover, one should never use a typical web browser at the same time they are using the TOR browser. By doing this an individual's

traffic goes over the non-attributed network and can be traced back through the anonymizing network to the original sender by looking at the anonymized traffic. When it comes to preserving privacy in cyberspace, cybersecurity practices can aid in the overall achievement of confidentiality for the average person.

CONCLUSIONS

Cybersecurity and privacy in the digital age are closely coupled topics. As more advanced protections and protocols are developed to maintain the confidentiality and overall data security of users, bad actors are simultaneously finding new ways to circumvent or compromise these protections. Protecting user privacy is everyone's responsibility. It is important for organizations charged with safeguarding PII to follow nationally recognized best practices, such as those outlined in NIST SP 800-53r5, in order to protect their customers' information. Individuals should also take an active role in managing the way companies and organizations collect, use, share, and sell their data by reviewing and understanding various terms and conditions presented to them. Additionally, users should adopt best practices to limit their exposure while navigating online, using IoT devices in their homes and offices, and sharing information with organizations. Researchers and organizations that have a need to share user data with affiliates and partners should investigate methods such as K-Anonymity and other methods to obfuscate personal information. Connected devices are becoming more prolific and companies will continue to collect, process, and utilize personal information for activities such as targeted advertisements and tailored user experiences. While these activities can help improve situational awareness and increase overall user experiences, users should take an active role in how their personal data is collected and used.

REFERENCES

- Dalenius, T. (1986). Finding a Needle in a Haystack or Identifying Anonymous Census Records. *Journal of Official Statistics*, 2(3), 329–336.
- Hsu, J. (2018). *The Strava Heat Map and the End of Secrets*, *Wired*. Retrieved August 22, 2023, from <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/>

- NIST Special Publication 800-53 revision 5. (2020). Retrieved August 22, 2023, from <https://doi.org/10.6028/NIST.SP.800-53r5>
- OPAL-RT Cybersecurity Overview. Retrieved August 22, 2023, from <https://www.opal-rt.com/cybersecurity-overview/>
- Privacy. (2023). Retrieved August 22, 2023, from <https://www.merriam-webster.com/dictionary/privacy>
- Samarati, P., & Sweeney, L. (1998). Protecting Privacy When Disclosing Information: K-anonymity and Its Enforcement Through Generalization and Suppression.
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8(2), 133.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 5

Data Governance, Privacy, and Ethics

Karl D. Schubert and David Barrett

INTRODUCTION

With the ever-increasing focus on artificial intelligence, exponential growth of generated data from private, public, and government sources (IDC & Statista, 2023) and the increase in the number of data generating devices, such as smart devices, wearable devices, and the everyday used and seen sensor devices around us (Greaton, 2019). Understanding data governance, privacy, and ethics surrounding the availability and use of data is more important than ever. Every day, new data breaches on individuals and organizations become known. Every day, new uses for data are envisioned and the ethical considerations around collection, storage, and use of these data are yet to be clearly thought out. The need for data governance to protect privacy and ensuring the ethical use of data is clear and there are many challenges to effectively define and implement effective data governance policies. And these must be implemented through legal and regulatory frameworks to be effective and enforceable. In this chapter, we will examine these topics and more related to data governance, privacy, and ethics.

K. D. Schubert (✉) · D. Barrett
University of Arkansas, Fayetteville, AR, USA
e-mail: schubert@uark.edu

Looking at data governance, privacy, and ethics from a data science point of view, understanding these is critically important. Governance is the purview of organizations in ensuring and insuring their data in all aspects. Privacy is the purview of the individual about their data and the data about them. Ethics is the purview of both the individual and organizations. Data privacy and ethics need to be integrated into data governance and be a real part of the organization's being. It is important that data science policies, practices, organizations, and people ensure the moral behavior of all to ensure ethical use of data and to ensure privacy.

THE IMPORTANCE OF DATA GOVERNANCE, PRIVACY, AND ETHICS IN TODAY'S WORLD

Much has been written about data governance, privacy, and ethics over the past several years. In fact, those terms have been used interchangeably in the popular press. However, they are not interchangeable and beginning with definitions of each will be helpful.

Data Governance. “Data governance is the specification of decision rights and an accountability framework to ensure the appropriate behavior in the valuation, creation, consumption and control of data and analytics.” (Gartner, 2023)

Data Privacy. “Data privacy is focused on the use and governance of personal data—things like putting policies in place to ensure that consumers’ personal information is being collected, shared and used in appropriate ways.” (IAAP, 2023)

Data Ethics. “...the norms of behavior that promote appropriate judgments and accountability when acquiring, managing, or using data, with the goals of protecting civil liberties, minimizing risks to individuals and society, and maximizing the public good.” (U.S. General Services Administration, n.d.)

While they are different, they are related and the three together are what provide “good hygiene” for data stewardship.

Data governance is rarely seen by the public or outside organizations. In fact, many do not even know it exists and, as a result, even organizations and those in organizations who *should* be designing and implementing data governance solutions have either yet to start or are at the very beginning of their journey. For example, a systematic literature review of the role of ethics in big data (Roche & Jamal, 2021) briefly

touches on data governance in the context of data ethics: “The question of using data ethically is being retrospectively applied to big data already in use, and is often considered alongside other data issues such as data governance, cyber security and data privacy.”

The emergence of the COVID-19 pandemic is widely recognized as an international crisis and in “crisis mode” decisions are made that are oftentimes expedient and the questions of data governance, data privacy, and data ethics shift from “are we doing the right thing” to “are we compliant.” As Yallop and Aliasghar (2020) observe from Yallop and Seraphin (2020), “...data governance frameworks need to expand from ‘solely compliance-based frameworks to inclusion of privacy and ethics solutions for an equitable and ethical exchange of data and information.’”

At this point, it would be reasonable to ask if these are addressed in the General Data Protection Regulation (GDPR). In fact, it does not explicitly. It does have several sections on processing personal data and the responsibility of those who “control” data, but it does not specifically address data governance. There are emerging internationally recognized guidelines for data governance such as ISO 38500 - International Standard for Corporate Governance of IT | IT Governance USA and ISO/IEC TS 38505-3:2021—Information technology—Governance of data—Part 3: Guidelines for data classification. There are even certifications available (Data Governance Certification: A Guide to the Top Certifications in 2023 (thedatagov.com)) from the Data Management Association (DAMA), the Association for Information and Image Management (AIIM), Project Management Institute (PMI), and the Data Governance Institute (DGI). Many of these are new and not widely subscribed, though this can be expected to change over the next 5–10 years as the realization of the importance of doing so grows.

For a concrete example of what, how, and why of data governance, consider a multinational corporation that collects data on customers who purchase their varied products in varied locations. Given language differences, currency differences, or the different practices within their locations, there are numerous occasions for inconsistency in databases. Processing of financial data may be compromised by inconsistency in noting currency values. If pounds and dollars are confused, for instance, analysts will inevitably draw misleading economic conclusions. If there are different names for the same products, owing to simple language differences from one store location to the other, attempts to draw insights about those products will be more difficult. Attempts to aggregate data

may also be complicated by varied data collection methods. If one store collects information about customers or transactions in a particular kind of format, while another store collects slightly different information about customers or transactions in still another kind of format, it will be difficult to combine that data and use it as evidence for better business decision-making. *What* data governance is partially about is “deciding on how to decide” about concerns like these in the collection and use of data.

But, of course, data governance is not only about the efficient business use and construction of databases. It is also about the oversight of the ethical dimensions of data use. What are examples of these dimensions and *why* is data governance concerned with them? Consider, again, the multinational corporation. Its analysts have mined its exceptionally large database and discovered various conclusions about its customers which are not readily evident from basic customer information. Suppose the analysts have discovered, based on purchase information, that it is possible to predict the credit score of customers to a high degree of accuracy. Clearly, this predictive ability raises questions about whether it is ethically permissible to make these predictions, use them for marketing purposes, share them with other businesses, and especially sell the predictive information to other businesses. Customers may not even have consented to the collection of data on which the inference depends, much less consented to the collection/storage of that credit information. Note also that there isn’t merely the loss of control over sensitive information that is at stake. The customers also stand to lose autonomy over their decision-making and how they conduct their personal relationships. The potential for others to know their credit score, not only financial institutions but also their friends, will alter the customers’ range of behavioral options and the landscape of those relationships. These changes are of self-evident moral significance. They are the reasons why data governance is not only about rules that affect the economic or structural properties of data gathering and analysis.

The *how* of data governance is the set of rules and accepted practices that oversee that gathering and analysis. In the context of ethics, these rules and practices are “data privacy.” Extending the example, the corporation will develop policies that balance the concerns of the relevant stakeholders. If there were some way that such credit score prediction could be simultaneously profitable for the corporation and beneficial to their customers—if, for instance, they were better able to offer useful financial services to customers by predicting those scores—then rules

would spring up about how to store the credit data safely, whether and how it can be shared with others, how to explain to customers what exact information is recorded, how it is used, and perhaps also whether they would like to opt out of its collection.

THE IMPACT OF DATA BREACHES ON INDIVIDUALS AND ORGANIZATIONS

Data breaches have been happening long before the advent of computers and data stores. For example, simple reading or copying the carbon copies of credit and debit card slips was common early on. Those impacts on individuals were originally limited in the United States by law to \$50 per misuse by someone else of the credit or debit card. Eventually, for competitive reasons, even the \$50 was waived if the individual reported the breach in a timely manner. That, however, does not reduce the impact on the credit or debit card issuer or the organization from whom goods and/or services were purchased.

The National Association of Attorneys General (National Association of Attorneys General, n.d.), have defined a data breach as

...the unlawful and unauthorized acquisition of personal information that compromises security, confidentiality, or integrity of personal information. What is considered personal information depends on state law but typically includes an individual's first name (or initial) and last name plus one or more of the following:

- Social Security Number
- Driver's license number or state-issued ID card number
- Account number, credit, or debit card number, combined with any security code, access code, PIN or password needed to access an account

Additional categories may include:

- Medical history or health information
- Biometric information
- Email address and password
- Tax ID number.

The “what” is important, and so is understanding the “how.” A recent security foundation report (IFF Lab, n.d.) identified seven major causes of data breaches:

1. Human Error. These include sending sensitive information to an incorrect email, leaving your computer or smart device unattended or unlocked, or leaving paperwork with confidential information open and available to others. This is one of the more common causes of data breach.
2. Physical Theft/Loss of Device. These are generally either negligence or a well-planned malicious event by others.
3. Phishing. These are malicious links provided on a website or email for users to fall prey to provide sensitive information to the attacker.
4. Stolen/Weak Credentials. Too many users have very simple passwords that are either easy to guess or easy to “crack.”
5. Application/Operating System Vulnerabilities. Many users have pirated software they use which oftentimes have vulnerabilities that enable hackers to capture sensitive information. Also, out-of-date browsers, applications, and operating systems also provide opportunities through vulnerabilities fixed in later and updated releases.
6. Malicious Cyber Attacks. These are among the most damaging to individuals and organizations and include denial of service (DoS) attacks and the use of ransomware.
7. Social Engineering. These are the use of deception to convince individuals to provide confidential or personal information using psychology rather than software programming. Oftentimes, these are designed to entice someone to provide data in exchange for some exciting reward or other offer.

Now that we have looked at the “how,” time to look at the effects.

Recently, IBM Security (IBM Security, 2022) studied 550 organizations impacted by data breaches from March 2021 through March 2022, across 17 countries and 17 different industries, and interviews with 3,600 individuals from organizations impacted by data breaches to understand the costs of data breaches. The impacts are significant:

- Organizations studied have had more than one data breach: 83%

- Organizations' breaches led to increases in prices passed on to customers: 60%
- Breaches occurred because of a compromise at a business partner: 19%
- Breaches that were cloud-based: 45%
- Average cost of a data breach: \$4.35M (USD)
- Average cost of a data breach in the United States: \$9.44M (USD)
- Average cost savings, fully deployed security AI & automation: \$3.05M (USD)
- Average cost of ransomware attack, excluding cost of the ransom: \$4.54M (USD)
- Frequency of breaches caused by stolen or compromised credentials: 19%
- Average difference in cost with remote vs. local work: \$1.00M (USD)
- Consecutive years the healthcare industry highest cost of breach: 12

A recent example is a data breach at Johns Hopkins (Higher Ed Dive, 2023), where it is alleged that “the health system failed to safeguard patients’ health information and provided insufficient details about stolen data....” The breach was through a third party in a file transfer by a ransomware group and is believed to have affected tens to hundreds of thousands of individuals. In the same week, HCA Healthcare (Health Care Dive, 2023) reported a data breach with personal information about approximately 11 million patients (hospitals and physicians offices) in 20 states. In the same article, federal reports were referenced identifying 385 million patient records exposed through data breaches from 2010 through 2022.

This is the “why” for caring about breaches at an organizational level. But why should one care about such breaches from an individual standpoint? To begin with the obvious, data breaches will cause emotional distress in the individuals whose personal information has been illegitimately accessed. The distress itself is intrinsically morally significant, but it also points to other harms that cause those feelings. For instance, stolen information affects one’s *dignity*. Depending on the type of information, a person’s reputation can be irrevocably tarnished. If the issue is, once again, about credit scores, one’s stature could easily be diminished in the eyes of those who access those numbers. The same would be true of a social media hack: information pried off these sites could easily affect

reputational standing. If a user's direct messages became known, they could contain information that person would never say to others—off-color jokes, vulgar ideas, vulgar language. If the hack was about health information, the consequences for dignity could run even deeper. Some health conditions could lead to stigmatization and subordination. If it were known that some carried sexually transmitted infections, or were diagnosed with a mental health disorder, they could be treated in such a way that they lose access to resources and opportunities because they are viewed as unworthy of them.

Another source of distress is the loss of *freedom*. Economically, data breaches can have large effects on individual freedom. If malicious actors obtain access to financial accounts, they can steal funds that leave the owners with far fewer economic options. Likewise, if health care information is breached, thieves might purchase prescription drugs that limit account owner's ability to care for themselves and others. The impacts on freedom can also extend beyond the economic realm. Suppose an academic institution suffers a data breach involving its records about applicants. Fraudsters can then muddy these records and cause issues about the status of applicants. Now the applicants' ability to gain admissions, which might represent important lifelong goals, is in jeopardy. Suppose a music studio suffers a data breach that makes available hours of work by its artists. If the work is plagiarized, artists' dreams of living a particular kind of life, in particular kinds of places, and having a large cultural impact, may be at an end.

Finally, there is the worry that one cannot live one's conception of the *good life* without privacy guarantees. When data breaches occur, they can affect relationships. Friendships, for instance, are built on intimacy, trust, and the willingness to confide information that would never be available to others. Data breaches could shatter the ability to maintain these bonds. In the health care situation, imagine that information about a mental health disorder becomes publicly available. The friend of the person who has the disorder might not want others to know that they support their friend with the disorder. This could cause a distancing in that relationship that undermines it altogether. Since relationships of these types relate to people's conceptions of what makes lives worth living, the distress of being a victim of a data breach is partly about this harm, too.

Of course, there are reasons why organizations should offer better data governance for individuals who *commit* data breaches, too. Those whose

data is stolen can bring civil cases against them and be awarded monetary compensation for the damages they suffer. There are also criminal penalties associated with data breaches that result in sizeable fines and even imprisonment. In the context of health care information, the Health Insurance Portability and Accountability Act (HIPAA) covers the laws and penalties associated with data breaches involving health information. Note that many organizations deal with such information and are not in the health care industry. IT or HR personnel, with no malevolent intentions, might have access to such information and would benefit from better data governance that automates HIPAA compliance.

THE ROLE OF DATA GOVERNANCE IN PROTECTING PRIVACY AND ENSURING ETHICAL USE OF DATA

Protecting privacy and ensuring ethical use of data is a significant role for data governance. Proper design and use of data governance frameworks include an understanding of data origin, how it has been and/or is being used, and the trustworthiness of the data. Data governance also plays a role in optimizing the value of data and usefulness of data while at the same time protecting privacy and ethical use.

Data governance is also important to ensure the appropriate privacy laws are understood and organizations are in compliance. Privacy laws are put into place to establish expectations to follow and consequences of non-compliance, willful negligence, breaches, and responsibilities (financial and other) and outcomes. These also point to the privacy policies published by organizations in the documentation and typically on their websites.

Data governance plays a role in establishing how data can be used ethically. This includes defining transparency in data collection, data storage, and what constitutes ethical use. Data governance frameworks include checks and balances to ensure the guidelines and controls for ethical use of data are followed. “Data ethics is at the top of the CEO agenda, as negligence may result in severe consequences such as reputational loss or business shutdown. To create an effective policy, companies need a formal program to ensure standards are upheld and evaluated regularly” (Janiszewska-Kiewra et al., 2020).

Figure 5.1 illustrates the “what” and “how” of data governance (adapted from Caserta, n.d.).

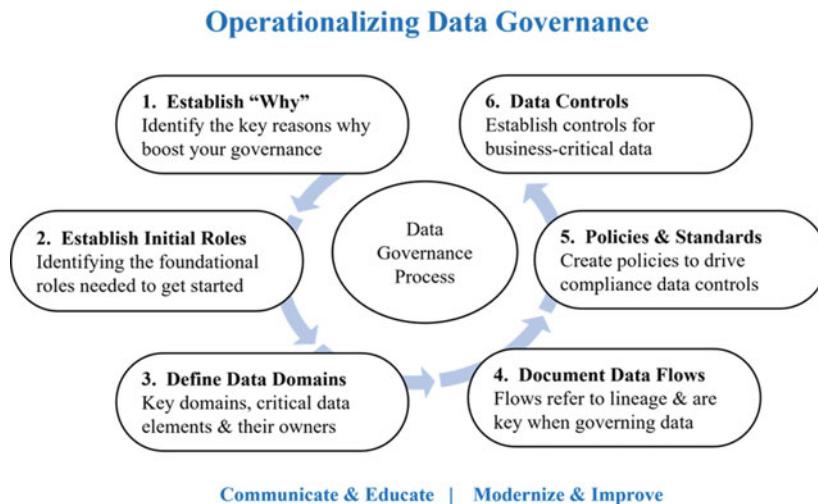


Fig. 5.1 Data governance (Adapted by authors from Caserta, n.d.)

Lack of adherence to a data governance process—or the complete lack of a data governance process—can have disastrous consequences for any organization and the individuals involved regardless of how they are involved.

Three examples of recent breakdowns or lack of adequate governance related to data breaches or exposure are illustrative:

1. SolarWinds: Third Party Infiltration
2. UpGuard: Misconfigured Software
3. Securitus: Misconfigured Data Access

In the SolarWinds case (Cyolo, 2020), a foreign country-backed hacker group was able to infiltrate the SolarWinds Orion Platform with malware. This is a software platform used by many Fortune 500 companies, the US government, and non-government organizations (NGOs) to monitor their IT systems. The proper use of data governance would have included (and subsequently does include) internal and external authentication of devices in every and all situations where they access systems, applications, and key assets. This is referred to as “zero trust” and as the term implies,

there is no trust and constant verification of identity is required and in this specific case, the network structure and assets would not have been visible to the malware. In this case, referring to Fig. 5.1, SolarWinds failed in operationalizing data governance in the areas of establishing initial roles (step 2), documenting data flows (step 4), establishing policies and standards (step 5), and establishing data controls (step 6).

In the UpGuard case (Fung, 2021), major corporations, federal and state governments, and other organizations (47+) were affected by a misconfigured setting in Microsoft Power Apps resulting in access to millions of pieces of personally identifiable data to the public internet for months. Examples of companies affected included American Airlines, the Maryland Department of Health, the New York Transportation Authority, J. B. Hunt, State of Indiana government, Ford Motor Company, and Microsoft itself. The 38+ million records breached included employee information, COVID-19 vaccination, and other related data, including Social Security numbers, phone numbers, date of birth, demographic information, addresses, and various employee events and memberships. This case is an example where checks and balances in understanding default security settings for software are needed. In this case, referring to Fig. 5.1, UpGuard failed in operationalizing data governance in the areas of establishing initial roles (step 2), documenting data roles (step 3), documenting data flows (step 4), establishing policies and standards (step 5), and establishing data controls (step 6).

In the Securitus case (Henriquez, 2022; Safety Detectives, 2023), 1.5 million files containing information on their employees and airport employees in the Latin American aviation industry were accessed. Information breached included photos of ID cards, full names and pictures of employees, occupations and national ID numbers, cameras used, GPS locations of the photos, and time and date of photos. Photos also included data of Securitus clients, airport employees, and other businesses. Misconfigured cloud data storage access allowed a breach of more than 3 TB (terabytes) of data in more than 1 million files. This could result in serious threats to airports, passengers, airlines, and airport personnel. Similarly to the previous example, checks and balances in understanding default security settings for software are needed. Higher security and less or no access by default should be the norm. In this case, referring to Fig. 5.1, Securitus failed in operationalizing data governance in the areas of establishing

initial roles (step 2), documenting data flows (step 4), establishing policies and standards (step 5), and establishing data controls (step 6), and documenting data roles (step 3).

An example of data ethics violations is the access by Cambridge Analytica to data mine Facebook data (Criddle, 2020; Federal Trade Commission, 2019a). Facebook (or, as it is now known, “Meta”) was sued by the Federal Trade Commission (FTC) for not protecting users’ personal data as the result of 87 million records of Facebook users being used for advertising during the US Presidential elections. “Facebook, Inc. [was ordered to] pay a record-breaking \$5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users’ privacy, to settle Federal Trade Commission charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information” (FTC, 2019a). The FTC went on to say that Facebook had a sustained history of using deceptive disclosures and settings to cause users to be lax in their privacy settings, thus making information available to Facebook and third-party applications and that Facebook knew that these data were being used inappropriately. They also, separately, acted against Cambridge Analytica for their harvesting of data (FTC, 2019b).

In the case of Facebook, the FTC imposed new, corporate-level mechanisms to ensure privacy protections. They established an independent privacy committee, composed of members of Facebook’s board of directors, who could only be removed from the board by a supermajority vote. The purpose was to strip CEO Mark Zuckerberg of total control over decisions that affect the privacy of the users of Facebook’s various subcompanies (Instagram, WhatsApp, Oculus VR, e.g.). The orders also require the appointment of compliance officers who are answerable only to that privacy committee and who must submit quarterly certifications demonstrating compliance with FTC privacy rules. Finally, the FTC also enhanced the powers of third-party assessors who, independently of the foregoing measures, test and verify Facebook’s privacy policies and who serve only at the direction of the FTC. So, while the previous examples involve systems-level, or software-level, governance structures, there are *corporation-level* data governance policies that can also provide further privacy safeguards. The Facebook example illustrates why it is important to establish initial roles (who heads what committees and who answers to whom) and how this establishment partly constitutes what it means

for “data governance” to ensure privacy controls. In this case, referring to Fig. 5.1, Facebook failed in all areas operationalizing data governance in the areas of establishing why data governance was necessary (step 2), establishing initial roles (step 2), documenting data roles (step 3), documenting data flows (step 4), establishing policies and standards (step 5), and establishing data controls (step 6).

THE CHALLENGES OF IMPLEMENTING EFFECTIVE DATA GOVERNANCE POLICIES

Even when there is consensus on the need for data governance, privacy, and ethical use of data, there are still many challenges ahead. There are challenges with identifying with the data, with the people who see themselves as owning the data, lack of agreement on who should lead data governance, and understanding the difference between managing and controlling the data. The greatest challenges are the lack of commitment by those who believe they own the data and lack of executive sponsorship to ensure governance becomes a reality.

In most companies, data have been created by many people, many departments, many divisions, and so on, and over time, so the proliferation of data has resulted in duplication, inconsistencies, uneven quality, and many “roll-your-own” (RYO) “applications” with untold numbers of interdependencies. Alongside this there is considerable selective knowledge of the data, the processes and transformations, and the meaning of results. Arriving at a collaborative agreement to implement effective data governance policies may well be seen by many as their losing control of their data and applications—forgetting, of course, that their organization owns the data and the applications, not the individual. Acceptance of the need and even requirement to create effective data governance can come from agreement that “(t)he primary goal of any data governance program is to deliver against the prioritized business objectives and unlock the value of your data across your organization” (IBM, 2022). From the start, data governance must keep business objectives in mind while creating realistic plans and defining measurable outcomes. These business objectives are far more than solely profit-oriented. They also recognize the custodianship responsibilities that come with their data. Once started, data governance is a journey, not a destination. To be successful, it will need to be implemented incrementally and iteratively with short-term successes in the direction of the long-term goals. Success requires

strong executive-level support, cross-functional collaboration, and visible and demonstrable results that positively affect the company, employees, customers, and more.

Data governance must include ethical considerations, which we will delve into next.

THE ETHICAL CONSIDERATIONS SURROUNDING THE COLLECTION, STORAGE, AND USE OF PERSONAL DATA

Many writers agree about specific harms having to do with privacy—like dignity and freedom, mentioned previously. But the more general work on the philosophy of privacy is much like any other area of philosophy: there is little agreement on what privacy is or what even should fall under the scope of privacy (Auxier et al., 2019; DeCew, 2018). A handy, if controversial, way of thinking about privacy is to divide it into the following four fields. One, privacy seems to be violated whenever your physical security is involuntarily threatened. This is why assault is harmful beyond the physical injuries involved. It is also why being the recipient of unwanted medical procedures would intuitively violate privacy. Second, privacy seems to be violated whenever some intimate, or personal, location is invaded in an unauthorized fashion. This is the sense in which a burglar who enters a house violates privacy, quite apart from the harms of any damage or theft of property. Third, privacy seems to be violated when the autonomy to make intimate, or personal, decisions is interfered with. This sense of privacy is closely aligned with laws about privacy. Many understand abortion laws, for instance, to be a matter of privacy. This is also the reason the recent Dobbs decision was immediately related to laws about same-sex marriage, access to contraception, and interracial marriage: in all cases there is the threat of interference with the freedom to make intimate decisions about how one's life goes (Goldhill, 2022). Fourth, finally, privacy seems to be violated when control over access to intimate, or personal, information is lost. This is, of course, the sense in which hacks of online databases raise privacy violation concerns, or the sense in which HIPPA seems like sensible privacy protection for health information.

It is tempting to think that data privacy would concern only the last, informational sense of privacy. But it is important to note that data privacy is at least tangentially connected to each of the other senses of privacy, too. Leaks of personal data from some data holder could include

home addresses. This makes it possible for those who illicitly access that information to invade actual locations, or, since it would be possible to pinpoint an individual, to threaten their physical security. With respect to the third sense of privacy, data privacy is much more related to it. Much of the legislation in the world (see the next section) is about automated information processing that could treat data subjects unfairly or discriminatorily. Unfairness and discrimination are important because they could limit people's freedom to make significant personal decisions. Financial institutions, for instance, could use automated means for deciding on loan offers. If the algorithm that makes the decision is trained on biased data, its output could reproduce that bias and have an evident impact on people's lives (Heaven, 2021; Klein, 2020).

Specifically owing to technological innovations involving data collection and processing, the ethical literature on privacy has changed significantly. In the past, privacy was seen as a matter of individuals being protected from the intrusion of society; it was seen as an individualistic good. This is related to the sense of privacy as resistance to autonomy interference. Whether or not one wants to have an abortion, for instance, is seen as a personal, individual decision which ought not be subject to societal or governmental pressures. But, in the current information age, many theorists have emphasized the societal goods that are fostered by privacy protections (Roessler & Mokrosinska, 2015). Even further, some theorists point out that today's technological advances render obsolete the old, individual-against-society understanding of privacy (Nissenbaum, 2010). That is, not only are there social goods promoted by privacy, but also that some privacy harms are collective harms.

To explain the former point, consider the simple fact that democracies protect privacy in voting. Without one's vote being expressed in privacy, it is not clear that a democracy could exist. Pressure being applied to one's voting is effectively the abandonment of allowing the conscience of people to hold political power. People are subject to many social pressures, from family, friends, business associates, and others. Any of these pressure points could sway voting decisions and effectively undermine democratic political participation. To the extent that democratic forms of government are socially worthwhile, privacy protections in the voting booth function as an extremely important social good. Privacy is not merely a trump card to play against society's wellbeing; it is a shield for that very wellbeing, too. In big data contexts, there are similar worries. The collection and processing of information about the voting public

allows microtargeted political persuasion (Dizikes, 2023). This is different from being in the voting booth watching someone vote, but it is a way of snooping on voters' behaviors and using the information gained to pressure their political decision-making. In the same way that privacy in the booth is an important social good, so, too, is data privacy.

To explain the latter point, consider that today's technology for data collection and analysis, particularly given how integrated so much of it is across public and private entities (think of consumer data, for instance), has created an environment where privacy protections exist only at the collective level. Where analysis of a small minority of users' personal data makes it possible to draw reliable inferences about data values of the majority of users, the lack of privacy concerns for the minority automatically destabilizes the privacy concerns of the majority. Social media users provide an obvious example of the community-based nature of privacy's value. If some are willing to share enough information, much can be learned about others who are not willing.

From a data governance perspective, there is much to consider. Though the mere collection of data may seem harmless enough, there are ethical worries that arise. The loss of control over sensitive information is unsettling for people in its own right. Think of losing a diary, even if it has thorough security mechanisms protecting it. Or think of how the knowledge that some others are tracking one's usage of the internet would be repressive, even if that information were never used for other objectives. It is, thus, quite common for data brokers to require the consent of persons before their data is gathered. There is further discussion in the section below, but many data companies also release details about exactly how personal data will be used and for what purposes. Consent and transparency are usually understood to be important barriers for data collection, and proper data governance would, where other business and societal needs do not clash, look to obtain that consent and be transparent to data subjects about what happens with their information.

More obviously, the storage of data is an important feature of data governance. Exacting security measures must be in place, and be routinely tested, to ensure a much greater range of harms do not occur. There are the same informational considerations as with collection; simply knowing that one's information is stored in a location one cannot control is worrying. But the disclosure of that information to the wrong parties, or its being illicitly accessed, raises many other ethical concerns. There is, of course, the repressive aspect of others accessing personal data. But

knowing location data could lead to trespassing harms and as noted earlier, even to physical harms. Think of a hack to an online dating website. Users' information being stolen could easily lead to stalking and physical confrontations.

Finally, the use of data is another key area of data governance. For still other ethical reasons, there must be guardrails in place to guarantee that data is used in appropriate ways. Consider, again, the possibility of automated decision-making. If the data processor does not fully understand the nature of the automated decision, they will not be able to assess the quality of the output. For financial information, or crime/security matters, such an inability could have severe consequences for data subjects. Requiring transparency in the use of data is thus also ethically important. Many data holders also consider selling (parts of) their databases to other entities. This creates many of the same ethical concerns that have been raised about informational, decisional, and physical forms of privacy, to say nothing of the physical harms that could come from personal information coming to be owned by the wrong party. Good data governance can avoid these problems by, for instance, informing data subjects about automation or third-party sharing of their information, or by allowing those subjects to opt out of various uses of their personal data.

THE LEGAL AND REGULATORY FRAMEWORKS GOVERNING DATA PRIVACY AND ETHICS

There are, of course, no universal regulatory frameworks that cover data privacy or mandate data governance. But there are nation-to-nation regulations and, within the United States (US), state-to-state regulations.

The most famous piece of law, mentioned above, is the European Union's *General Data Protection Regulation* (GDPR). It offers significant protections for data subjects, including rights to transparency, access, rectification, erasure, and even the right to object to certain forms of processing. Outside of compliance with the rights of data subjects, the GDPR also requires data "controllers" and "processors" to protect their data, pseudonymize it, keep records of processing, and even to appoint Data Protection Officers whose job is to ensure compliance with GDPR instructions.

From the perspective of privacy, the rights of data subjects in the GDPR cover plenty of ground. Many understand privacy to concern a

“right to be forgotten.” That is, they maintain that an important part of privacy is the ability to have one’s past (decisions, actions, events) remain overlooked. The GDPR specifically includes Article 17 (Art. 17 GDPR, n.d.) that states the right of data subjects to demand that controllers erase their personal data under certain conditions. The GDPR requires a high level of openness about the data being collected and how it is processed. Article 15 (Art. 15 GDPR, n.d.) states that data subjects have a right of access, to know the content of the data, the purposes of its processing, who it has been or will be shared with, how long it will be shared, whether any automated processing of that data will occur, and even access to meaningful information about how the automation works and what conclusions are hoped to be drawn from it. As discussed, many see a dimension of privacy as covering our own personal autonomy—whether one has the freedom to make personal decisions affecting their pursuit of the good life. This right of access supports that dimension of privacy. European data subjects can ensure, for instance, that no automated processing can affect their ability to obtain credit, which could otherwise negatively impact personal decision-making about how those subjects want their lives to go.

From the perspective of data governance, the GDPR also guarantees some measures will be taken. Article 25 (Art. 25 GDPR, n.d.) mentions pseudonymization: controllers must have the technological capacity to transform personal data into a form that cannot be attributed to any natural person. This rule, then, builds in a decision about how data can be processed; it automatically requires a form of data governance. Similarly, Article 37 (Art. 37 GDPR, n.d.) requires the appointment of a Data Protection Officer (DPO): this officer can be from the relevant company’s staff, or be contracted from an external firm, but they are effectively a compliance officer who must have IT and legal competences. This person advises the data processors on the obligations the GDPR imposes and monitors for compliance in the processing operations. The existence of this position, then, is a manifestation of data governance. The DPO enforces certain structures that regulate the flow and use of data within the company (to preserve the privacy of data subjects).

Many other nations have laws modeled after the GDPR: Japan, South Korea, and Brazil, for instance. The United Kingdom, in the aftermath of Brexit, also adopted an identical piece of legislation. The United States, on the other hand, has no such national legal code.

There are *specific* US federal-level codes, however. One is the Privacy Act of 1974 (Office of Privacy & Civil Liberties, 2020), which covers disclosure of personal data that is held by federal agencies. It has exceptions that are similar to the GDPR and US citizens are even entitled to access that information. But this only concerns information held by federal entities, not by any (private) data holder or processor in the United States.

Also in the United States, there is the Gramm-Leach-Bliley Act (GLBA) (Federal Trade Commission, n.d.), which, while having a broader regulatory scope than privacy preservation, requires that financial institutions with personal data to explain to its customers how their data is being used and provide opt-out information. It also includes a safeguard rule that requires those institutions to have (at least) written plans for protecting that nonpublic, personal data about its customers. These plans, then, function as a kind of mechanism for installing data governance within the companies covered by the Act. Again, the focus here is narrowly on financial information.

There is also HIPPA, which, among other things, imposes rules on disclosure of personal health data gathered by healthcare providers and businesses. As with the other Acts, HIPPA also concerns only this specific realm of data.

Finally, the most general federal-level law is the Children's Online Privacy Protection Act (COPPA) (Federal Trade Commission, n.d.), which, as the name suggests, covers the collection of personal data of those under 13 years of age. The existence of COPPA is largely the reason many social media companies will not allow people under 13 to have accounts. Instagram, for example, had toyed with the notion of allowing children to have them, but, as of writing, still requires users to be over 13.

There are individual US *states* that have adopted data privacy legislation. The California Privacy Rights Act (State of California, 2023) functions much like the GDPR with the exception of health and financial information, which is already federally covered by HIPPA and GLBA. It is considered the “strongest” piece of data privacy law in the United States, partially because it is the only one that allows citizens to sue companies for privacy violations. The Act only applies, unsurprisingly, to residents of the state. Virginia instituted its Consumer Data Protection Act (Office of the Attorney General, 2023) only at the beginning of 2023. The Colorado Privacy Act (Colorado Attorney General, n.d.) and

Connecticut Data Privacy Act (The Connecticut Privacy Act, n.d.) also followed in July of 2023. Utah's Consumer Privacy Act (DataGuidance, n.d.) will take effect at the end of 2023. More states are sure to follow until there is US federally based legislation.

LOOKING TO THE FUTURE

The trifecta of data governance, data privacy, and data ethics have finally reached the consciousness of nearly everyone. Erroneous reports sent to consumers based on bad data, data breaches, and horrendous misuse of data have been in the news weekly, if not daily. One of the few things that we know we can count on (besides death and taxes) is the continual growth in the amount of data collected and used (though much more is collected than used). And with the abundance of data, and the fact that implementations for the trifecta are at the very early stages, there is much more to come of the good and the bad before we can or should feel comfortable.

The actions in Europe with the GDPR are far ahead of the rest of the world. The United States has states that are developing their own regulations which means that it will not be long before the Federal Government steps in to provide necessary consistency. Even with all the safeguards and best intentions, there is no practical means by which guarantees can be enforced because, at the heart, the proper governance, respect for privacy, and ethical use, are in the hands of human beings. Mistakes, malfeasance, maliciousness, and ignorance are our worst enemies. The best we can hope for is to have the mechanisms, training, and oversight to optimize the business value of data while minimizing those things that can go wrong. The alternative, no data, is not realistic. Therefore, we need to focus on ensuring that the best possible data governance is put into place, enforced, audited, managed, and evolved to ensure the data privacy and ethical use of data we should all expect.

REFERENCES

- Art. 15 GDPR. (n.d.). Right to Erasure ('Right to be Forgotten'). General Data Protection Regulation (GDPR). Retrieved August 22, 2023.
- Art. 17 GDPR. (n.d.). Right to Erasure ('Right to be Forgotten'). General Data Protection Regulation (GDPR). Retrieved August 22, 2023.

- Art. 25 GDPR. (n.d.). Right to Erasure ('Right to be Forgotten'). General Data Protection Regulation (GDPR). Retrieved August 22, 2023.
- Art. 37 GDPR. (n.d.). Right to Erasure ('Right to be Forgotten'). General Data Protection Regulation (GDPR). Retrieved August 22, 2023.
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information Pew Research Center. Retrieved August 22, 2023.
- Caserta. (n.d.). What Is Data Governance | Consulting & Implementation Services. Retrieved August 2, 2023.
- Colorado Attorney General. (n.d.). Colorado Privacy Act (CPA). Retrieved August 22, 2023.
- Criddle, C. (2020, October 28). Facebook Sued Over Cambridge Analytical Data Scandal. Retrieved August 2, 2023.
- Cyolo. (2020, December 31). 7 Cybersecurity Breaches in 2020 and How They Could Have Been Prevented. Retrieved August 2, 2023.
- DataGuidance. (n.d.). Utah. Retrieved August 22, 2023.
- DeCew, J. (2018). Privacy. In *The Stanford Encyclopedia of Philosophy* (Spring 2018 ed., E. N. Zalta, Ed.). <https://plato.stanford.edu/archives/spr2018/entries/privacy/>
- Dizikes, P. (2023, June 21). Study: Microtargeting Works, Just Not the Way People Think. MIT News. Retrieved August 22, 2023.
- Federal Trade Commission. (2019a, July 24). FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. Retrieved August 2, 2023.
- Federal Trade Commission. (2019b, July 24). FTC Sues Cambridge Analytical, Settles with Former CEO and App Developer. Retrieved August 2, 2023.
- Federal Trade Commission. (n.d.). Children's Online Privacy Protection Rule ("COPPA"). Retrieved August 22, 2023.
- Federal Trade Commission. (n.d.). Gramm-Leach-Bliley Act. Retrieved August 22, 2023.
- Fung, B. (2021, August 24). Data Leak Exposes Tens of Millions of Private Records from Corporations and Government Agencies. Retrieved August 2, 2023.
- Gartner. Gartner Glossary—Information Technology Glossary—D. Definition of Data Governance—IT Glossary | Gartner. Accessed July 11, 2023.
- General Data Protection Regulation (GDPR). (n.d.). General Data Protection Regulation (GDPR)—Official Legal Text. <https://gdpr-info.eu/>. Accessed July 12, 2023.
- Goldhill, O. (2022, June 24). Supreme Court Decision Suggests the Legal Right to Contraception Is Also Under Threat. *STAT News*. Retrieved August 22, 2023.

- Greaton, T. (2019, December 23). What's Causing the Exponential Growth of Data? *Nikko AM Insights Site*. https://insights.nikkoam.com/articles/2019/12/whats_causing_the_exponential. Accessed October 1, 2023.
- Healthcare Dive. (2023). HCA Reports Data Security Incident Affecting Estimated 11M Patients. Retrieved from HCA Reports Data Security Incident Affecting Estimated 11M Patients | Healthcare Dive on July 17, 2023.
- Heaven, W. D. (2021, June 17). Bias Isn't the Only Problem with Credit Scores—And No, AI Can't Help. *MIT Technology Review*. Retrieved August 22, 2023.
- Henriquez, M. (2022, January 31). Security firm Securitas Exposed Airport Employees in Data Breach. Retrieved August 2, 2023.
- Higher Ed Dive. (2023). Johns Hopkins hit with Class Action Lawsuit Following Data Breach. Retrieved July 17, 2023 from <https://healthcareservicesinvestmentnews.com/2023/07/12/johns-hopkins-hit-with-class-action-suit-following-data-breach/>
- IAAP. International Association of Privacy Professionals. What Is Privacy. <https://iapp.org/>. Accessed July 11, 2023.
- IBM Security. (2022). Cost of a Data Breach Report 2022. IBM. Retrieved July 14, 2023, from <https://www.ibm.com/downloads/cas/3R8N1DZJ>
- IDC & Statista. (June 7, 2021). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025 (in zettabytes) [Graph]. In *Statista*. Retrieved March 25, 2024 from <https://www.statista.com/statistics/871513/worldwide-data-created/>
- IFF Lab. (n.d.). 7 Major Causes of a Data Breach and Identity Theft. Retrieved July 14, 2023, from <https://ifflab.org/7-major-causes-of-a-data-breach/>
- Immuta. (2022). DBTA Report: Meeting the Growing Challenges of Data Security & Governance. Retrieved July 12, 2023 from <https://www.immuta.com/resources/dbta-report-meeting-the-growing-challenges-of-data-security-governance/>
- Janiszewska-Kiewra, E., Podlesny, J., & Soller, H. (2020, August 26). Ethical Data Usage in an Era of Digital Technology and Regulation. Retrieved from McKinsey & Company on August 2, 2023.
- Klein, A. (2020, July 10). Reducing Bias in AI-Based Financial Services. Brookings Institution. Retrieved August 22, 2023.
- National Association of Attorneys General. (n.d.). Data Breaches. Retrieved July 14, 2023, from <https://www.naag.org/issues/consumer-protection/consumer-protection-101/privacy/data-breaches/>
- Nissenbaum, H. (2010). *Privacy in Context: Policy and the Integrity of Social Life*. Stanford University Press.
- Office of Privacy and Civil Liberties. (2020). *Overview of the Privacy Act of 1974* (2020 ed.). United States Department of Justice. Retrieved August 22, 2023.

- Office of the Attorney General. (2023, February 2). *The Virginia Consumer Data Protection Act*. Commonwealth of Virginia. Retrieved August 22, 2023.
- Roche, J., & Jamal, A. (2021). A Systematic Literature Review of the Role of Ethics in Big Data. In H. Jahankhani, A. Jamal, & S. Lawson (Eds.), *Cybersecurity, Privacy and Freedom Protection in the Connected World* (p. 20). Springer International Publishing. https://doi.org/10.1007/978-3-030-68534-8_20
- Roessler, B., & Mokrosinska. (2015). *Social Dimensions of Privacy*. Cambridge University Press.
- Safety Detectives. (2023, March 15). Securitas Leak Report: 1.2 Million Records Exposed. Retrieved August 2, 2023.
- State of California—Department of Justice—Office of the Attorney General. (2023, May 10). California Consumer Privacy Act (CCPA). Retrieved August 22, 2023.
- The Connecticut Data Privacy Act. (n.d.). Office of the Attorney General. Retrieved August 22, 2023.
- U.S. General Services Administration. (n.d.). Federal Data Strategy Data Ethics Framework. Retrieved July 11, 2023 from <https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf>
- Yallop, A., & Seraphin, H. (2020). Big Data and Analytics in Tourism and Hospitality: Opportunities and Risks. *Journal of Tourism Futures*, 6(3). <https://doi.org/10.1108/JTF-10-2019-0108>
- Yallop, C., & Aliasghar, O. (2020). No Business as Usual: A Case for Data Ethics and Data Governance in the Age of Coronavirus. *Online Information Review*, 44(6), 1217–1221. <https://doi.org/10.1108/OIR-06-2020-0257>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 6

Web2 Versus Web3 Information Privacy: An Information Systems Discipline Perspective

Mary C. Lacity and Erran Carmel

INTRODUCTION TO WEB2 AND WEB3

We begin this chapter with a hypothetical question: Would you let a stranger live in your home and eavesdrop on everything you and your family and friends say?

Most readers will instinctively answer, “No!” The thought of a stranger invading the privacy of our homes invokes scenes from George Orwell’s novel, *Nineteen Eighty-Four*. Digital personal assistant devices like Amazon’s Alexa, Google’s Assistant, and Apple’s Siri devices, however, do just that—they are always listening. While the companies who sell these devices promise that their products only process information when the devices detect their wake-up word, all of these devices

M. C. Lacity (✉)
University of Arkansas, Fayetteville, AR, USA
e-mail: mclacity@uark.edu

E. Carmel
American University, Washington, DC, USA

have *false accepts*, meaning they record conversations even though the person did not invoke the wake-up word. Whistle-blowers and employees report that humans have access to these recorded conversations. Apple contractors, for example, said that they routinely hear drug deals, medical details, and people having sex from Siri devices (Hern, 2019). Humans working for Google read sample recordings, including false accepts (Aten, 2019). If we think false accepts are isolated incidents, consider the US Federal Trade Commission's 2023 enforcement actions against Amazon's Alexa and Ring devices. Amazon agreed to pay \$30.8 million for violating users' privacy, including through misleading data retention practices, over-broad employee access to user data, and inadequate cybersecurity practices (Nahra & Evers, 2023).

These stories of digital assistants serve as powerful examples for the context of this chapter. The stories highlight a defining attribute of the version of the Internet known as Web2. Whereas *Web1* was the era of the Internet that enabled web browsing and online shopping (e-commerce), *Web2* introduced easy content generation for users via social media applications like Facebook, YouTube, and Twitter. *Web2* is the dominant version of the Internet used for economic and social activities.

With *Web2*, individuals rely on centralized platform providers to access online services. Many centralized platform providers collect user data in exchange for free or low-cost services, apply artificial intelligence (AI) to predict behavior, and then sell these predictions to other organizations. Amazon's e-commerce site, Bing, Facebook, Google Search, Instagram, Snapchat, TikTok, Twitter, WeChat, YouTube, and any other applications that display advertisements work this way. The economic model is called *surveillance capitalism* and it eviscerates user privacy (Zuboff, 2019).

Identity theft is another common occurrence with *Web2*. Our online relationships with centralized platform providers are managed with accounts and passwords, which are stored—along with our personal data—in the provider's centralized databases. These databases then become prime targets for cyberthieves. The United States (US) Bureau of Justice Statistics estimated that 23 million US residents were victims of identity theft in 2021, costing victims more than \$56 billion (US Bureau of Justice Statistics, 2021).

Given *Web2*'s downsides of privacy invasion and identity theft, why do users willingly give these centralized platform providers their personal information? Information Systems (IS) scholars have investigated this question.

IS scholars study how digital information systems are designed and used by individuals, organizations, and communities. In the context of privacy, IS scholars examine *information privacy*, defined as “the ability of individuals to control the terms under which their personal information is acquired and used” (Culnan & Bies, 2003, p. 326). IS research escalated when the threats to information privacy skyrocketed during the rise of Web2 in the 2000s. IS scholars have conceptualized and examined information privacy in terms of an individual’s information privacy concerns and have examined why these concerns do not prevent individuals from disclosing personal information with centralized platform providers; the phenomenon is called the *privacy paradox*. As we discuss in this chapter, IS scholars have four common explanations for Web2’s privacy paradox: privacy calculus, privacy fatigue, trust, and lack of choice.

We, along with other IS scholars, take a different approach to user privacy. We believe that the root cause of information privacy leakages stems from the design of Web2. Unauthorized security breaches—including identity theft and intentional sharing of user data under the surveillance capitalism model—largely occur because the software and user data is controlled by centralized platform providers. Web3 aims to fix those issues of Web2. *Web3* is the era of the Internet that is based on decentralized infrastructures.

Let’s begin with the *why* of Web3. Many people believe that the decentralization of economic and social activities is the best way to increase individual’s privacy, power, and cybersecurity (Allen, 2016; Nakamoto, 2008; Preukschat & Reed, 2021; World Economic Forum, 2020). Decentralized activities discourage abuses of power and ideally promote more inclusive participation, unity around decisions, and individual empowerment, freedom, and privacy. Since most of our modern economic and social activities happen online, decentralized activities need decentralized digital platforms, applications, and governance—thus the creation of Web3 (Lacity & Lupien, 2022).

Bitcoin was the first Web3 application, launched in 2009. Bitcoin was invented by Satoshi Nakamoto—a pseudonym used by an unknown person or persons who remains unknown to this day. Nakamoto imagined a world where people could safely, securely, and anonymously transfer value directly with each other (1) without using government-issued currencies; (2) without relying upon trusted third parties (TTPs) like banks or brokers; and (3) without the need to reconcile records across trading partners. Bitcoin has its roots in Libertarian and Cypherpunk

values, which aim to create social and political change by circumventing governments and large financial institutions through privacy-enhancing technologies (Lacity & Lupien, 2022).

While most people are familiar with Bitcoin, which is a cryptocurrency, we highlight Ethereum because Ethereum is the most commonly used platform for deploying decentralized applications. Whereas Bitcoin is just a peer-to-peer payment system (it does not do much else), Ethereum was designed to allow anyone to use it as a platform for deploying decentralized applications. Launched in 2015, Ethereum is a network of dispersed computers, with no master computer in charge, meaning no single company or individual can alter the decentralized application or the transactions that are stored on its distributed ledger, also called a blockchain.¹ The *distributed ledger* is a time-stamped, permanent record of all valid transactions that have occurred within the Ethereum network. The ledger also stores copies of distributed applications (software). The ledger is replicated on all the computers in the network, which is why it is called *distributed*. Anyone with access to the Internet can view it (see <https://etherscan.io/>). No PII is stored on Ethereum's distributed ledger.

Users can be confident that the Ethereum network will only allow valid transactions. Like all Web3 applications, two validations are always performed. First, users prove they own the asset with the private key stored in their digital wallet (explained later in the chapter). Second, the computers on the Ethereum platform check the shared distributed ledger to make sure the user has enough funds in their wallet to cover the transaction, thus preventing the double spend.

Keeping with the values of Web3, Ethereum is not owned or controlled by any company. Changes to the Ethereum software are based on *meritocracy*, meaning that ideas are evaluated based on their quality. Anyone can suggest improvements by submitting an Ethereum Improvement Proposals (EIPs). The whole Ethereum community (computer operators, developers, and users) can vote on the proposal based on its merit. Any

¹ This term “blockchain” is used several ways. Sometimes the term refers broadly to what we are calling a decentralized application or platform. For example, people call Bitcoin and Ethereum “blockchains.” The term can also be used to describe the structure of the digital ledger. With a blockchain structure, newly submitted transactions are sequenced and collected into a block. Each block points to its immediate predecessor, forming a chain of sequenced blocks over time, all the way back to the first block.

person with access to the Internet can review the proposals (see <https://eips.ethereum.org/>). By 2023, over 1000 EIPs had been submitted, with more than 80 finalized. The non-profit organization, Ethereum.org, coordinates the process. Ethereum.org is led by a core team in Bern Switzerland with contributions from thousands of people across the world (<https://ethereum.org/en/about/#>).

In addition to Web3's increased privacy, decentralized applications also improve cybersecurity. Decentralized applications that run on platforms like Ethereum are resilient to cybersecurity attacks because the attack surface is diffused across many locations. Over 500,000 computers operate the Ethereum platform in 80 countries, each with its own identical copy of the ledger (Liu, 2023). The only way to infiltrate the platform is to commandeer more than 50% of the computers. So far, the Ethereum platform has never been overtaken.²

Some concerned law enforcement agencies have argued that Web3's privacy enhancing features invite more criminal activity than Web2 applications. So far in Web3's development, the percentage of crime in the Web3 market has not been significantly different than the percentage of crime in Web2. Both markets see between 1 and 5% of illegal activity (Chainanalysis, 2023; Hopper, 2023; United Nations, 2023). The expectation is that Web3's privacy enhancements will reduce opportunities for identity theft that exist today with Web2.

While it is still early days for Web3, education is an important driver of adoption. This chapter educates readers on how Web3 enhances information privacy (and cybersecurity) compared to Web2. By the end of this chapter, readers will be familiar with the Web3 concepts of digital wallets and distributed ledgers. We illustrate concepts by comparing Web2 versus Web3 applications for browsing, financing, storage, and visiting virtual worlds known as metaverses. While our Web3 application examples focus on *anonymity*, many services require *confidentiality*, meaning that data is viewable by authorized parties. Web3 applications are emerging that allow for confidential (not anonymous) transactions that enhance privacy while ensuring user credentials are valid.

² While this statement is true for the Ethereum platform, some specific decentralized applications have been compromised due to poorly written computer code.

INFORMATION SYSTEMS (IS) SCHOLARS' APPROACH PRIVACY RESEARCH

First, we explain how information system (IS) scholars approach privacy research. IS scholars primarily conceive of—and study—privacy in terms of digital information privacy. Our field studies how computers are used to collect, process, store, and retrieve *personal identifiable information* (PII) that can describe, characterize, identify, or otherwise verify an identifiable legal person or a group of people (AICPA/CICA, 2020). A person's name, home address, identification (ID) number (like a national ID or an employee ID), criminal record, healthcare record, gender, age, and religious affiliation are examples of PII. PII also includes the individual's data associated with their online activities, such as their computer's unique Internet Protocol (IP) address, email address, logon account name, and website cookies that remember an individual's online activities.

Privacy Paradox

Hundreds of IS studies on information privacy have been published. Many IS scholars have surveyed individuals and their information privacy attitudes, privacy concerns, and information sharing intentions. Overall, individuals are deeply concerned about online privacy (Bélanger & Crossler, 2011; Mitchell & El-Gayar, 2022). Pavlou, 2011; Rath & Kumar, 2021; Smith et al., 2011). This concern, however, does not prevent individuals from disclosing PII online. This inconsistency between attitude and behavior is called the *privacy paradox* (Li et al., 2017; Pavlou, 2011; Zhu et al., 2021).

The privacy paradox has been found to exist in general Internet use and in specific instances of online applications (e.g., Dinev & Hart, 2006). IS scholars have studied the privacy paradox in the contexts of social media (e.g., Mosteller & Poddar, 2017), online shopping (e.g., Li et al., 2017), online reviews (e.g., Mosteller & Mathwick, 2014), healthcare applications (e.g., Zhu et al., 2021), and mobile applications (e.g., Pentina et al., 2016).

Although the IS literature is too rich to summarize adequately here, in general, IS scholars theorize that the privacy paradox can be explained by either a rational decision-making process called *privacy calculus* or by

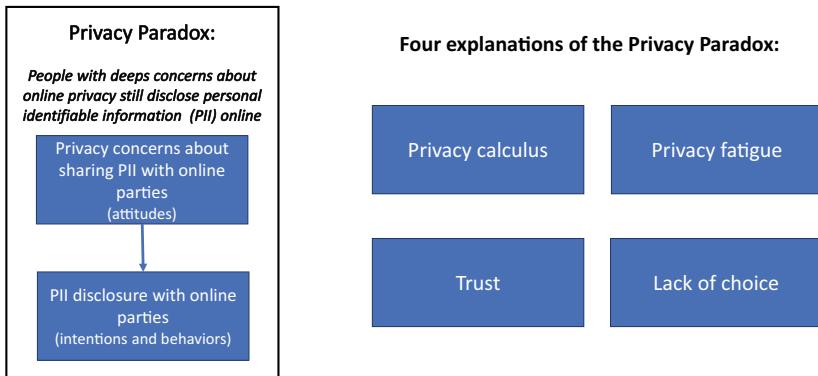


Fig. 6.1 An overview of Information Systems research on information privacy (*Image credit* The authors)

an emotional decision-making process called *privacy fatigue*. IS scholars also explain the privacy paradox with additional variables such as *trust* and *lack of choice* (see Fig. 6.1).

Privacy Calculus

Ackerman (2004) was one of the first scholars to theorize that users perform a privacy calculus to determine whether the benefits received from revealing personal information are worthwhile. This theory assumes a rational view of the individual's decision-making process. In the context of social media, researchers have found that users consider the benefits of enjoyment, affirmation, and connection against the risks of privacy concerns (Mosteller & Poddar, 2017; VanMeter et al., 2015; Zalmanson et al., 2022). With respect to posting online reviews, users consider the benefits of pleasure associated with posting a review, gaining knowledge, feeling connected, and promoting one's opinions against the risks of privacy concerns (Mosteller & Mathwick, 2014). In terms of trusting the Internet for e-commerce, researchers have found that an individual's personal Internet interest outweighed their privacy risk perceptions in the decision to disclose personal information. The authors conclude, "These findings provide empirical support for an extended privacy calculus model" (Dinev & Hart, 2006, p. 61).

Support for the privacy calculus theory is found across cultures. For example, one survey of 106 American and 120 Chinese millennials found support for privacy calculus theory in the context of users' intentions to download and deploy mobile applications that require access to personal information. Individuals in the study valued the informational and social benefits provided by the application more than they valued their privacy (Pentina et al., 2016). In another study of 422 US and 889 Italian users, both samples found support for privacy calculus theory, although the Italians had lower propensity to trust and higher privacy concerns than the Americans (Dinev et al., 2006).

Privacy Fatigue

In contrast to the privacy calculus theory that focuses on rational explanations of the privacy paradox, privacy fatigue theory focuses on human emotions.

Many studies show that individuals experience *privacy fatigue*, defined as a user's feelings of exhaustion, cynicism, helplessness, and powerlessness to protect their data privacy, often to the point where individuals feel defeated (Tian et al., 2022). According to the theory, privacy fatigue leads individuals to disclose personal information.

In one study, data from 324 Internet users found that high levels of privacy fatigue were positively related to intentions to disclose personal information. The authors concluded, "repeated consumer data breaches have given people a sense of futility, ultimately making them weary of having to think about online privacy" (Choi et al., 2018, p. 42).

One literature review of 18 academic studies on privacy fatigue summarized the antecedents and consequences of privacy fatigue (van der Schyff et al., 2023). Privacy concerns, lack of knowledge, information overload, loss of control, and fear of privacy invasion were the major antecedents (precursors) of privacy fatigue. Self-disclosure, privacy burnout, privacy resignation, and mistrust were the major consequences/outcomes of privacy fatigue.

Trust

IS scholars have also theorized that trust may offset privacy concerns. IS scholars for decades have found trust to be a core variable for explaining individual uses of information systems. The IS discipline does not have a

standard definition of trust, although IS scholars generally agree that trust entails the presence of a human subject who forms a trust perception about the object of the subject's trust, such as another person, organization, or technology. Under circumstances of risk, *trust* is a subject's psychological belief that an object of trust will discharge their obligations as expected in a specific context (Lacity et al., 2023a). Initially, in the mid-1990s, the concept of trust helped scholars understand individuals' willingness to use the Internet for shopping (e.g., Jarvenpaa & Todd, 1996). In the years that followed, trust has been examined in many other contexts including blogging, e-government, e-healthcare, mobile applications, and social networks (Lacity et al., 2023a). Trust is more generally understood as a key determinant of people's willingness to use and rely on IS (Lacity et al., 2024; Schuetz et al., 2023).

Privacy concerns, the willingness to disclose PII, and trust have complex relationships. Some IS studies found direct relationships while other studies found moderating or mediating relationships.

A direct relationship involves two variables that are closely associated. For example, one study of 369 respondents found that high levels of Internet trust were associated directly with a willingness to disclose PII (Dinev & Hart, 2006).

A mediated relationship involves three variables, with the mediating variable explaining how the other two variables are related. For example, one study found that users who are concerned about privacy will disclose personal information if they trust the website (Mosteller & Poddar, 2017). In this example, trust mediates the relationship between privacy concerns and the willingness to disclose personal information.

A moderated relationship also involves three variables, with the moderating variable affecting the strength of the relationship between the other two variables. For example, one laboratory experiment with 667 individuals found that privacy concerns moderated the relationship between privacy assurance mechanisms (like a Website's policy statement) and the user's trust in the website (Bansal et al., 2015).

IS scholars also study institutional safeguards. *Institutional safeguards* are practices and policies centralized platform providers use to increase users' trust in and willingness to disclose PII (Bansal et al., 2015; Boritz & No, 2011; Guo et al., 2021). Institutional safeguards that increase trust include assurance services, escrow services, privacy seals, third-party endorsements, and guarantees. Institutional safeguards that increase information security include encryption, certificate authorities (to

prove you are at a legitimate website), and tools that authenticate users, such as multifactor authentication (Mitchell & El-Gayar, 2022). Some centralized platform providers use CAPTCHAs, which are tasks to prove the user is human and not a software robot, such as asking a user to identify a word that appears within a blurry image. Some IS scholars argue that institutional safeguards are not enough; organizations should also create a culture of privacy that begins with top management (Culnan & Clark-Williams, 2009).

Lack of Choice

Lack of user choice is another explanation for the privacy paradox. As Onora O'Neill, philosopher and prior president of the British Academy, observed about why people rely on institutions they mistrust, “We cannot opt out of government, or the legal system, or the currency even if we have misgivings” (O’Neill, 2006 transcript of BBC Radio Broadcast). Similarly, the privacy paradox exists in part because users have no choice. Users are forced to consent to a centralized platform’s privacy policy or they can’t use the application. Once users agree to a privacy policy—which is often pages long and filled with legalese—they cannot easily backtrack. Individuals who try to protect themselves by deleting their accounts cannot do so because they don’t have create, read, update, and delete (CRUD) rights—the centralized platform providers do. Individuals, for example, cannot directly delete their Facebook accounts because Facebook has the CRUD rights; individuals must trust that Facebook will execute their requests.

Readers interested in learning more about IS scholarship may consult several literature reviews on information privacy (e.g., Bélanger & Crossler, 2011; Boritz & No, 2011; Rath & Kumar, 2021; Smith et al., 2011; van der Schyff et al., 2023).

The four explanations of the privacy paradox—privacy calculus, privacy fatigue, trust, and lack of choice—are all by-products of Web2’s centralized design. Web3 bypasses the need for centralized platform providers, and thus reduces and even eliminates the need to disclose PII for many types of applications.

WEB2 AND WEB3 EXPLAINED

Readers are likely familiar with how Web2 applications work for online searching, shopping, banking, data storage, social media, and other services. Users access a Web2 application with an account and password and must disclose any additional PII required by the centralized platform provider. An online banking application, for example, in order to verify consumer identity at a high threshold, may require a national ID (such as driver's license or passport), a credit report, and proof of employment in addition to an account and password. Readers probably understand that the bank governs the software that provides the service. The banks software processes user requests and stores transactions on a database which is, again, governed by the bank. Most Web2 applications work this way (see left column of Fig. 6.2).

Web3 applications work differently; they aim to protect *anonymity*, the ability to conceal a person's identity. Individuals can choose to be totally anonymous, pseudonymous, or identifiable (Smith et al., 2011). Rather than accounts and passwords, users access Web3 applications with a digital wallet—no PII is required for many Web3 applications. Rather

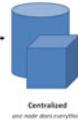
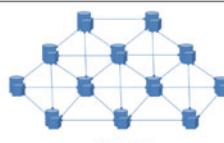
	Web2	Web3
User access and PII data required to connect and transact	<p>Centralized</p>  <ul style="list-style-type: none"> • Account and password • Personal identifiable information (PII) as required by the centralized platform provider <p>Federated</p> <ul style="list-style-type: none"> • Log in with Facebook • Log in with Google • Log in with Twitter • Log in with LinkedIn • Log in with GitHub • Log in with Microsoft 	<p>Decentralized</p>  <ul style="list-style-type: none"> • no PII is required for many Web3 applications
Location and governance of software and data	<p>Ledger of transactions and other data storage →</p>  <p>Software that processes transactions ←</p> <ul style="list-style-type: none"> • Centralized software and data governed by the centralized platform provider 	<p>Decentralized</p>  <ul style="list-style-type: none"> • Decentralized software and databases replicated on many computers that are peers, with no single computer in charge; Decision-making rights are held by a community, a non-profit organization, or owners of governance tokens.
Economic model	Surveillance capitalism	Token economics

Fig. 6.2 Fundamentals of Web2 and Web3 (*Image credit* The authors)

than a centralized platform provider storing transactions on a centralized database, transactions are copied and stored on tens or even hundreds of thousands of peers computers, meaning no single computer is in control (see right column of Fig. 6.2).

Let's take a closer look by comparing Web2's and Web3's user access and PII data required, location and governance of software and data, and the primary economic model of each.

User Access and PII Data Required

For most of the history of the Internet, users access online services by creating an account and password with the centralized platform provider. Users need an account and password because the Internet was initially designed without an identity layer.

The Internet traces its roots to ARPANET, a computer network designed by the US Defence Advanced Research Projects Agency (DARPA) to share information among researchers who already knew and trusted each other. As more computers were added and as other networks emerged (ARPANET was not the only one), a standard way to connect computers was needed. Two DARPA scientists—Vint Cerf and Robert Khan—did just that when they developed the Transmission Control Protocol/Internet Protocol (TCP/IP) in the 1970s (Lacity & Lupien, 2022).

TCP/IP became a standard in 1982 and it is still the Internet's primary protocol used today. Every device connected to the Internet has a unique IP address. For example, the IP address for the University of Arkansas server is 130.184.0.0/16. While TCP/IP provides a way to identify the machines connected to the Internet, the standards do not verify the individuals who are sending messages from those machines. Governments and organizations needed to know who is using devices, leading us to the first era of identity on the Internet, known as the *centralized identity model*. Centralized identity models are account based, requiring users to create logon IDs and passwords. Accounts and passwords date back to the 1960s when multiple people were sharing the same computer (McMillan, 2012). Web2's user access is a legacy of this history.

Web2's accounts and passwords. Web2's centralized identity model gives centralized platform providers control over a user's data (Preukschat & Reed, 2021). Even when users "delete" an account, all

they have done is revoke their access privileges, as it is up to the centralized platform provider to decide when an account is deleted from their databases. Also, online identities are not portable across webpages (Allen, 2016). The proliferation of accounts and passwords is another limitation of the centralized model. By 2015, the average United Kingdom (UK) Internet user had 118 online accounts; by 2017, the average US Internet user had 150 online accounts (Caruthers, 2018).

More recently, some organizations invite users to access multiple sites through a single account managed by a centralized platform provider such as Facebook, Google, Amazon, LinkedIn, and others called the *federated identity model*. While the federated model reduces the number of accounts users need to manage, it increases the amount of PII collected and used by centralized platform providers—resulting in fewer organizations now having much more PII.

Web3's digital wallets. Privacy experts have struggled for years to come up with a better way to establish identities and relationships while preserving privacy, leading to the Web3 solution for Internet identity: the decentralized identity model. Web3 aims to empower individuals to control their own identities, credentials, and assets. Web3 replaces user-names and passwords with peer-to-peer connections via digital wallets. To transfer money or other assets, two people must each have a digital wallet (see right column of Fig. 6.2).

While digital wallets are easy to use, there's a lot of sophisticated technology under the hood of a digital wallet. A digital signature is the most important feature to understand because if a user doesn't protect the private key that is used to generate a digital signature, the user risks losing/revealing all their digital assets. Digital signatures ensure the individual submitting the transaction (sender) is authentic, the transaction was not tampered with in transit, and the receiver cannot later deny getting paid (Lacity & Lupien, 2022).

Here's how a digital signature works: A digital wallet generates a unique pair of numbers that are mathematically related, called a private-public key pair. A private key is a sort of super-safe password created and managed by the digital wallet. Here is an example of a private key:

DDA78BA47C7D3A1A49AA02E6C1CF7A30691603827E7DACE3C
4EE63CA0D26DAE2

The key above is a very large number, expressed in hexadecimal, which is why we see letters A through F. A super-secure algorithm uses the private key to create its mathematical mate, called a public key (also called an *address* or *public key address*). A typical public key address looks like:

0x77300C71071eCa35Cb673a0b7571B2907dEB77C7

Although the private key will always generate the same public key address, it's nearly impossible to guess a private key if only given the public key address. Today's digital computers would take millions of years to randomly guess a private key that matches a public key address (Sharma, 2017). That's the power of *cryptography*, defined as "a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it" (Techtarget.com).

When the user wants the wallet to transfer value out of it, the digital wallet automatically uses the private key to sign digitally the transaction. The digital signature works in such a way that all the computers on the platform can be confident that ONLY the wallet with the private key associated with this public key address could have generated the transaction.

The private key is stored ONLY in the user's digital wallet. When a transaction takes place on the decentralized platform, ONLY the public key address is stored on the distributed ledger.

Users must remember two important things about digital wallets. First, digital wallets enhance privacy. Parties can connect to each other without revealing PII. For many Web3 applications, two parties minimally need to share public key addresses. As we saw from the example above, the public key address is just a large number; it doesn't tell us anything about the individual! Moreover, a user's digital wallet generates hundreds of key pairs. So, unlike a bank account number that is used over and over again, a Web3 digital wallet can generate new public key addresses for each transaction to help enhance privacy.

Second, wallet users must protect their digital wallets! Most Web3 heists happen at the vulnerable access points of digital wallets where private keys are stored. Once a hacker steals a private key, they control the assets and can easily transfer funds to their own digital wallet. Because users store their digital wallets on their own devices, users should:

- keep very few digital assets in “hot” wallets that are connected to the Internet;
- keep most digital assets offline in a “cold” wallet; keep the cold wallet backed up on multiple devices;
- print wallet recovery keys³ on paper and store them in a vault. Or better yet, divide recovery keys across multiple pieces of paper and store parts in different secure locations;
- keep wallet software updated.

Soon, social recovery key sharding will be another common approach. With *sharding*, a user instructs the wallet to divvy up the recovery keys among people the user trusts, and pieces of the key are stored in those people’s wallets. More backup and recovery methods are being developed because protecting the private keys are paramount to the entire Web3 model.

Location and Governance of Software and Data

For any online application, we need software to process transactions and a record of every transaction.

Web2’s centralized software and databases. With Web2 applications, every party manages its own systems of records (software and databases, including ledgers that track debits and credits). A monthly bank account statement is an example of a report from a bank’s ledger. A bank statement lists all the receivables coming into an account (credits) and payments made (debits) out of an account. The summation of all transactions over time results in the account balance. Bank customers must review and reconcile any differences between the bank’s records and the customer’s own records. The bank has the power in this relationship because banks govern the official records accepted by regulators. The same is true of other centralized platform providers that store user transactions on their centrally controlled databases.

Web3’s distributed ledger. Web3 uses a different bookkeeping method, called *triple-entry accounting*, in which every transaction has three entries:

³ Most digital wallets require a locally stored password, and if you forget your password, most digital wallets have *recovery keys*, which are typically 12 random words in a sequence.

the debit in the sender’s digital wallet, the credit in the receiver’s digital wallet, and the public receipt stored on a shared distributed ledger. Anyone with access to a Web browser can view the ledger, but all they will see are the sender’s public key address, the receiver’s public key address, and the amount of the transfer—no PII is stored on the distributed ledger.

The computers in the network constantly reconfirm the ledger to make sure no party tampers with the records after-the-fact. If anyone cheats, the other computers in the network automatically ignore it. Parties no longer need to reconcile records because every party agrees “this is what transpired.”

Economic Model

Web2’s primary economic model is surveillance capitalism, which was explained in the introduction. Here, we focus on Web3’s economic model.

Web3’s token economics. Web3 is based on a new economic model called *token economics* in which individuals earn digital tokens for engaging in desired behaviors. On the right column of Fig. 6.2, we see a network of computers, with each computer operating an identical copy of the software and storing an identical copy of the ledger. Why would someone use their computer for this purpose? Because they are paid to do so in the form of digital tokens! In the Bitcoin network, for example, computer operators are called “miners” and each computer competes to validate and add the next set of transactions to the shared ledger. The winning computer earns a fee in the form of bitcoins. So that’s one part of token economics—using tokens to reward strangers from all over the world to operate software and to store a copy of the distributed ledger.

Tokens are also used for governance. Many Web3 applications have completely decentralized governance through a *decentralized autonomous organization* (DAO). A DAO is a software program that runs an entire organization automatically based on codified rules. The idea of a DAO is to create a completely independent entity that is exclusively governed by the rules that everyone can see. Holders of governance tokens vote on decisions.

Token economics also applies to many asset classes. Digital tokens can represent fungible assets, like bitcoin or digital versions of fiat currencies

(called stable coins). Digital tokens can represent unique assets, called non-fungible tokens (NFTs), like artwork or an event ticket. Digital tokens may be transferable to others, such as trading NFTs. Digital tokens may be non-transferable, like tokens that represent credentials (e.g., a university diploma) or voting rights. Non-transferable tokens are sometimes called “soul bound” tokens because they are tied to a single person.

WEB2 AND WEB3 APPLICATION EXAMPLES

In this section, we learn how any user can earn digital tokens by watching online advertisements, making loans, selling land in a metaverse, and renting excess computer storage.

We examine four examples of Web2 and Web3 applications. For web browsing, Chrome is a Web2 version and Brave is a Web3 version. For borrowing and lending, traditional banks use a Web2 model and Aave is a Web3 version. For metaverse, Meta is a Web2 version and Decentraland is a Web3 version. For file storage, Dropbox is a Web2 version and Filecoin is a Web3 version. The first three decentralized applications are deployed on Ethereum: Brave, Aave, and Decentraland. We also cover Filecoin, which uses a different decentralized platform, to show that Ethereum is not the only decentralized platform in use. Since most people are familiar with Internet search engines for web browsing, we begin this section by comparing Google’s Chrome (a Web2 application) with the Brave Browser (a Web3 application).

Web Browsing: Chrome vs. Brave

Web2’s Chrome. Google’s Chrome is a Web2 application for web browsing. Released in 2008, users access Chrome for free. Google monitors user activity and applies AI to target advertisements presented as search results. In 2022, advertisers paid Google over \$162 billion for placing ads in search results (Oberlo, 2023).

Web3’s Brave. In contrast to Chrome, the Brave web browser shifts a high percentage of advertising revenues from a centralized platform provider to individuals. Brave blocks all advertising and web tracking to protect privacy, but users can activate a feature that directly compensates them for watching ads online. Users can earn *basic attention tokens*, called

BAT. After downloading and configuring the Brave browser, the user can earn BAT for clicking on a webpage, worth about USD 0.02 in June of 2023. While this is small, it quickly adds up to create seeds of disruption.

When a user watches an advert, 70% of the BAT that the advertiser credited to the application is transferred to a user's digital wallet and 30% goes to Brave Software, the company that maintains the platform. The only thing stored on Ethereum's public ledger is the advertiser's public key address (debit), the individual's public key address (credit), Brave Software's public key address (credit), and the amount coming from and going into these addresses.

By July 2023, Brave had over 58 million active monthly users and advertisers from 187 countries (Brave.com/transparency), which was about 2% of Chrome's user base. In 2021, the *New York Times* rated the Brave web browser as the best privacy browser (Chen, [2021](#)).

Borrowing and Lending: Traditional Bank vs. Aave

Readers are familiar with how to access banking services online. We've already discussed that banks control the software and databases that record our money transactions. Let's look closer at lending money to and borrowing money from a traditional bank.

Web2's borrowing and lending with a traditional bank. Lenders deposit money in a bank in return for earning interest, but the interest rates they earn on deposits are paltry. In May of 2023, the US national bank average for interest payments on savings accounts was only 0.36% (Bond, [2023](#)). If you deposit \$1000 in a savings account, after a year, you will only earn \$3.60 cents in interest! So why do it? Some depositors like to keep cash on hand in case of emergencies, and a bank is a relatively safe bet. In the US, banks must be insured by the Federal Deposit Insurance Corporation (FDIC) to get a bank charter. The FDIC insures an account holder up to \$250,000 per insured bank. So, from a lender's perspective, traditional banking services offer a relatively safe place to deposit money, but the financial returns are small.

Banks use our deposits to loan money to borrowers. Borrowers pay relatively high interest rates to the bank. In July of 2023, the average borrowing rate was 6.95% (Bankrate, [2023](#)). If a borrower borrows \$1000 for one year at 6.95%, the borrower will pay the bank \$69.50 in interest. The difference between what the bank pays to depositors

and receives from borrowers is called the spread. In our little scenario of depositing and borrowing \$1000 for one year, the spread is huge!

Banks loan out more money to borrowers than they retain in deposits. It's called fractional reserve banking and it is allowed because it helps to expand the economy. But there are risks! If a large portion of depositors suddenly demand their money back in cash, the bank could go bankrupt. It's called a run on the bank, and the history of banking is littered with them. Additionally, borrowers may default on their loans, which happened in droves during the 2008 Global Financial Crisis (Lacity & Lupien, 2022).

Web3 applications for finance, called Decentralized Finance (DeFi), work differently. They require 100% (or more) in reserves, meaning the DeFi application cannot loan out more money than it keeps in reserves. DeFi applications are also non-custodial, meaning that only the users can move funds, i.e., there is no central company or government that can lock users out or deny them access to their assets.

Web3's Aave. Aave is an example of pure DeFi—it is a completely decentralized set of applications that deals only in cryptocurrencies. All decisions are programmed (no human mortgage broker) and the software is published so people can be confident the system is processing transactions as expected. Aave allows lenders to earn interest on their cryptocurrency deposits and enables borrowers to take out cryptocurrency loans. No PII is needed; a user just sends or receives digital tokens from their digital wallet to an Aave liquidity pool address to loan or borrow money.

The CEO and founder of Aave was a Finnish law student who became fascinated with how Ethereum could be used to disrupt traditional finance. Aave, originally called ETHLend, launched in 2017 on the Ethereum platform. On July 7, 2023, Aave had \$8.6 billion worth of crypto deposited (see <https://aave.com/>).

Loaning rates varied from 0.01% to 2.77%; borrowing rates varied from 0.61% to 3.97%. The company, also called Aave, makes money from a small percentage of a loan, about 0.09% (de Isidro, 2023). The spread is much smaller with DeFi than with traditional banks.

Like many Web3 applications, Aave is governed by a community through a DAO. Holders of AAVE governance tokens may vote upon Aave Improvement Protocols (AIPs). AIPs are published on GitHub (<https://github.com/aave/aip>). AAVE tokens can also be staked to the

safety module to provide a type of deposit insurance. As another example of token economics, individuals who stake AAVE tokens earn rewards and fees (Lacity & Lupien, 2023).

Aave is just one of many DeFi applications. Readers are also encouraged to investigate Uniswap, Chainlink, SushiSwap, PancakeSwap, and Maker. On July 7, 2023, the total DeFi market was worth \$41 billion (see <https://www.tradingview.com/>).

Metaverse: Meta vs. Decentraland

For our third side-by-side comparison of Web2 and Web3 applications, we examine metaverse. A metaverse is computer-generated environment one visits with an *avatar*, a digital representation of ourselves (see Fig. 6.3b for Mary Lacity's Decentraland avatar). A metaverse is an immersive experience, particularly when users access the virtual world with virtual reality (VR) headsets.

Future generations may earn most of their income and spend much of their money in the metaverse. New jobs will emerge, such as virtual real estate agents, virtual fashion designers, virtual security guards, virtual teachers, and others we cannot yet envision (Lacity et al., 2023b).

As the metaverse potentially evolves into one interoperable meta-universe, we must seriously question who we trust to operate it. Do



Fig. 6.3 Web3 applications—Decentraland: **a** Location of British Blockchain Association (BBA) in Decentraland metaverse, located at (24, -28); **b** Mary Lacity's avatar visits the BBA in Decentraland (*Image credit* The authors)

we trust one or a few centralized platform providers to create, control, and govern the access, digital assets, and transactions via privately owned infrastructure and databases (Web2)? Or do we trust decentralized crowds to create and govern the metaverse (Web 3)? Web3 metaverses aim to protect privacy better than Web2 metaverses.

Web2’s Meta. Worldwide interest in metaverse escalated in October 2021 when Facebook’s CEO, Mark Zuckerberg, announced that Facebook was changing its name to Meta. In the video announcement, Zuckerberg said, “I believe the metaverse is the next chapter for the Internet.” Zuckerberg had been investing in metaverse prior to this announcement. Facebook bought Oculus, the company that built the Oculus Rift VR headsets, in 2014 for \$2 billion. At the time, Facebook promised Palmer Luckey—the creator of Oculus Headsets, that Facebook would not introduce advertisements (ads) on Oculus headsets, but Facebook did introduce ads in 2021 (O’Flaherty, 2021).

Meta’s latest Quest VR headsets collect a massive amount of PII on hand movements, eye movements, facial expressions, audio data, payments, places visited, and Meta keeps user-generated content such as photos and videos. Readers are encouraged to read Meta’s “privacy” policy.⁴

Web3’s Decentraland. Decentraland is a virtual world launched on Ethereum network in 2017. Unlike Meta’s metaverse applications that are accessed with virtual reality headsets, users access Decentraland with a web browser, so the user experience is less rich. It is, however, privacy enhancing.

To enter Decentraland, a user must first create an avatar; a user decides the amount of PII to reveal through their choices of designing and naming their avatar. Once an avatar is ready, the user is free to explore the different plots of land.

A location in Decentraland is depicted as an (x, y) coordinate on the map of the entire space. The center square is at address (0, 0). Figure 6.3a shows the address for the plot of land owned by the British Blockchain Association (BBA), on plot (24, -28). The BBA built a two-story building on its plot of land. Mary Lacity’s avatar is “inside” BBA’s building in Fig. 6.3b.

⁴ See “Supplemental Meta Platforms Technologies Privacy Policy”, <https://www.meta.com/legal/quest/privacy-policy/>.

If users want to transact in Decentraland, they need a digital wallet and some of Decentraland's token called MANA. Anyone can buy virtual plots of land with MANA. However, virtual plots of land near the town center can cost over \$2 million worth of MANA (Howcroft, 2021). Users can buy and sell virtual goods and services with MANA; transactions are stored on Ethereum. Decentraland has completely decentralized governance through a DAO.

What kind of metaverse will we create? Web2 has the advantage of a clear path to revenues and it's hard for Web3 communities to compete with Meta's \$10 billion investment in metaverse. Because of the deep funding, Meta's VR applications provide vastly more immersive three-dimensional experiences compared to Decentraland's two-dimensional experiences. As Forbes contributor Alison McCauley writes, "Web3 communities are still looking for business models that reduce the cost of decentralization, which inherently shifts the expense of the network to the people who use it" (McCauley, 2022).

If privacy is our aim, however, Web3 metaverses are superior. Web3's metaverses share the vision of individuals owning and monetizing their identities (via avatars) and digital assets; of freely coming and going across virtual worlds; of securely executing transactions peer-to-peer with low transaction fees, of having a voice in the governance of the applications; and protecting the privacy of all (Lacity et al., 2023b).

File Storage: Dropbox vs. Filecoin

Today, most readers use a cloud-based file hosting service, such as Dropbox, Box, Google Drive, or Microsoft OneDrive. These Web2 cloud services allow users to upload files that can be accessed from any device over the Internet after providing a username and password (and perhaps another authentication method). As with all Web2 applications, the centralized platform providers control the software and data. Let's compare Dropbox (a Web2 application) with Filecoin (a Web3 application).

Web2's Dropbox. Dropbox Inc. is the company that built and operates Dropbox. Founded in 2007 in San Francisco California, it grew to one million users by April of 2009. Today, Dropbox has over 700 million users, many which use Dropbox for free. Dropbox Inc. earns about \$2 billion in annual revenues for users who pay fees for additional storage.

Depending on the amount of storage needed, Dropbox costs about \$10 a month for up to 2 terabytes of data storage (<https://www.dropbox.com/plans>).

Who can see your files on Dropbox? According to the Dropbox website, “Like most major online services, Dropbox personnel will, on rare occasions, need to access users’ file content (1) when legally required to do so; (2) when necessary to ensure that our systems and features are working as designed (e.g., debugging performance issues, making sure that our search functionality is returning relevant results, developing image search functionality, refining content suggestions, etc.); or (3) to enforce our Terms of Service and Acceptable Use Policy” (<https://help.dropbox.com/security/file-access#>). Here again, users are relying on trust placed in a centralized platform provider to refrain from viewing/using their private content, even though technically Dropbox Inc. can view all content.

Web3’s Filecoin. Most of us have excess storage capacity on our computers. What if we could get paid for renting out excess computer storage? That’s the question answered by Protocol Labs, the founder of Filecoin. After six years of development and testing, Filecoin was launched in October of 2020. According to Filecoin’s website, “With Filecoin, anyone can participate as a storage provider, monetize their open hard drive space, and help store humanity’s most important information.” The main benefits of Filecoin are low costs, data resilience, and censorship resistance. (Peaster, 2023).

As with all Web3 applications, users need a digital wallet to connect to the Filecoin network. Instead of Ethereum, Filecoin uses the Interplanetary File System (IPFS) as its decentralized platform. IPFS was launched in 2015 by Protocol Labs. As of June 2023, there were nearly 500,000 computers in the IPFS network (Peaster, 2023).

Storage renters and storage providers enter into deals; they find each other on the decentralized filecoin marketplace. Storage renters pay a small fee in the form of filecoins to storage providers. It costs about the equivalent of \$0.38 per month for 2 terabytes of data storage—which is much cheaper than Dropbox (Qian, 2023). Storage renters encrypt data before sending it so that the storage provider cannot read the contents. How can a storage renter trust a storage provider? Each deal is posted to the distributed ledger, while other computers in the network constantly verify that storage providers are storing files correctly.

CONCLUSION

To recap, this chapter has shown that IS researchers have found a privacy paradox: individuals are deeply concerned about information privacy, yet they routinely disclose PII to centralized platform providers. We covered four explanations of the privacy paradox: (1) privacy calculus where individuals weigh privacy concerns and risks against the benefits of disclosing PII; (3) privacy fatigue where individuals are emotionally exhausted from trying to protect PII; (4) trust in the centralized platform provider that encourages users to disclose PII; and (4) a lack of user choice—individuals must disclose PII as required by the centralized platform provider—or they cannot access the services. All of these explanations pertain to Web2 applications, where centralized platform providers govern the software and data.

Next, we introduced readers to Web3's privacy enhancing approach to online applications. With Web3 applications, users can transact anonymously, meaning individuals can choose to be totally anonymous, pseudonymous, or identifiable. We compared Web2 and Web3 versions of web browsing (Chrome vs. Brave), borrowing and lending (traditional bank vs. Aave), metaverse (Meta vs. Decentraland), and file storage (Dropbox vs. Filecoin). We showed that the Web3 versions are superior in terms of protecting privacy.

While our four Web3 application examples focused on anonymity, many services require *confidentiality*, meaning that data needs to be viewable by authorized parties. Modern life necessitates that we *prove* our identities and credentials to others for jobs, airline tickets, border crossings, driver's licenses, apartment rentals, banking, and more (Cameron, 2005). Web3 applications can accommodate confidential transactions on public decentralized platforms, but it requires learning more concepts such as decentralized identifiers, verifiable credentials, and zero knowledge-proofs, which are beyond the scope of this chapter. If these Web3 technologies become widely adopted, we will be able to replace our physical wallets with digital wallets that contain digital versions of our credit cards, memberships, licenses, and other credentials. We will possess and control who sees our digital credentials, which will be another milestone in protecting information privacy (Lacity et al., 2023c).

REFERENCES

- Ackerman, M. (2004). Privacy in Pervasive Environments: Next Generation Labeling Protocols. *Personal and Ubiquitous Computing*, 8(6), 430–439.
- AICPA/CICA. (2020). Privacy Management Framework. Issued by the *Information Management and Technology Assurance Executive Committee*. Retrieved June 3, 2023 from <https://www.aicpa-cima.com/resources/download/privacy-management-framework>
- Allan, D. (2015). We All Have Too Many Online Accounts—And Can't Remember the Passwords. *ITProPortal*. Retrieved July 10, 2021 from <https://www.itproportal.com/2015/07/23/we-all-have-too-many-online-accounts-and-cant-remember-the-passwords/>
- Allen, C. (2016). The Path to Self-Sovereign Identity. Retrieved July 12, 2021 from <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- American Airlines. (2021, May 20). Press Release. Retrieved July 11, 2021 from <https://news.aa.com/news/news-details/2021/American-Airlines-Customers-Can-Now-Choose-Convenient-Vaccine-Verification-Option-in-VeriFLY-OPS-DIS-05/default.aspx>
- Aten, J. (2019). Google Is Absolutely Listening to Your Conversations, and It Confirms Why People Don't Trust Big Tech. *Inc. Magazine*. Retrieved June 27, 2023 from <https://www.inc.com/jason-aten/google-is-absolutely-listening-to-your-conversations-it-just-confirms-why-people-dont-trust-big-tech.html>
- Bankrate. (2023). Compare Current Mortgage Rates for Today. Retrieved July 11, 2023 from <https://www.bankrate.com/mortgages/mortgage-rates/>
- Bansal, G., Zahedi, F., & Gefen, D. (2015). The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. *European Journal of Information Systems*, 24(6), 624–644.
- Bélanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), 1017–1041.
- Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems*, 11(3–4), 245–270.
- Bond, C. (2023). The Average Savings Account Interest Rate Is (Finally) on the Rise. Retrieved July 11, 2023 from <https://fortune.com/recommends/banking/average-savings-account-interest/>
- Boritz, J. E., & No, W. G. (2011). E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery. *Journal of Information Systems*, 25(2), 11–45.
- Brave.com: Brave's platform statistics and token activity may be found at <https://brave.com/transparency/>

- Cameron, K. (2005). *The Laws of Identity*. Retrieved July 12, 2021 from http://www.ict-21.ch/ICT.SATW.CH/IMG/Kim_Cameron_Law_of_Identity.pdf
- Caruthers, M. (2018). World Password Day: How to Improve Your Passwords. *Dashlane Tech News*. Retrieved July 10, 2021 from <https://blog.dashlane.com/world-password-day/>
- Chainanalysis. (2023). The 2023 Crypto Crime Report. Retrieved July 11, 2023 from https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf
- Chen, B. (March 31, 2021). "If You Care About Privacy, It's Time to Try a New Web Browser". *The New York Times*. Retrieved July 11, 2023 from <https://www.nytimes.com/2021/03/31/technology/personaltech/online-privacy-private-browsers.html>
- Choi, H., Park, J., & Jung, Y. (2018). The Role of Privacy Fatigue in Online Privacy Behavior. *Computers in Human Behavior*, 81, 42–51.
- CNBC. (2021, May 22). Covid Vaccine Passports: Everything We Know So Far. <https://www.cnbc.com/2021/05/22/covid-vaccine-passports-everything-we-know-so-far.html>
- Culnan, M., & Bies, R. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), 323–342.
- Culnan, M., & Clark-Williams, C. (2009). How Ethics Can Enhance Organizational Privacy. *MIS Quarterly*, 33(4), 673–687.
- De Isidro, R. (2023). Aave: The Basics. Global X. Retrieved July 13, 2023 from <https://www.globalxetfs.com/aave-the-basics/#>
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy Calculus Model in E-Commerce—A Study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389–402.
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-commerce Transactions. *Information Systems Research*, 17(1), 61–80.
- Guo, W., Straub, D., Zhang, P., & Cai, Z. (2021). How Trust Leads to Commitment on Microsourcing Platforms: Unraveling the Effects of Governance and Third-Party Mechanisms on Triadic Microsourcing Relationships. *MIS Quarterly*, 45(3), 1309–1348.
- Hern, A. (2019). Apple Contractors ‘Regularly Hear Confidential Details’ on Siri Recordings. *The Guardian*. Retrieved June 27, 2023 from <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings>
- Hopper, A. (2023). Debunking the Myth: Cryptocurrency Is Used for Criminal Activity. *CoinTelegraph*. Retrieved July 11, 2023 from <https://cointelegraph.com/news/debunking-the-myth-cryptocurrency-is-used-for-criminal-activity>
- Howcroft, E. (2021). Virtual Real Estate Plot Sells for Record \$2.4 Million. *Reuters*. <https://www.reuters.com/markets/currencies/virtual-real-estate-plot-sells-record-24-million-2021-11-23/>

- Jarvenpaa, S. L., & Todd, P. A. (1996). Consumer reactions to electronic shopping on the world wide web. *International Journal of Electronic Commerce*, 1(2), 59–88.
- Johnson, B. (2010). Privacy No Longer a Social Norm, Says Facebook Founder. *The Guardian*. Retrieved June 5, 2023 from <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>
- Lacity, M., & Lupien, S. (2022). *Blockchain Fundamentals for Web 3.0*. Epic Books/University of Arkansas Press, Fayetteville Arkansas.
- Lacity, M., Schutz, S., Kuai, L., & Steelman, Z. (2023a). *IT's a Matter of Trust*. Blockchain Center of Excellence, University of Arkansas Research Paper Series.
- Lacity, M., Mullins, J., & Kuai, L. (2023b). Evolution of the Metaverse. *MIS Quarterly Executive*, 22(2), 165–172.
- Lacity, M., Carmel, E., Young, A., & Roth, T. (2023c). The Quiet Corner of Web 3 That Means Business. *Sloan Management Review*, 65(1) (Spring Issue).
- Lacity, M., Schuetz, S., Kuai, L., and Steelman, Z. (2024). It's a matter of trust: Literature reviews and analyses of human trust in information technology. *Journal of Information Technology*, 39(2), 1–35.
- Li, H., Luo, X., Zhang, J., & Xu, H. (2017). Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors. *Information & Management*, 54, 1012–1022.
- Liu, B. (2023). Ethereum Hits 500,000 Validator Milestone. *Blockworks*. Retrieved July 4, 2023 from <https://blockworks.co/news/ethereum-to-reach-500000-validators>
- McCauley, A. (2022, March 22). The Battle For Control of the Metaverse: Can Open Innovation Outrun Corporate Domination? *Forbes*. Retrieved May 11, 2022.
- McMillan, R. (2012). The World's First Computer Password? It Was Useless Too. *Wired Magazine*. <https://www.wired.com/2012/01/computer-password/>
- Mitchell, D., & El-Gayar, O. (2022). Privacy and Online Social Networks: A Systematic Literature Review of Concerns, Preservation, and Policies. *Pacific Asia Journal of the Association for Information Systems*, 14(4), 1–25.
- Mosteller, J., & Mathwick, C. (2014). Reviewer Online Engagement: The Role of Rank, Well-Being, and Market Helping Behavior. *Journal of Consumer Marketing*, 31(6/7), 464–474.
- Mosteller, J., & Poddar, A. (2017). To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors. *Journal of Interactive Marketing*, 39, 27–38.

- Nahra, K., & Evers, A. (2023). FTC Announces Enforcement Actions Against Amazon's Alexa and Ring Divisions for Violations of User Privacy. *Wilmerhale Law*. Retrieved June 27, 2023 from <https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20230606-ftc-announces-enforcement-actions-against-amazons-alexa-and-ring-divisions-for-violations-of-user-privacy>
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved July 16, 2023 from <https://bitcoin.org/bitcoin.pdf>
- Oberlo. (2023). How Does Google Make Money? Retrieved June 28, 2023 from <https://www.oberlo.com/statistics/how-does-google-make-money>
- O'Flaherty, K. (2021). Facebook Just Gave 1 Million Oculus Users a Reason to Quit. *Forbes*. <https://www.forbes.com/sites/kateoflahertyuk/2021/07/04/facebook-just-gave-1-million-oculus-users-a-reason-to-leave/?sh=417e22bf76f5>
- O'Neill, O. (2006). *A question of trust. Transcript from BBC radio.* https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/BBC_UK/B020000O.pdf
- Pavlou, P. (2011). State of Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, 35(4), 977–988.
- Peaster, W. (2023). NFT Storage: Comparing IPFS, Filecoin, and Arweave. Metaversal. <https://metaversal.banklesshq.com/p/nft-storage>
- Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison. *Computers in Human Behavior*, 65, 409–419.
- Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Manning Publications.
- Rath, D., & Kumar, A. (2021). Information Privacy Concern at Individual, Group, Organization and Societal Level—A Literature Review. *Journal of Management*, 18(2), 171–186.
- Schuetz, S., Kuai, L., Lacity, M., & Steelman, Z. (2023). *A Qualitative Systematic Review of Trust in the IT Artifact* (University of Arkansas Working Paper).
- Sharma, N. (2017). *Is Quantum Computing an Existential Threat to Blockchain Technology?* <https://singularityhub.com/2017/11/05/is-quantum-computing-an-existential-threat-to-blockchain-technology/-sm.00009y4jmx95sdw-w11rov5gdjdlzo>
- Smith, H., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989–1015.
- Techtarget.com. Cryptography. Retrieved July 16, 2023 from <https://searchsecurity.techtarget.com/definition/cryptography>

- Tian, X., Chen, L., & Zhang, X. (2022). The role of privacy fatigue in privacy paradox: A PSM and heterogeneity analysis. *Advanced Technologies in Data and Information Security*, 12(19). <https://doi.org/10.3390/app12199702>
- Qian, L. (2023). Centralized vs Decentralized Storage Cost. *CoinGecko*. Retrieved July 10, 2023 from <https://www.coingecko.com/research/publications/centralized-decentralized-storage-cost>
- United Nations. (2023). *Money Laundering*. Retrieved July 11, 2023 from <https://www.unodc.org/unodc/en/money-laundering/overview.html>
- US Bureau of Justice Statistics. (2021). Victims of Identity Theft. Retrieved June 28, 2023 from [https://bjs.ojp.gov/library/publications/victims-ide ntity-theft-2018](https://bjs.ojp.gov/library/publications/victims-identity-theft-2018)
- van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online Privacy Fatigue: A Scoping Review and Research Agenda. *Future Internet*, 15, 1–31.
- VanMeter, R. A., Grisaffe, D. B., & Chonko, L. B. (2015). Of ‘Likes’ and ‘Pins’: The Effects of Consumers’ Attachment to Social Media. *Journal of Interactive Marketing*, 32, 70–88.
- World Economic Forum. (2020). Presidio Principles Foundational Values for a Decentralized Future. Retrieved July 13, 2021 from http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf
- W3C. (2020). Decentralized Identifiers (DIDs) v1.0. Retrieved on July 12, 2021 from <https://www.w3.org/TR/did-core/>
- Zalmanson, L., Oestreicher-Singer, G., & Ecker, Y. (2022). The Role of Social Cues and Trust in User’s Private Information Disclosure. *MIS Quarterly*, 46(2), 1109–1133.
- Zhang, N., Wang, C., Karahanna, E., & Xu, Y. (2022). Peer Privacy Concern: Conceptualization and Measurement. *MIS Quarterly*, 46(1), 491–530.
- Zhu, M., Wu, C., Huang, S., et al. (2021). Privacy Paradox in mHealth Applications: An Integrated Elaboration Likelihood Model Incorporating Privacy Calculus and Privacy Fatigue. *Telematics and Informatics*, 61, 1–15.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Public Affairs.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 7

Multi-party Computation: Privacy in Coopetition

Daniel Conway and Kiran K. Garimella

INTRODUCTION

In matters of love and war, all is fair. The centuries-old saying suggests that rules of fair play only apply to the space in between love and war, a space we refer to as “coopetition.” Coopetition is a portmanteau of two words—*cooperation* and *competition*. Coopetition recognizes that firms have complex interdependencies. In some realms, firms that compete for market share also cooperate to achieve mutual benefits (Dagnino & Padula, 2002). These rules of play are often established externally to ensure a fair game and take the guise of laws, regulations, and policy.

There are many reasons, however, why an occasional effort in collaboration might be beneficial to members of a particular industry group. All automobile companies promote large highway spending bills. Standards

D. Conway (✉)
University of Arkansas, Fayetteville, AR, USA
e-mail: DConway@walton.uark.edu

K. K. Garimella
University of South Florida, Tampa, FL, USA
e-mail: kgarimella@usf.edu

making bodies exist to ensure interoperability of competing products. Companies who both compete and cooperate comprise supply chains. Complicated organizations often find some units competing with other organizations and some units cooperating. As an example, Amazon and Netflix compete on video content, but Netflix servers run on the Amazon cloud. Fraternizing with the enemy? The reality is more complicated than that.

War is a zero-sum game (at best), in which one person's gain is equal to another person's loss. Love is a plus sum (sum+) game. With love, two parties can achieve a state where they exceed their individual potential. The question remains: can competing organizations achieve a higher outcome (sum+) by leveraging forms of cooperation which preserve their competitive advantage as well as protect their data from roaming or being misused? This is where Multi-Party Computation (MPC) plays, where new information is created while preserving the privacy of an organization's data. It contributes to the "+" in sum+.

TWO-PARTY COMPUTATION

We illustrate MPC with a series of examples that can be done manually.

Four faculty members agree to meet for coffee after a term ends to talk over their experiences. Two parties arrive early and start discussing matters. After some small talk, the faculty members Alice and Bob are curious as to who they are going to elect as department chair in the following year. Neither want to state their preference, but they are curious as if they agree who would be best. The question then is, how could they determine they agree or not without telling the other whom they favor?

The simple answer would be to have the barista serve as a trusted third party. Alice and Bob could write their preferences on a slip of paper hidden from each other and the barista could look over the two submissions and determine if they were the same or not. After some discussion, Alice and Bob decided that they didn't like that idea, as the barista might disclose the preferences to another employee, who was the daughter of faculty member Carol.

While the barista said he would not disclose the data to the other party, he had another suggestion. He laid out four coffee cups on the table in a line and said they would represent faculty members Alice, Bob, Carol, and David going north to south. They would then be given four scraps of paper, and on three of them they would write "no" and on one of them

they would write “yes.” The papers were folded so the other could not see the selection. Alice and Bob voted with a “yes” in one cup and placed their “no” vote in each of the other cups.

Next, Bob turned away from the table and Alice scrambled the cups in the line. After getting the all-clear, Alice turned away from the table and Bob scrambled the cups in the line. Finally, both Alice and Bob faced the table. They started at the top and opened the two papers in each cup. If a cup held two “no” scraps, they went on. If a cup held two “yes” scraps, then they knew they agreed. If two cups held “yes” and “no” scraps, then they concluded that they were not in agreement. If Alice and Bob had decided that they couldn’t vote for themselves, the solution of two-yes papers would reveal if they did.

In this case, Alice and Bob were able to determine that they didn’t favor the same candidate without either disclosing their private information. They repeated it to determine if there was a candidate who they thought would be a poor candidate for department chair, and, in this case, they agreed. They both smiled and acknowledged that David was a poor choice, one whom they each secretly expected to be 15 minutes late, without having mentioned David by name or referring to any reasons.

In essence, Alice and Bob computed a bitwise-AND function. A bitwise-AND function represents an action as a bit with either a “1” or a “0” value. The bitwise-AND function compares the bit of the first operand to the corresponding bit of the second operand. If both bits are 1, the corresponding result bit is set to 1. Otherwise, the corresponding result bit is set to 0. This outcome is logically equivalent to multiplication. Thus, a result of 0 implies no agreement (at least one party chose a 0), and a result of “1” implies agreement (both parties chose 1). With multiple participants, the result would have the potential leaking additional information and thus we would want to use a different computation.

The barista brought them two additional cups for their actual coffee and suggested that there were other calculations that could be done with the shop’s cups. When asked who wanted the check, both stepped up to accept. The barista said they would have plenty of time to determine how to break the tie, and suggested Andrew Yao’s millionaire problem (1986) as a potential solution. In that problem, two millionaires are having dinner and they decided that the wealthiest of the two would pay the bill. The problem was to compute the inequality without either diner stating their net worth.

As faculty at State U, salaries were already public, so both knew that Alice had the higher salary. But they decided that the person with the highest teaching evaluations in the prior term would pay for the coffee. The experiment would require the four cups, but this time cups would represent ranges of the evaluation scores. The first cup (from the north) was 4.0. If Alice had evaluations above 4.0, then she would put a “>” on a scrap of paper and place it in the first cup folded. If her evaluations were below 4.0, then she would put a “<” on the folded scrap of paper and place it in the cup. The second cup represented 4.25. Similarly, if Alice had evaluations less than 4.25, she would write a “<” on the second scrap of paper, otherwise she would put a “>” on the scrap of paper. Alice would repeat this for cups 3 and 4 with boundaries 4.5 and 4.75.

Bob then would use the previous “yes” and “no” scraps and place them into the cups based on the ranges. “Yes” would go into the range where his evaluations landed. The cups would be scrambled as before and then the scraps read. As an example, if Alice had average student evaluations of 4.4, then the comparisons would be “>,” “>,” “<,” “<,” meaning “ >4 ,” “ >4.25 ,” “ <4.5 ,” and “ <4.75 .” Say Bob had average evaluations of 4.6. Then the cups would hold “no,” “no,” “yes,” and “no,” meaning “not $x < 4.25$,” “not in the range of $4.25 < x < 4.5$,” “yes in the range of $4.5 < x < 4.75$,” “not in the range of $4.75 < x < 5.0$.” The scrambling left the information of {“yes,” “<”}, indicating that the range where Bob chose, Alice had “<.” Thus, we would conclude that Bob had higher evaluations than Alice, again without Alice nor Bob giving their actual value. Bob is buying coffee this morning.

After narrating the two examples, we see a couple of important considerations emerge if this were to be implemented on a digital computer. One is that the parties must be honest for the calculated value to be interpreted as meaningful. In general, MPC favors environments where the parties are incentivized to play honestly. There are many extensions though that give meaningful results if at least fifty-one percent of the participants are honest. We save those variations for the ambitious reader.

Also, if the ranges are too wide, the barista would need to bring more cups so that the experiment can use more narrow ranges.

MULTI-PARTY COMPUTATION—MEAN

Carol and David arrive for coffee, with Carol mentioning that David was late picking her up. Alice and Bob describe what they have been doing, and Carol and David are keen to participate in order to regain eligibility for the bill. They first discuss the recently announced merit bonuses of \$1000 to \$5000 per faculty member. The group wondered if everyone received \$1000 or if the mean were closer to \$2500 or higher. Technically the average could be anywhere from \$1000 to \$5000 depending on how the merit bonuses were distributed. Naturally, no one wanted to share their actual bonus. Instead, they would calculate the mean without anyone sharing their actual bonus, which is the input to the function.

The barista suggested a way to calculate this, which required each person to have a clean cup as well as several scraps of paper. First, for each party Alice, Bob, Carol, and David, they would generate three random numbers and then calculate the fourth so that each person's four numbers add up to their individual bonuses. (Table 7.1 shows their actual bonuses). Obviously, the random numbers would have to be in an appropriate range, but they can choose their own range. Then, each party would have a cup to receive folded papers. Alice would give one of her random numbers to Bob, Carol, and David and hold one back in her cup. Bob would give each of the random numbers to Alice, Carol, and David and hold one back in his cup. Carol and David would each do the same.

Upon receiving the random numbers from the other parties, each would then calculate the sum of the values in their cup and share that sum with the group. The overall sum would represent the sum of the bonus and dividing that by 4 would result in the average bonus.

As an example, say these are the actual bonuses for the four parties, which are not shared (held privately). The average is of course $\$11,000 / 4 = \2750 . But no one knows all four numbers to start, so there is no way to calculate this.

Table 7.1 Faculty bonuses

<i>Party</i>	<i>Bonus</i>
Alice	\$3000
Bob	\$4000
Carol	\$3000
David	\$1000

Table 7.2 Three random numbers plus a calculated number to equal the bonus

Party Secret	#1	#2	#3	#4
Alice \$3,000 =	56	410	741	1793
Bob \$4,000 =	867	670	1303	1160
Carol \$3,000 =	49	416	96	2439
David \$1,000 =	229	205	296	270

The parties calculate their three random numbers, as shown in Table 7.2. The number in the box represents the number they put in their own coffee cup.

The columns then are the numbers that get moved to the peer's cups. So, Alice receives {867, 49, 229} to put along with the number she held back (56). The sum of these numbers is 1201. Similarly, Bob receives the numbers in #2 {410, 416, 205} along with the number he put in themselves (670) for a sum of 1701. Carol has column #3 with a sum of 2435, and David has a sum of 5662. Each party adds up the columns and broadcasts their own sums of 1201, 1701, 2435, and 1701, which sum to \$11,000, and thus the average is \$2750. There is muted happiness that the average is above \$2500, which would represent equally likely bonuses between \$1000 and \$5000.

David notes that calculating a mean has a lot of applications, observing that he had built a trusted third-party application to do a similar thing. Several private equity companies wanted to know if they were pricing private bonds similarly to the industry, however, there was no market to share prices due to legal restrictions. They weren't particularly concerned about knowing the exact prices set by others; their primary interest was in assessing whether their prices consistently deviated from the industry average, either higher or lower. This seemed a perfect application for MPC, since their pricing data would remain private while they would be able to calculate the overall average and internally determine if they were constantly deviating from the others.

MULTI-PARTY COMPUTATION—STANDARD DEVIATION

The four parties were curious if everyone received the same bonus amount or close to the same amount, or if there was significant variance in the bonuses. After ordering another round of coffees and asking for more scraps of paper, the barista suggested that the population variance could be computed as the average deviation from the mean. As they all knew the mean, they could repeat the experiment using the deviations rather than the mean.

The population standard deviation of {3000, 4000, 3000, 1000} is 1089.7.

Each party calculates their deviation from the population mean as shown in Table 7.3

Table 7.4 shows the results of squaring the deviations and generating random numbers.

Table 7.3 Faculty member's deviation from the mean bonus

<i>Party</i>	<i>Bonus</i>
Alice	\$3000 – \$2750 = \$250
Bob	\$4000 – \$2740 = \$1250
Carol	\$3000 – \$2750 = \$250
David	\$1000 – \$2750 = -\$1750

Table 7.4 Three random numbers plus a calculated number to equal the deviation from the mean

Party	Secret	#1	#2	#3	#4
Alice	\$62,500 =	8173	5400	16009	32918
Bob	\$1,562,500 =	431007	397867	20561	713065
Carol	\$62,500 =	2565	11585	2203	46147
David	\$3,062,500 =	573341	1589103	591729	308327

Similar to the previous mean calculations, each party sums their column (papers they received in their cups) and the result is {1,015,086 2,003,955 630,502 1,100,457}, which sum to 4,750,000. Dividing that by 4 results in 1,187,500, and the square root of that is 1089.7. The group can determine that there is variance (that everyone didn't get the same amount). Naturally, they then wanted to know who had the biggest bonus. After a danish...

MULTI-PARTY COMPUTATION—MOMENTS OF DISTRIBUTIONS

It is appropriate to discuss here how privacy might be eroded if we were to continue and calculate the skewness and kurtosis of the dataset. Skewness is a measure of symmetry (really a lack of symmetry). A skewness of zero implies perfectly symmetric; a positive skewness implies that there are outliers to the right; a negative skewness implies there are outliers to the left. Kurtosis is a measure of the tailedness of a distribution as compared with the Normal distribution. Positive kurtosis implies the distribution is tall with skinny tails compared to the Normal distribution, and negative kurtosis implies a distribution is flatter with fatter tails.

Four “moments” or MPC calculation rounds with these types of functions can be used to construct the entire four-point dataset. In general, this is related to the Degrees of Freedom, or pieces of information, in a dataset. We illustrate this with an example.

Consider the four numbers {1, 2, 3, 4}. What if we knew three of the numbers and the sum (or average)? Then we should be able to calculate the 4th number. Convince yourself this is true. If we know {1, 2, 3} and that the sum is 10, then we should be able to calculate that the missing number is a 4. Thus, the sum of 10 and the last number is 4 are the same piece of information—given one, we can calculate the other. By computing the sum, we have not added information. We still have four pieces of information.

Further, what if we calculated the standard deviation of the four numbers to be 1.118, the skewness to be 0, and the kurtosis to be -1.2. Then we could conclude that the following contained the same information, and given any of the five options, we could calculate the others.

- (a) {1, 2, 3, 4}
- (b) {any three} plus {sum is 10}
- (c) {any two numbers} plus {sum is 10, standard deviation is 1.118}
- (d) {any one number} plus {sum is 10, standard deviation is 1.118, skewness is 0}
- (e) {sum is 10, standard deviation is 1.118, skewness is 0, kurtosis is -1.2}.

In essence, MPC reverses this. Each party has one piece of information and represents it as three random numbers (no information) and one computed number, which is not distributed. Sending random numbers to each other is akin to sending encryption keys, so the distribution of these numbers should be secret. (MPC is often used for this purpose.) Upon receiving the random numbers, the withheld number is added, which serves to randomize it. Thus, no degree of freedom (piece of information) ever crosses the network.

Of course, there are potential weaknesses. Consider the case where David decides to share his bonus with Carol. Now Carol is in step (c) above. She has 2 degrees of freedom. In order to know all four bonus values, she only needs to understand the sum (or average) and standard deviation, whereas everyone else is in state (d). Thus, performing more MPC, combined with parties sharing with each other, can weaken the anonymity of the raw data. If none of the P parties share with each other, then we can recreate the entire dataset with P moment calculations using MPC, and the dataset would be separated from the parties' identities.

This can be helpful, as this is a form of anonymizing data. It allows us to recreate entire datasets without knowing the origin of the data. It requires one round of MPC for each moment calculation, so with 1000 data points, we could perform 1000 rounds of MPC and know the entire 1000-point dataset, though we would not know who contributed which point.

MULTI-PARTY COMPUTATION—VOTING

After several cups of coffee, the group of Alice, Bob, Carol, and David now are thinking of many applications where MPC would be appropriate, including anonymous feedback, voting, applications involving signaling, and auctions. In the meantime, the remaining faculty Eve, Frank, Grace, Heidi, Ivan, and Judy, who had been sitting outside the coffee shop,

joined the inside group, and there were now 10 people sitting around several tables. The dynamics have changed with the broader group, and there is less intimacy, but other topics can now be brought up to discuss because the entire department is now present.

Department chair Judy suggested that she has heard that some of the companies recruiting their students are interested in content related to artificial intelligence. Frank knew that Judy wanted to use ChatGPT in class the previous term, but he and Grace, who was not tenured, were uncomfortable with AI and wanted to discourage usage, but they were afraid to say anything. Judy suggested that they vote as to whether they should allow ChatGPT to be used in class, but David suggested that they vote anonymously using MPC.

In the case of computing averages, the random numbers created can be anything that add to 0 or 1, representing no ChatGPT in the classroom (0) or yes ChatGPT in the classroom (1). Then calculating the overall average should give the percent of those who voted yes.

Table 7.5 captures an example. In this case, there are 7 “yes” votes. Random numbers are distributed, and the diagonals are held back for later summation. Alice’s cup contains column #1, and when contributing their number –97, the sum is –236. The sum across the bottom row labeled “ColSum” is 7, which is the number of votes to permit use of ChatGPT.

MPC determined that 7/10 parties agreed, without anyone knowing who voted yes and who voted no.

MULTI-PARTY COMPUTATION—MAXIMUM

Before the group dispersed, Alice suggested that they would like to know if anyone received the highest bonus of \$5000. They had previously determined that not everyone was given the same bonus, but they hadn’t yet calculated the maximum of the group. The barista suggested a way to compute the maximum without anyone giving away their actual value. It would work like the following:

Table 7.5 Nine random numbers and one calculated number for faculty votes

	Vote	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Alice	1 =	-97	85	-92	66	7	-91	-55	65	82	31
Bob	1 =	12	-91	31	-90	57	-33	-42	64	100	-7
Carol	0 =	-18	-24	-52	76	80	78	-29	-98	62	-75
David	1 =	-61	40	88	16	37	-60	-44	47	-26	-36
Eve	1 =	-30	31	32	-32	-15	94	1	-88	99	-91
Frank	0 =	15	65	16	-66	50	82	-54	-35	-90	17
Grace	0 =	-7	-83	0	10	3	91	28	85	-93	-34
Heidi	1 =	54	80	81	-67	-97	38	-54	-18	-32	16
Ivan	1 =	-11	-61	-31	98	74	80	-74	15	-39	-50
Judy	1 =	-93	37	76	44	91	-70	91	57	-52	-180
ColSum		-236	79	149	55	287	209	-232	94	11	-409

1. Each party must represent their bonus amount in binary format (see Table 7.6).
2. Each party chooses the left most bit of the binary representation and has MPC compute an average across the 10 parties.
 - (a) If the average is zero (all parties have a 0), then record a zero for the solution, return to step 2 until the average is >0. Then continue to (b).

Table 7.6 Faculty bonuses represented in the binary numbering system

<i>Party</i>	<i>Secret</i>	<i>Binary</i>
Alice	\$3000	0101110111000
Bob	\$4000	0111110100000
Carol	\$3000	0101110111000
David	\$1000	0001111101000
Eve	\$2000	0011111010000
Frank	\$3000	0101110111000
Grace	\$2500	0100111000100
Heidi	\$1000	0001111101000
Ivan	\$4500	1000110010100
Judy	\$5000	1001110001000

- (b) For each player, if their bit is 1, stay in the game. If their bit is 0, then use all 0's in each round from this point. Return to step 2 until the bits are exhausted.

In this example, the leftmost bits are zero for the parties A through H, and one for parties I and J (Ivan and Judy). Thus, the max solution begins with a “1” as the leftmost bit, as the average >0 . Parties A–H must now participate with zeros until the iteration is complete. Ivan and Judy continue with their actual bits.

MPC continues to the second leftmost bit. Parties A through H must contribute “0,” and Ivan and Judy have zero also. A zero is appended to the temporary solution yielding “10.” The third bit is also all zeros, appending to the temporary solution yielding “100.”

The fourth bit is now calculated as $1/10$, as parties A–H contribute zero, Ivan has a zero, and Judy has a one. At this point, party Ivan must only contribute zeros from now on, and the temporary maximum is now “1001.” Only party Judy will continue, and the temporary solution will build into party Judy’s binary representation after 13 more iterations.

The maximum value of the bonus is 1001110001000 or \$5000. MPC has computed this while keeping the individual bonuses private.

If the group desired a minimum bonus amount, they could repeat the above process where everyone used (\$5000 – individual bonus) and compute the maximum.

Rather than recalculate the highest overall teaching evaluation, Judy said she would pay for breakfast, and the other parties accepted. Judy kept the tip private.

LIMITATIONS AND OTHER APPLICATIONS

While MPC promotes privacy, it is not computationally efficient. With 10 parties, a round of computation to compute the mean requires $10*9 = 90$ peer-to-peer messages in the early round. For the maximum function, there were 16 rounds of 90 peer-to-peer messages (1440) to calculate the 16 averages. For an election with 10,000 voting parties, that is roughly 100M messages to be sent. In a practical application, each message would be encrypted and digitally signed. There are opportunities for improved performance, but essentially the tradeoff is privacy against computational performance.

Obviously, by computing distributional moments, summary statistics such as confidence intervals and common risk metrics can be calculated. In 1987, it was demonstrated that any function could be securely computed (Goldreich et al., 1987). Today there are thousands of applications that use MPC. Below is a list of a few use cases, as well as a list of several domains in which MPC has been used in practice.

1. Privacy-Preserving Machine Learning (Knott et al., 2021): This paper describes the design of CrypTen and measures its performance on state-of-the-art models for text classification, speech recognition, and image classification.
2. Digital Twins (Hörandner & Prünster, 2021): This paper describes how MPC can be used for keeping digital twin data private.
3. Secure Voting (Bermúdez, 2016): This paper presents an online voting architecture based on partitioning the election in small clusters of voters and using a Multi-party Computation algorithm for obtaining voting results from the clusters.
4. Secure Key Exchange (Archer et al., 2018): The paper highlights a number of applications, ranging from securing small high value items such as cryptographic keys, through to securing an entire database.
5. Data Exchange Between Law Enforcement (Treiber et al., 2022): The authors propose a system for lawful information exchange between LEAs using MPC and private set intersection and show its feasibility by giving a legal analysis for data protection and a technical analysis for workload complexity.

6. Privacy-Preserving Blockchain Applications (Wang et al., 2021):

This paper presents an integrated solution to enable privacy-preserving energy storage sharing, such that energy storage service scheduling and cost-sharing can be attained without the knowledge of individual users' demands.

MPC has been used in several other domains (Cramer et al., 2015), including:

- (a) Secure Auctions,
- (b) Secure Financial Transactions,
- (c) Secure Voting,
- (d) Supply Chain Collaboration,
- (e) Fraud Detection,
- (f) Genomic Data Sharing,
- (g) Privacy-Preserving Authentication, and
- (h) Privacy-Preserving Smart Contracts.

MPC functions preserve the privacy of inputs and create information that cannot be obtained otherwise. This information is akin to the “+” of a sum game in coopetition, as the competition would suggest sharing nothing and the cooperation would suggest sharing everything. In the case of MPC, we share nothing but yield information that is of collective value.

REFERENCES

- Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From Keys to Databases—Real-World Applications of Secure Multi-Party Computation. *The Computer Journal*, 61, 1749–1771.
- Bermúdez, J. (2016). A Practical Multi-party Computation Algorithm for a Secure Distributed Online Voting System. ArXiv, abs/1603.04228.
- Cramer, R., Damgård, I., & Nielsen, J. (2015). *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press.
- Dagnino, G., & Padula, G. (2002). *Coopetition Strategy: Towards a New Kind of Interfirm Dynamics for Value Creation*. EURAM 2nd Annual Conference, Stockholm School of Entrepreneurship, Sweden.

- Goldreich, O., Micali, S., & Wigderson, A. (1987). How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. *STOC, 1987*, 218–229.
- Hörandner, F., & Prünster, B. (2021). Armored Twins: Flexible Privacy Protection for Digital Twins through Conditional Proxy Re-encryption and Multi-Party Computation. *International Conference on Security and Cryptography*.
- Knott, B., Venkataraman, S., Hannun, A. Y., Sengupta, S., Ibrahim, M., & Maaten, L. V. (2021). CrypTen: Secure Multi-Party Computation Meets Machine Learning. ArXiv, abs/2109.00984.
- Treibler, A., Müllmann, D., Schneider, T., & Spiecker, I. (2022). Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies. *Proceedings of the 21st Workshop on Privacy in the Electronic Society*.
- Wang, N., Chau, S. C., & Zhou, Y. (2021). Privacy-Preserving Energy Storage Sharing with Blockchain and Secure Multi-Party Computation. *ACM SIGENERGY Energy Informatics Review*, 1, 32–50.
- Yao, A. (1986). How to Generate and Exchange Secrets. *27th FOCS*: 162–167.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 8

Zero-Knowledge Proofs and Privacy: A Technical Look at Privacy

Kiran K. Garimella and Daniel Conway

INTRODUCTION

Data breaches and the digital invasion of privacy seem to have become an inevitable part of daily life. In securing our privacy, we have two formidable tasks: communicating information securely and keeping information secure. The essence of privacy is to keep either the identity, transactions, or data private, ideally all three. Much of the data we exchange is for the purpose of verifying, validating, and proving that people are who they are, that they have what they claim to possess, or can do or have certain abilities.

There are various approaches to privacy, ranging from regulation, education, corporate policies, paying for privacy, physical security, and technology. In this chapter, we cover the technical approach to privacy,

K. K. Garimella (✉)
University of Arkansas, Fayetteville, AR, USA
e-mail: kgarimella@usf.edu

D. Conway
University of South Florida, Tampa, FL, USA
e-mail: dgconway@uark.edu

beginning with the foundations and reviewing an intriguing set of techniques collectively known as zero-knowledge proofs. To stimulate interest in this topic, we define *zero-knowledge proofs* broadly as follows: A zero-knowledge proof (ZKP) is a method by which one party can prove to another that they are who they claim to be, have something, or know something without disclosing the details of their identity, what they have, or what they know. ZKP certainly sounds like an impossibility on the face of it and sounds like a neat trick to pull off. In this chapter, we explain how this trick is made possible through a variety of ingenious techniques.

Because of their ability to prove conclusively without actually disclosing the secret, we expect to see ZKPs become the dominant infrastructural technology that will power all electronic transactions in the future. With the widespread adoption of the ZKP-embedded infrastructure technology layer, applications do not have to engineer ZKP explicitly into their software. The situation is similar to how software developers explicitly do not program the TCP/IP stack from scratch; rather, they rely on the underlying Internet infrastructure, thanks to Dr. Vint Cerf and Dr. Bob Kahn, co-founders of the Internet, who received the ACM A.M. Turing Award in 2004—the Nobel Prize of Computer Science—for their contribution.

The technical approach to privacy through ZKP is not meant to exclude the other approaches, such as regulation and education. Privacy demands a multi-faceted approach. This is similar to automotive safety, where the technical safety of automobiles must be accompanied by clear traffic laws, a social culture where everyone obeys the traffic laws, and the drivers who go through rigorous education in order to operate their vehicles. However, the best drivers who operate their vehicles with full compliance and drive them under sober conditions may still cause accidents. It is the technology of automotive safety that then becomes the differentiating factor. Similarly, the technology ZKP can be a set of powerful guardrails that function not only as enforcers of privacy but also offer the safety net when the other approaches fall short.

SIMPLE ZKP EXAMPLES

In order to mine the depths of cryptography, mathematics, and algorithms of ZKP, a few simple examples will demonstrate that with some ingenuity that it is possible to craft ZKP-like solutions to some interesting problems. Some of them are motivated by games, such as the four scenarios below, and a few by real-world applications.

Leaves in a Tree: Verifying a Secret Power

Consider this dialog between Alice and Bob (the traditional fictitious participants in the roles of prover and verifier used by the cryptographic community):

Alice:	"I have this weird power. I can look at any tree and instantly tell you how many leaves it has exactly."
Bob:	"You mean an exact number, not approximately? Without counting or trying to estimate the number of leaves?"
Alice:	"That's right. Exactly and instantly."
Bob:	"I don't believe it."
Alice:	"You point out a tree to me and I'll tell you exactly how many leaves it has."
Bob, pointing to a tree that's behind her back:	"How about that one?" Alice turns around, looks at it, and says immediately, "That tree has exactly 227,927 leaves."

How would Bob verify her power? Bob can go to that tree and count up the number of leaves. That will take Bob a very long time. Worse, while Bob is counting, some leaves are bound to fall off (it is a bit windy). There is no way Alice will tell Bob the secret of her power.

Alice suggests a method to verify her claim. "Blindfold me, then go up to the tree and remove a few leaves at random from the tree, and put them in your pocket where I can't see them. Then come back and remove the blindfold and I'll tell you how many leaves the tree has remaining."

Bob follows her instructions and removes four leaves from the tree and pockets them. Bob takes care to make sure she doesn't hear him ripping out the leaves. If she then says that the tree now has 227,923 leaves, then there is a strong possibility she has the power. Her response, however, could be a lucky guess. So, Bob repeats this process several times and Alice gets it right every time.

By this procedure, Alice has now demonstrated to you that she has power, but Bob is still in the dark about how exactly she does it.

Where's Waldo?

Suppose you want to play the ‘Finding Waldo’ game with a few friends. (“Where’s Waldo?” is a visual puzzle where people search for the character named Waldo, who is hidden in a detailed, crowded scene.) The first three to spot Waldo get the prize, the first prize going to the one who found Waldo first. The problem with this game is how to prove you found Waldo without actually pointing to Waldo?

One solution is to use a large plain cardboard (or sheet of paper) and cut a small window in the center of it (just small enough to show Waldo’s head without revealing any of the surrounding image). Let’s say you found Waldo. You can place the cardboard on top of the Waldo game-board, positioning the hole on Waldo. Your friends can see Waldo through the hole, but they will not know where Waldo is on the game-board itself. One caveat is that the plain cardboard must be large enough in relation to the Waldo game-board so that the relative positions of each do not convey any knowledge of the orientation of the game-board. This way, you can prove that you found Waldo without giving away his position on the game-board.

Are You Old Enough To Drink?

In many bars, people who look young are required to provide an ID to ensure they are of drinking age. The usual ID that bar patrons provide is the driving license that contains the date of birth. Unfortunately, it also contains other pieces of information that should be sensitive: name and address. An unscrupulous bartender or bouncer could note the address and misuse that information. In fact, the bartender does not need to know the date of birth, just whether the patron is of eligible drinking age or not. Imagine an ID card that has no information on it besides a barcode or a QR code. Assume that the bartender is licensed, his identity has been verified and has a special mobile app keyed to his identity. The bartender scans the person’s ID card (or face) and authenticates himself through a facial recognition scan. The app connects to an authoritative source (regulated service or blockchain—see Chapter 6 for an explanation of blockchain) and responds back with a ‘yes’ or ‘no.’ Indeed, as artificial intelligence (AI) technology becomes better, more prevalent, and safer,

even the mobile app would be unnecessary; walk-through facial recognition technology would be sufficient. The main point is that the bar patron has been verified to be legal drinking age without disclosing his or her actual date of birth.

Proof of Color

Suppose that you want to prove to a color-blind friend (who cannot see red and green colors) that you are not color-blind. Suppose you have two marbles that are identical but differ only in color: one red and one green marble. You want to prove that you can distinguish between them, but you do not want to tell your friend the actual color of the marbles. One way to accomplish this is to have your friend place this ball behind him and switch it with the other hidden ball with 50% probability, bring it forward to show it to you, asking you if he switched the balls or not. You both go through this process a number of times, where each time you have to say if he switched the balls or not. If you were guessing because you could not tell the colors apart, you would be right approximately only 50% of the time, otherwise your score would be 100%. This way, you could prove you have the ability to tell red and green apart, but without revealing the actual colors of the marbles.

Never Write Checks

We must also remember how legacy systems exacerbated the privacy problem, so we can learn how to avoid them in the future. The most egregious of this is the practice of check writing at retail outlets, a practice that is thankfully becoming rapidly extinct. In the 1960s, check writing was the main method of payment besides cash. Checks expose *everything* about the customer: full name, address, phone number, bank name, bank account number, and even the SSN (especially when tellers ask for the SSN to be written in the memo field of the check). Frank Abagnale, a notorious con artist, whose exploits were popularized by the movie “Catch Me If You Can,” took advantage of these security loopholes to steal several million dollars by creating his own near-perfect counterfeit checks and fake identities. After serving time, he became a consultant to the US federal government and became instrumental in several significant changes to the processing of checks and financial transactions. One of the authors met him at a CIO dinner, where he was a keynote speaker

and advised the audience most strongly never to write checks at retail establishments.

In the next several sections, we will review the backdrop of cryptography and its mathematical foundations, then review the technical underpinnings of ZKPs.

CRYPTOGRAPHIC SOLUTIONS

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, it is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

Cryptography serves the dual purpose of communicating secrets in a way to prevent them from falling into unauthorized ears and also preventing unauthorized people from reading secret information. Cryptography plays a key role in the lifecycle of privacy by ensuring that:

- The sending and receiving parties are legitimate
- The medium of communication is secure
- The information is stored in a secure way
- Only authorized parties can unlock and read the information

Communicating Secrets

Cryptography, or ‘secret writing,’ has ancient roots, dating back to the beginning of recorded history. The most famous of ancient cryptography is the Caesar substitution cipher, which involves a simple exchange of letters. By modern standards, this code is very easy to break. Techniques to break substitution ciphers, developed by Al-Kindi during the ninth century, included frequency analysis (Singh, 2000). Leon Battista Alberti, an Italian Renaissance personage, developed a mechanical disk for encryption in the 1460 s and is credited to be one of the fathers of cryptography (Kahn, 1996; Selleri, 2020).

While these were rudimentary by modern standards, they helped secret communications between armies, statesmen, and merchants. The goal of cryptography has never changed since those times but has become the basis for zero-knowledge proofs in modern systems.

Evolution of Cryptographic Proofs

Cryptography has evolved from the simple to the complex, starting with the easily breakable Caesar ciphers to cryptography based on simple mathematical operations, to the more complex foundations modern cryptography through public key cryptography developed by Whitfield Diffie and Martin Hellman in the 1970s (Diffie & Hellman, 1976). Goldwasser, Micali, and Rackoff (Goldwasser et al., 1985) developed the concept of the Zero-Knowledge Proof was developed during the 1980s. Additional sophistication was introduced through the concept of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) in 2012 (Bitansky et al., 2012), which makes verifications of cryptographic proofs computationally efficient, based on the non-interactive version of ZKP (Blum et al., 1988). The field continues to evolve rapidly, with the latest ZKP protocol being zk-STARK, developed in 2019 by Ben-Sasson, et al. (2018).

Characteristics or varieties of cryptographic proofs are transparency, universality, post-quantum security, and programming paradigm. Zk-SNARKs require a trusted setup phase prior to use. A transparent protocol such as zk-STARK, which uses public randomness, does not. This makes zk-STARK open and verifiable by any party since the algorithms are publicly available. This property is highly desirable since many experts (including hackers) can test the system for vulnerabilities, ensuring that the algorithm does not operate with some undisclosed data which, if it were to be disclosed, would compromise its security. Universality in ZKP is the ability to use the same method for multiple types of claims, whether the claim is about identity verification, compliance with securities laws, or other complex transactions. Universality, therefore, makes the system very versatile and applicable to many use cases.

Of particular concern for cryptography professions, and especially so for ZKP adopters, is how secure will their systems be after quantum algorithms become usable. While the current focus is on ZKP mechanisms that are unbreakable using classical computers, there is active research in the area of mathematical proof constructs that would be safe against hacking through quantum computers (Post-Quantum Cryptography, NIST, 2022).

The methodology used to construct ZKPs is known as the programming paradigm. zk-SNARKs, for example, uses the method of arithmetic circuits, where the computations are represented as ‘circuits’ that contain

gates that perform arithmetic operations. Other examples include Boolean circuits (representing mathematical logic), Rank-1 Constraint System (R1CS) where the computations are represented as a system of polynomial equations, traditional programming techniques using procedural languages, and many others. One of these is the Interactive Proof method, which is now being replaced by zk-SNARKs.

TECHNICAL FOUNDATIONS OF ZKPs

This section describes some of the key concepts and terminology of ZKP technology, its foundational characteristics, protocols, and methods.

Key Concepts and Terminology

There are three important parts in the ZKP protocol, namely prover, verifier, and witness. The prover is the party that wishes to convince the verifier that it (the prover) can do something, has something, or knows something, without revealing the details of how it does it, the object or asset it has, or the specific secret. The prover generates a proof that, when verified, validates the truth of the prover's assertion. The prover uses the witness to construct the proof and sends the proof to the verifier. For example, the prover could be a seller of shares in a company or a buyer; both have to prove that they have the shares to sell or the cash to buy without disclosing the exact number of shares or cash, or details of the holding account. The verifier is the party that needs to accept the proof by verifying it. The verifier receives the proof from the prover and attempts to verify the proof by using certain public parameters, processes, or some form of evidence. The verifier then accepts or rejects the proof based on the outcome of the verification process. The witness is some secret data that is known only to the prover that the prover uses to compute the proof.

A full understanding of cryptography and ZKP requires knowledge of many areas of mathematics, such as number theory (modular arithmetic, prime numbers, the discrete logarithm problem), algebra (groups, rings, fields, elliptic curves), computer cryptography (hash functions, random numbers, bit operations), complexity theory (big-Oh notation, NP-complete, and NP-hard theory), probability, statistics, and mathematical logic.

Foundational Characteristics

ZKP protocols must satisfy three important properties: completeness, soundness, and the zero-knowledge property:

- Completeness: An honest verifier will always be convinced by an honest prover when the statement is true.
- Soundness: No dishonest prover can convince the verifier of a false statement.
- Zero-Knowledge: The verifier learns nothing besides the validity of the prover's statement.

Protocols, Algorithms, and Methods

There are two basic methods of communication between the prover and the verifier within the ZKP protocols: interactive and non-interactive. While the fundamental difference is in the method of communication, the method of communication has implications for real-time and high-volume systems.

Interactive protocols require multiple iterations of communication between the prover and the verifier. The prover sends a proof to the verifier or the verifier gives a challenge to the prover. The verifier verifies the proof produced by the prover. The verifier suspects that the correct proof could be a coincidence, and therefore repeats the challenge (or demands proof) multiple times until the verifier is satisfied. The verifier challenges the prover (the person who possesses a secret power of knowing the exact number of leaves in a tree without counting) to provide a count of the number of leaves after the verifier has removed a certain number of leaves without the prover's knowledge. Only several repeated experiments of this type will convince the verifier that the prover indeed has the secret power.

Interactive proofs have two major challenges. First, the proof is not portable or transferable. Another verifier needs to repeat the process all over again. Second, they are not scalable, since both the prover and verifier need to interact over multiple iterations; in real-time systems, such a method of multiple interactions implies almost synchronous communication between the two, similar to multi-factor authentication.

Schnorr's protocol is an example of an interactive ZKP. It is a very clever interactive technique that a prover can use to prove to the verifier

that he or she knows a secret number without revealing it. Below is a very simple example that is not cryptographically secure. This example requires simple exponentiation and modulus arithmetic to understand:

The Setup Phase: In this phase, the prover selects two numbers, a generator g and a modulus p , which should be a very large prime number for cryptographic security. Technically, g should be a primitive root modulo p . The prover calculates a public key, y as follows:
 $y = g^x \text{ mod } p$.

Let us use some simple numbers for ease of illustration.

Suppose the prover's secret number is $x = 6$.

The prover selects $g = 2$, $p = 17$.

The prover calculates the public key, $y = g^x \text{ mod } p = 2^6 \text{ mod } p = 64 \text{ mod } 17 = 13$.

The prover shares the public key $y = 13$ with the verifier.

The Commitment Phase: The prover now 'commits' to using g and p by generating a random number r (not the prover's secret number!). Let $r = 11$.

The prover calculates another number, t as follows: $g^r \text{ mod } p = 2^{11} \text{ mod } 17 = 2048 \text{ mod } 17 = 8$.

The prover gives the commitment number $t = 8$ to the verifier.

Note that the prover only committed to using g and p , which the verifier also knows, but the prover has not shared the secret number ($x = 6$) with the verifier.

The Challenge Phase: The verifier now challenges the prover by generating a different random number, c . Suppose $c = 2$ (a small number just for illustration). The verifier gives the challenge number ($c = 2$) to the prover.

The Response Phase: The prover uses the verifier's challenge number $c = 2$ to generate a response number, s , as follows: $r + c * x = 11 + 2 * 6 = 11 + 12 = 23$.

The prover gives the number $s = 23$ to the verifier.

The Verification Phase: The verifier, at this point, has the following information:

$g = 2$ (the generator), $p = 17$ (the modulus), $y = 13$ (the public key), and $t = 8$ (the commitment), all given by the prover; $c = 2$ (the verifier's own challenge number), and finally, the prover's response number to the verifier's challenge number, $s = 23$.

The verifier calculates two quantities using the known numbers:

First, $g^s \bmod p = 2^{23} \bmod 17 = 9$.

Second: $t * y^c \bmod p = 8 * 132 \bmod 17 = 9$.

Since both the results (9) agree, the verifier is assured that the verifier knows the secret number.

In reality, computer software programs of the prover and verifier perform the protocol described above. The reason the Schnorr protocol works is that the exchange of some data (g , p , and y) in the setup phase, establishes trust between the prover and verifier, but not to the extent that the prover is willing to share a secret with the verifier. The prover also commits to using the data and the method of calculation (the exponentiation and modulo arithmetic). The description above does not make the protocol fully secure. To do so, the prover and verifier should follow other process requirements. For example, the verifier should pick a different random number r every time the protocol is repeated, the verifier should not send the challenge number c to the prover until the prover has first committed by sending the commitment number t to the verifier, the modulus number p should be a very large prime number, and the generator g should be the primitive root of p .

The protocol works because the calculation of the secret number x by the verifier is computationally hard using g , p , and y . A simple example is that if the prover had some milk and wanted to assure the verifier of that fact without disclosing the exact amount of milk in the prover's possession, the prover simply pours some milk into a cup of black coffee and gives it to the verifier. The verifier can see the milk that has been added to the cup of coffee but is not able to figure out how much milk the prover poured without extensive chemical analysis. In other words, combining milk and coffee is easy; separating them is very hard. This is analogous to computational infeasibility, and such infeasibility is at the heart of cryptographic techniques.

Interactive proofs, as described above, require an interactive process to function. Non-interactive proofs, on the other hand, require only a single interaction or message from the prover to the verifier. The prover generates proof without requiring a challenge from the verifier. The verifier can check the proof without requiring any interaction with the prover. In this protocol, the verification can happen asynchronously. Examples include zk-SNARKs, zk-STARKs, Bulletproofs, and the non-interactive version of Sigma protocols.

Zk-SNARK (Bitansky et al., 2012), the most well-known among them, stands for Zero-Knowledge Succinct, Non-Interactive Argument of Knowledge. The proof is succinct, meaning it is short, small in size, and can be verified quickly regardless of how complex the original statement or data may be. This brevity is an important property when transactions need to be verified rapidly, as in online or retail financial transactions. An ‘argument’ differs from a proof in that an argument need not prove the verifier’s statement with complete certainty. It is designed to be generally secure but may fail if the verifier is dishonest. The reason this possibility of failure is acceptable in practice is because real-world verifiers for transactions that truly matter are those whose own identity is verified and they are usually regulated parties (e.g., money transmitters, banks, healthcare organizations, etc.). Arguments are typically more efficient than proofs.

zk-STARK (Ben-Sasson et al., 2018) stands for Zero-Knowledge Scalable Transparent ARgument of Knowledge. Unlike zk-SNARK, it does not require a trusted setup before using it. The proof and the verification process can be made public since anyone can verify without requiring any secret data to be used in the verification process. This mechanism is highly scalable since it can handle large amounts of data and complex computations efficiently. A further benefit is that zk-STARK is post-quantum secure, which means it is resistant to attacks by quantum computers in the future. The proofs are themselves small and quickly verifiable, making this ZKP mechanism attractive for many applications that are very sensitive to scaling, require transparency, and depend on independent and repeated verifications.

Bullerproofs (Bünz et al., 2018) are a type of cryptographic tool that a prover can use to prove to the verifier that the prover has or knows a secret number. The prover creates a proof to state that the secret number is within a certain range, without revealing the actual number. The prover performs complex cryptographic operations (this is done by computer, not by hand) to provide the verifier a digitally secure proof that the secret number is within a certain range (who also verifies the proof by computer).

Sigma protocols (Groth & Kohlweiss, 2015) use a three-step interactive conversation between the prover and verifier. The three steps are commitment, challenge, and response. The prover creates a commitment of some random number (not the secret) and sends it to the verifier. The verifier sends a random challenge number to the prover. The prover takes the challenge and combines it numerically with the secret and sends the

result back to the verifier. The verifier performs complementary calculations that ‘unpack’ this last result and compares it with the original commitment number from the prover to see if it is the same or not.

Commitment schemes are cryptographic protocols that implement hiding and binding of messages. For example, a message that is placed inside an opaque envelope and sealed by the sender cannot be read by the receiver unless and until the sender unseals it. In addition, the sender cannot alter the message since the receiver has possession of the sealed envelope. In this protocol, the sender is known as the committer since he or she commits to the data by sealing it. The receiver or verifier cannot see the message, hence the ‘hiding.’ Because the committer cannot change the message without the verifier’s knowledge, the committer is ‘bound’ to honor the message. Secure commitments play a key role in fostering trust in widely distributed and decentralized systems. Commitment schemes have had a long history of continuing development and innovation (Brassard et al., 1988; Even, 1982).

Homomorphic encryption, first proposed by Rivest, Adelman, and Deaouzon (Rivest et al., 1978), is a fascinating innovation in cryptography and ZKP where computations can be performed on encrypted data without needing to decrypt it first. The practical Fully Homomorphic Encryption (FHE) scheme was introduced much later (Gentry, 2009). For example, assume that a service provider is engaged to compute the commission of a broker-dealer in a financial services transaction; however, neither party to the transaction wants to expose the original amount of the transaction or the amount of commission paid to the broker-dealer. Using homomorphic encryption, the service provider can apply the broker-dealer’s percentage of commission to the encrypted amount, derive the encrypted amount, and send both to the parties involved in the transaction, who can then decrypt the numbers securely. This process ensures privacy of the original data yet allows the service provider to apply complex rules to calculate commission and certify that the rules have been applied correctly. This mechanism is especially useful for performing data analytics, which is becoming widely used in many companies, on sensitive data.

Given that non-interactive proofs have significant advantages over interactive proofs in terms of scalability, computational efficiency, and the non-requirement for synchronous, real-time interactions, the Fiat-Shamir

heuristic is an important technique. Introduced back in 1986–1987 by Amos Fiat and Adi Shamir, this heuristic guides the conversion of an interactive proof to a non-interactive version.

ZKP USE CASES

ZKPs can be used in both personal and business situations. This section outlines some of the more common use cases. The implementation of ZKPs can happen in many ways, ranging from reengineering existing processes, creating new processes, using new technologies (AI, blockchain), or new devices. In use cases involving or requiring ZKP, researchers follow the principle of least information that will prove the case.

Personal Privacy

Digital Identity Verification. Identity verification is crucial in situations where private data, regulated transactions, or money are involved. ZKP is specifically useful when some or all of the *personally identifiable information* (PII) should not be disclosed. In many of these situations, the verifying party only needs to authenticate some aspect of the identity and does not need access to the actual data itself. For example, only people above the age of eighteen can buy securities, vote, or drink. Their actual date of birth need not be disclosed. Residency requirements (such as those in universities) only require that the person's residence or tenure in a particular jurisdiction satisfy some constraints. The actual address itself need not be revealed. In many financial transactions involving non-bearer instruments in particular, the holder is required to have their 'Know Your Customer' (KYC) verification done successfully. This process is usually done using information provided by data aggregators such as Lexis-Nexis, ComplyAdvantage, Trulioo, or Jumio. Licensed compliance officers check the information itself. KYC verification typically includes checking bad actors and sanctions lists. Needless to say, not everyone who needs to know the outcome of the KYC check requires obtaining the actual data itself.

The other aspect of identity verification is for secure login to online applications and authorization to the application's capabilities. This system has implications for how the information is stored and protected. One can imagine a future where everyone owns their own information

and stores it encrypted in a widely distributed blockchain. They would disclose only the relevant aspects of their data and answer only the question at hand (age, for example). They would refuse access to the actual data (date or birth, for example), while the verifier can be assured that the data is truthful and untampered.

Secure Messaging. This capability currently exists within secure messaging apps. The message that should be kept secret and available only to the intended recipient is hashed, encrypted with the public key of the recipient, and signed by the private key of the sender. The sender also separately encrypts parts of the message that will allow an intermediary to verify the claims of the message without reading the rest of the message. Secure file-sharing is included in this use case, where ZKPs can be used to prove ownership of a file, grant permission to access a file, verify the type of contents in the file, or the presence or absence of certain types of information in the file. Such verification is accomplished specifically through commitment schemes that separate the verification process into two parts.

Secure and Anonymous Voting. ZKPs can be used for voting, where the challenge is either security, anonymity, or both. ZKPs exist to verify identity without disclosing the identity to other parties. Anonymous voting with ZKPs proves to the stakeholders that the person voted, but not how. Indeed, with fully decentralized security coupled with ZKPs, stakeholders can be assured that voting has taken place and that quorum has been achieved, without revealing who voted and who did not, let alone how they voted. A complete solution with ZKPs would also prevent double voting. Many of the concerns with fake voters and errors in vote counting would be prevented while maintaining voter privacy.

Health Data Privacy. Privacy of health information is a sensitive topic that is subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (See Chapter 10 for a detailed discussion of health-care data privacy). ZKPs can help individuals prove that they meet certain criteria, including fitness levels (such as the ability to perform certain jobs, but without disclosing specific fitness parameters), vaccination status (such as proof of meeting travel requirements but without disclosing the actual vaccinations), presence or absence of a medical condition (such as diabetes, but without revealing A1c or blood glucose readings), and ordering prescriptions without disclosing their name (as well not disclosing to the shipper the type of package, but proving that the contents meet the hazardous materials constraints).

Location privacy. ZKPs can help prove to service applications that the user is within a geographical region without disclosing the address. Knowing the location (without necessarily disclosing the address) is important for delivering or denying certain types of services. Additionally, knowing the location is also useful for the application of AI (machine learning and data analytic) techniques to better serve customers. For example, a business can suggest UV products to online visitors from regions that are suffering from a heat wave. Government agencies can send advisories on imminent extreme weather or disease outbreak to people online. Intermediaries for financial securities can enable or disable transfers if they contravene the blue-sky laws (“Frequently asked questions about Exempt Offerings,” the SEC). Each country has its own data privacy laws and requirements to adhere to GDPR (“Does the GDPR apply to companies outside of the EU?”), while some countries have privacy laws based on state, territory, or region, such as, for example, the California Consumer Privacy Act (CCPA).

Private financial transactions. ZKPs can be used to provide insights to advisors (human or robo) so that they can better tailor financial plans for their customers, without revealing any detailed financial data. For example, a CPA will require complete financial details, but a financial advisor may only need to know their customer’s risk profile (high, medium, or low, depending on age, investment experience, and level of funds to invest, without disclosing the actual numbers).

Some cryptocurrency technologies use ZKP to shield private transactions in the public blockchains. Zcash, a cryptocurrency that was designed to be more privacy-enhancing than Bitcoin, for example, uses zk-SNARKs for shielded transactions, where the details of the sender, the receiver, and the transaction amount are encrypted, while allowing miners to use zk-SNARKs to verify the validity of the transaction. Selective disclosure for reasons of audit or meeting regulatory compliance requests is also possible through ZKPs.

Privacy in Social Media Interactions. There is no doubt that social media has transformed the nature of social interactions. They have expanded the reach, scope, and scale of interactions, from the confines of the local community to the entire planet. Online marketers have taken advantage of this information to provide targeted advertisements and recommendations. While this is useful in tailoring the experience of the online user and making it more meaningful and productive, it does not require the marketer to have access to many other pieces of information

about the user. Scammers, on the other hand, use sensitive information to create fake identities and perpetrate fraud. Assuming online social media platforms evolve to incorporate stronger data privacy policies and encryption, ZKPs can be used to provide proof of certain conditions or behaviors of the user without disclosing the actual data. For example, online recommendation engines can use ZKP to target recommendations more precisely than regular collaborative filtering (which is well-known and quite prevalent among the larger online businesses) to adults and seniors without knowing the users' actual date of birth. Similarly, users can enable sharing of their preferred products without disclosing their identity.

Educational Records. Using ZKPs, students can prove that they meet certain qualifications or that they have completed certain courses without revealing their full educational records (or transcripts) which contain grades. Similarly, politicians and other government officials can provide proof of attendance at or graduation from institutions as declared in their public bios, and that their qualification is in good standing, without disclosing any more details.

Privacy with Sunshine Laws. States in the US have enacted Sunshine Laws in varying degrees and scope to ensure transparency in government. In many cases, however, these laws also impinge on the privacy of the government officials, most especially salaries. If the intent is to assure the public that the salaries of government officials are equitable and in line with the general population, or to assure the lack of any discriminatory practices, ZKPs can provide that proof without disclosing the actual salaries.

Privacy with Internet-of-Things (IoT). ZKPs can allow users to control their devices (smart home, drones, cars, etc.) by proving their identity and authorization to control them without disclosing private information. This is an important capability since many IoT devices and technology infrastructures are mediated by independent third parties.

Privacy in business. Privacy in business mirrors many of the same concerns as privacy for individuals since many of the business and even social interactions are between consumers and businesses. In addition to the business-to-consumer (B2C) privacy concerns, business-to-business (B2B) privacy concerns also need to be addressed in order to increase trust in business settings.

Employee Verification. Companies can verify employee's credentials, qualifications, and background information without accessing or storing

sensitive data. Typically, these services are offered to companies by third-party service providers. Companies need not see sensitive information about candidates but use ZKPs to verify information provided by these third-party services. Similarly, when outside agencies (such as a mortgage company processing an employee's loan application) require employment verification, the company can provide a zero-knowledge proof of employment and the number of years of tenure with the company without disclosing the employee's details, such as the exact dates of employment. If the verifier requires additional personal data, the verifier should either obtain directly from the loan applicant or obtain through similar ZKP solutions with other providers).

Intellectual property. Companies can protect their intellectual property by proving ownership of copyrighted and confidential material without disclosing the contents themselves. ZKPs can provide not only proof of ownership but also prove the presence of certain types of information within the document using commitment techniques.

Contract Documents. Many company contracts are confidential documents and their contents are not disclosed to parties that are not involved in the contract. Companies, however, may need to prove that they have signed certain agreements, such as pre-orders (order commitments), that impact their ability to secure financing. ZKPs help prove that these contracts are legitimate and that the company is reporting the order book truthfully without revealing the details to potential competitors. This capability of ZKPs is particularly useful in supply chains where multiple parties are involved, but individual arrangements need to be kept private while assuring the other parties that the agreements are in place. Supply chains and networks have complicated business models that require verification of different pieces of information while ensuring that the details are private. Multi-party computation is an important ZKP technique that was covered in Chapter 7.

Verification of Organizational Structure. Companies may have corporate investors or have merger and acquisition (M&A) deals. Part of the due diligence for such transactions is performing KYC verification of the officers and board of directors of the corporate parties. Included is also verification of other affiliations of the individuals to ensure there are no conflicts of interest. ZKPs allow all parties to verify such information without requiring disclosure of the underlying data.

Privacy in Smart Contracts. Smart contracts in blockchain execute code based on business logic. Smart contracts use data and rules that

are encoded within them. ZKPs help smart contracts execute the business logic without exposing any of the underlying data. This is especially important since smart contract logic is available to all the participants on the chain so that validation and consensus can be formed before committing the results of the smart contract computation to the distributed ledger.

CHALLENGES AND LIMITATIONS

ZKPs are subject to three critical challenges: computational efficiency, trusted setup prior to use, and scalability.

Issues with Computational Costs and Efficiencies

Computational performance and operational costs are critical factors in the design and implementation of enterprise software systems. In the case of ZKPs, they take on added importance depending on the potentially high volume of transactions. There is a tradeoff between low cost and high performance on one hand and security and privacy on the other. Generating zero-knowledge proofs that can capture rich business scenarios can be computationally intensive, requiring complex mathematical operations that may not be feasible in real-time, high-volume scenarios. The verification process is generally less computationally demanding than proof generation; however, it too incurs computational costs that may not meet the business needs. These tradeoffs are especially important in decentralized ledger networks, where every node may need to verify a proof and participate in a consensus process, thus increasing the overall computational cost and performance.

Various ZKP schemes offer different tradeoffs. For example, zk-SNARK proofs are quicker to verify but require a trusted setup, while zk-STARKs do not require a trusted setup but are more computationally intensive. Cryptographic research is continually testing the boundaries of such tradeoffs: increase speed, reduce cost, increase security, and increase privacy.

Issues With Trusted Setup

Many cryptographic schemes require that both parties exchange some initial secret information before they communicate the first secret

message. Examples of such initial information include code books, substitution keys, or initial sharing of decrypting keys. This process of initial exchange of information is also a requirement in certain ZKP mechanisms such as zk-SNARKs. In the initial phase (prior to first use), a shared piece of data called the Common Reference String, is generated using a random string (called the ‘toxic waste’). To prevent leakage of the random string used to generate the public parameters, some implementations such as Zcash perform ‘ceremonies,’ which are standardized interactions between multiple parties. Newer ZKP schemes such as zk-STARKs eliminate the need for this trusted setup, thereby reducing the risk of compromised secret keys.

Scalability Issues

ZKP transactions can be computationally intensive, sometimes requiring several thousand computations for every ZKP transaction. In large, decentralized networks such as Ethereum, this complexity creates an enormous computational burden since every node has to perform the same verification of the proof to achieve consensus. This computation burden could result in slow transaction processing times and limit the network’s throughput, making it difficult to scale the system to accommodate a large number of users or transactions. ZKP schemes like zk-SNARKs produce relatively small proofs, while zk-STARKs can generate larger proofs, creating computational, storage, and transmission challenges.

CONCLUSION

The world is getting smaller in many ways; logically yet perhaps paradoxically, the bubble in which individuals and companies live is getting bigger every day. Increased number of participants, frequent and rapid interactions, increased distances, and lack of reliable intermediaries in many of the business and social interactions cause the challenge in establishing trust in people, companies, and transactions. At the same time, there is considerable anxiety over privacy of data. ZKP technology is all about enabling the increasing engagement and trust while reducing, if not eliminating, the concerns over privacy of data. ZKPs offer several interesting solutions to meet this challenge. Technology solutions can use ZKPs independently of blockchain but incorporating them into a blockchain can significantly enhance the value proposition of blockchain solutions.

ZKPs can enable verification of blockchain transactions without violating the privacy of the participants. ZKPs can make blockchain applications more scalable through succinct schemes such as zk-SNARKs. Research and innovation in this space, as well as cautious experimentation by practitioners, is continuing at a brisk pace.

REFERENCES

- ACM A. M. Turing Award, (2004). https://amturing.acm.org/award_winners/cerf_1083211.cfm
- Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, Transparent, and Post-quantum Secure Computational Integrity. *Cryptology ePrint Archive*.
- Bitansky, N., Canetti, R., Chiesa, A., & Tromer, E. (2012). From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference on—ITCS '12. ACM* (pp. 326–349). <https://doi.org/10.1145/2090236.2090263>. ISBN 9781450311151. S2CID 2576177.
- Blum, M., Feldman, P., & Micali, S. (1988). Non-Interactive Zero-Knowledge and Its Applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988)* (pp. 103–112).
- Brassard, G., Chaum, D., & Crépeau, C. (1988). Minimum Disclosure Proofs of Knowledge. *Journal of Computer and System Sciences*, 37, 156–189.
- Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G., (2018). Bulletproofs: Short Proofs for Confidential Transactions and More (conference version). In *Security and Privacy (SP)*, IEEE Symposium on, (pp. 319–338). IEEE.
- California Consumer Privacy Act (CCPA). <https://oag.ca.gov/privacy/ccpa>
- Diffie, W., Hellman, M. E. (1976). New Directions in Cryptography (PDF). *IEEE Transactions on Information Theory*, 22(6), 644–654. CiteSeerX 10.1.1.37.9720. <https://doi.org/10.1109/TIT.1976.1055638>. Archived (PDF) from the original on 2014–11–29.
- Does the GDPR Apply to Companies Outside of the EU? <https://gdpr.eu/companies-outside-of-europe/>
- Even, S. (1982). Protocol for Signing Contracts. In A. Gersho (Ed.), *Advances in Cryptography (proceedings of CRYPTO '82)* (pp. 148–153).
- Fiat, A., & Shamir, A. (1987). How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Proceedings on Advances in cryptology—CRYPTO '86* (pp. 186–194). Springer-Verlag.

- Frequently asked questions about Exempt Offerings, the Securities Exchange Commission. <https://www.sec.gov/education/smallbusiness/exemptofferings/faq>
- Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing (STOC '09)* (pp. 169–178). Association for Computing Machinery. <https://doi.org/10.1145/1536414.1536440>
- Goldwasser, S., Micali, S., & Rackoff, C. (1985). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18(1), 186–208.
- Groth, J., & Kohlweiss, M. (2015). One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin. In *Advances in Cryptology—EUROCRYPT 2015—34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, April 26–30, 2015, Proceedings, Part II* (pp. 253–280). Springer. https://doi.org/10.1007/978-3-662-46803-6_9
- Health Insurance Portability and Accountability Act of 1996 (HIPAA). <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
- Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (p. 9781439103555). Simon and Schuster.
- Post-Quantum Cryptography, Selected Algorithms, NIST Information Technology Lab, <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>
- Rivest, R. L., Adleman, L., & Deouzos, M. L. (1978). On Data Banks and Privacy Homomorphism. In R. A. DeMillo (Ed.), *Foundations of Secure Computation* (pp. 169–179). Academic Press.
- Selleri, S. (2020, December). The Roots of Modern Cryptography: Leon Battista Alberti's 'De Cifris'. *URSI Radio Science Bulletin*, 2020(375), 55–63. <https://doi.org/10.23919/URSIRSB.2020.9663133>.
- Singh, S. (2000). *The Code Book*. Anchor Books (pp. 14–20). ISBN 9780385495325.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



PART III

Domain-Specific View of Privacy



CHAPTER 9

An Architect's View of Privacy

Marlon Blackwell, Lynda Coon, and Mary C. Lacity

INTRODUCTION

Marlon Blackwell is the E. Fay Jones Chair in Architecture and a Distinguished Professor in the Fay Jones School of Architecture and Design at the University of Arkansas in Fayetteville. In addition to being a full-time faculty member, he is also the founder and the principal at Marlon Blackwell Architects (MBA), based in Fayetteville Arkansas.¹ We interviewed him in June of 2023 to capture his design philosophy in relation to privacy. The conversation focused on four architectural privacy themes:

(1) the relationship between privacy and comfort, and the roles of (2) primary, secondary, and tertiary spaces, (2) light, and (3) sounds in creating private moments in public spaces. A fifth theme encapsulates the essence of his design philosophy: “ennobling the prosaic.” This chapter is an edited transcript of the conversation.

¹ To view Marlon’s work, see: <https://www.marlonblackwell.com/> or MacKeith, P. & Boelkins (Eds.). (2023). *Radical Practice: The Work of Marlon Blackwell Architects*. Princeton Architectural Press.

M. Blackwell · L. Coon · M. C. Lacity (✉)
University of Arkansas, Fayetteville, AR, United States
e-mail: mclacity@uark.edu

THEME 1: PRIVACY AND COMFORT IN DESIGN

Lynda: Marlon, thank you for meeting with us today. We'd like to first ask you to put architecture privacy in a bigger global and historical context of privacy design, then share your own experiences from your global travels. Have you noticed shifts in privacy design between Eastern and Western cultures?

Marlon: While I am not a historian, I did teach a course called "house culture," which was on the origins and evolution of the American private house. We went through the whole history of privacy in architecture. The medieval times stick out in my mind as an example of a culture with a very different sense of privacy and personal space. People were more communal and familial. The idea of comfort was very different in terms of furniture design and room size. Their beds were often as big as the room. Guests traveled far, so when guests came over to visit, by the end of the evening everybody just slept in the same giant bed. So that is a different form of privacy and comfort. Privacy and comfort tie together to indicate whether someone is comfortable or uncomfortable in a space.

For many Americans in the United States to feel comfortable, they seem to require much larger personal spaces than for example, someone from Japan, the Middle East, and elsewhere. Americans' concept of privacy and comfort may come from our pioneering spirit; we have all this space and horizons that extend endlessly. In addition to this notion of the prevalence of horizon, the sense that everyone should have their own space comes along with American individualism. That doesn't mean that Americans don't share, but in terms of one's own space as an abode, an American ideal is to have the detached single-family dwelling, surrounded by land—preferably agrarian—with secondary structures for the livestock. Americans don't typically put animals in the house.

I've been to the city of Shibam in Yemen. They have hundreds of ancient towers, six to eight stories tall, made from mud brick, gypsum, and other natural materials (see Fig. 9.1). The ground level is given over to the animals, the next level to the women, above them is the kitchen, then the men. Above the men is the mafraj, which is the living area where people take food, socialize, and enjoy the views. Gypsum screens on the windows protect the privacy of the women inside. The bathrooms are near the top and human waste is funneled down a chute at the side of the building and lands at the bottom to become a compost pile used to fertilize their fields. It's the true definition of indigenous—nothing is



Fig. 9.1 Panorama of Shibam, Hadhramaut Province, Yemen
(Image credit licensed from iStock.com/javarman3)

left to chance; nothing is wasted, everything is recycled. Even the city of Shibam is organized around gender, which is a different form of privacy compared to the West.

I've also traveled to Mexico, Mali in West Africa, and to places in South America like Peru where the animals people eat live inside with the residents, such as the local guinea pig (cuy). So, there is a lot of variation in privacy and comfort as it relates to different cultures.

I think comfort is a big driver of ideas about privacy, so that's why I put privacy and comfort together. Architecture accommodates and facilitates privacy and comfort. Comfort informs how we think about space, how it's used, and how it's articulated in the activities within the space.

THEME 2: PRIVATE MOMENTS IN PUBLIC SPACES: PRIMARY, SECONDARY, AND TERTIARY SPACES

Mary: Marlon, you've designed so many types of spaces. You've designed a church, several schools, a museum shop, a golf clubhouse, a bike barn, a library, a pediatric center, and much more. You described in our Honors class that one of your design principles is "creating private moments

in public spaces.” Would you talk about that principle and how it was realized in some of your works?

Marlon: Yes, the idea of the private within the public and the notion of making spaces that can be used for fellowship and for solitude is often a goal in our projects. We think in terms of primary, secondary, and tertiary spaces and how they are used.

I’ll use the example of church design. One of the most tragic things to happen is for someone to lose a child. In that space of mourning at a funeral service, it’s rare that people grieve alone (physically isolated); they grieve in their own kind of mental world, but they also want to be near people. So, as an architect, we can accommodate a space in a church where someone can be part of the group but also be in solitude. Crypts, choir lofts, and side chapels are examples of creating private moments in public spaces.

Another example is the design of medieval monasteries. At the end of the monastery, the walls are thickened and carved out to the shape of a body. A forlorn window opens to the outer world. A monk could sit on the wall and not look frontally but sit in a moment of privacy. I’ve also seen examples where there is space for two people to sit and have an intimate and introspective conversation, with the world just beyond them.

For schools, we also think in terms of primary, secondary, and tertiary spaces, but we also think of school buildings as didactic. You can learn from them by the way materials come together, light comes together, and how space comes together. I think space is more stable at the center, but can be wilder at the edges. Keeping spaces open at the center means it has purpose, but the purpose isn’t so finite that there’s no wiggle room for other kinds of uses. It’s at the perimeter you can discover things, whether it’s the way in which a window is carved out of a wall, a nook that is punched through a wall, or even a stairwell can be a spatial proposition. Rather than just something that you look through or look at, you can occupy the space physically. Those become moments that are very intimate (see Fig. 9.2).

In our designs, we develop degrees of intimacy, whether it’s with oneself or with a few people. We look for clefts and canopies, a kind of back-and-forth play between the primordial notion of the cave and the



Fig. 9.2 Marygrove Early Education Center, designed by MBA
(*Image Credit* With permission from Marlon Blackwell Architects)

forest. Fay Jones² would talk about that idea in this work. His work was really a dialogue between cave and forest that determined the choice of materials and how that material was used. Stone is more cave-like and can be used as an extension of the landscape. Tall wood structures are more like the forest that provide the canopy. When we think about the cave, again, we think about the primary, secondary, and tertiary spaces. So, in the schools we design, you'll find places where children can just crawl up into them (see Fig. 9.3).

Porches work well too as a liminal zone between the interior and exterior, between the public and the private. In schools, a porch can be a place of learning, a play area, or a refuge. On a porch, you are in an interface between the private world of the school and the public world of the street.

² E. Fay Jones (1921–2004) was an American architect and the only apprentice of Frank Lloyd Wright to have received the AIA Gold Medal.



Fig. 9.3 Lamplighter School Innovation Lab, designed by MBA
(*Image Credit* With permission from Marlon Blackwell Architects)

Furniture is also an important factor in creating private moments in public spaces. In a public garden or park, a single park bench invites solitude. Clusters with multiple seating suggest a more social interaction.

We come at design section by section in the design of schools. There's a notion about democratic space where everybody gets the same thing, every classroom is the same, but that idea is a simplistic idea of equality about socialism. In America, the culture is more about individuality, choice, and dissimilarity. That's why we fold the roof section so that every classroom has a different character. As students move through the curriculum, they experience different spaces. That's very stimulating to students. It also speaks to how, for example, the Thaden School works. It has a logic, but it's not overly systemic. We vary the volume of the space to create feelings of intimacy and feelings of community. For example, we designed a room where the ceiling is higher on one end of the classroom. Larger groups naturally congregate where the ceiling is higher, and that group will be more social. The part of the classroom with the lower ceiling naturally creates feelings of intimacy and promotes small project

work. So, varying the volume of space promotes how people will use it in an equitable way. If the teacher is attentive, she understands that as well.

Lynda: In school design, how do you get around the hierarchy of the teacher at the front of the classroom speaking and the students are passive listeners?

Marlon: Yes, that's the convention. There's often a whiteboard or a screen for projection in a traditional classroom design. There's nothing wrong with the convention, but there are other ways to learn. The schools we design have those things, but we design a range of classrooms with different functions. For example, in a small lab room, there is a Harkness table; it's an elliptical table with no head of the table, where up to ten people can sit around it. It invites a seminar format and it's a way to break down the hierarchy. In the breezeways we designed, I've found students out there with chalk doing math on the concrete paving. In addition to design, those uses are really driven by the teacher and the philosophy of the school.

THEME 3: PRIVATE MOMENTS IN PUBLIC SPACES: LIGHT

Marlon: Light relates to privacy and intimacy in many ways. Most building codes require uniform lighting, the same amount of light wherever you are in an office or retail store. James Turrell, a very famous artist who deals with light, came to the University of Arkansas a few years ago. One of the first things he said in his lecture was that in Western cultures, there is too much light. We are overexposed through the insistence of uniform lighting of spaces.

That's a big driver of mine: how can we create a greater sense of spirituality, sacredness, and serenity in space? Spaces with shadows, funnels of light, and light that changes throughout the day all have a mystery about them. They have a way of affecting our emotions, helping us to go inward, helping us to detach from the world a little bit, encouraging a sense of privacy or a sense of introspection. Why is it that those experiences only seem acceptable in the realm of the sacred? Why couldn't you have those experiences in a doctor's office? Why couldn't you have them in a school? We've been stubbornly trying to find those moments in the schools and the medical centers we design. There are some places you can't get around having brighter illumination but maybe you could have a dialogue between dark and light. I think that has great potential in making distinction between the public and the private.

Lynda: Would you provide an example from your work?

Marlon: In the Harvey Medical Clinic we designed, the HIPAA³ law does not allow windows in treatment rooms for children—the government is very strict about that. It doesn't want people seeing in or seeing out. So, we skylit the spaces from above and sealed up the walls. So, you're filling the patient rooms with natural light, but you're not having views. The design reinforces privacy, but it doesn't cut you off from the world. I think that is critical.

In that clinic, we created something strange because most architecture is about punching as many windows as you can in a wall; it's strange to see a wall with no windows. By not knowing that it's skylit until you are inside the building, it creates an active discovery from outside to inside. So, it is a masking of the façade. The exterior veils the hidden surprise on the interior.

THEME 4: PRIVATE MOMENTS IN PUBLIC SPACES: SOUND

Mary: How do you think about audio privacy in design? In particular, the freedom from not hearing noise?

Marlon: Acoustics are key. It's important to get the balance right. You may want some discrete sounds, but not make the space so quiet that it feels muffled. We want to optimize that.

We are looking at how to make an architecture that's more thick, slow, and implicit rather than architecture that is thin, fast, and explicit. Most of the architecture today is made of planes and lines; it's always about some kind of seamless relationship between outside and inside. When you cut through a wall, it's like cutting through a piece of glass because there's nothing there, so the walls are diminished in some ways, which leads to lots of acoustic issues. We've been very interested in thickening walls and carving into the walls or faceting of the wall to have a more distinct relationship between what's interior, what's exterior, and that affects acoustics as well.

³ The US Health Insurance Portability and Accountability Act (HIPAA) passed in 1996. The law specifies how healthcare and healthcare insurance companies should protect personally identifiable information (PII).

THEME 5: ENNOBLING THE PROSAIC

Lynda: Of all the buildings you shared with our honors students, the students were most impressed with the Saint Nicholas Eastern Orthodox Church in Springdale Arkansas (see Fig. 9.4). Why do you think they were so mesmerized?

Marlon: Because it captures the imagination. It's got a great story. It's an example of ennobling the prosaic. It was a welding shed that we transformed into a sacred space and fellowship hall where one can worship and come together. It bridges ritualized worship with something manifested from a type of ruin. That building's abstraction is appealing. When I presented the design to the church, people were taken aback. They were expecting a traditional Byzantine church, but with only \$100 per square foot in the budget, we had to get creative. Father John understood the



Fig. 9.4 Saint Nicholas Eastern Orthodox Church, designed by MBA
(*Image Credit* With permission from Marlon Blackwell Architects)

design. He said to the church leaders, “It’s got everything we asked for—the symbols, the colors, a dome, and places for the iconostasis.” After we explained that the proportioning system was all Greek, using the golden means and rectangles, they started to go, “Oh, I get that.” And I might add, that proportion and scale don’t cost anything—it’s free.

So, we ennobled this humble welding shed. I think it’s the modesty of it all; the lack of being ostentatious. It’s almost like a country church, but a new version of a country church. It’s not a church hidden away in the woods; it’s sitting out like a billboard along the Interstate. The notion of it being contemporaneous with our own suburban sensibilities, a kind of improvised but also dignified church. I think the church resonates with people because it is transcendent regardless of whether you are religious or not.

Mary: What are some other examples of ennobling the prosaic?

Marlon: People love the Gentry Public Library in Gentry Arkansas. We made a public library out of a 100-year-old hardware store. We also designed a bike barn in Northwest Arkansas that is a new form, but it is reminiscent of a traditional Ozark gambrel barn. They all have great stories, and a great story touches people.

Lynda: Marlon, thank you so much for sharing your thoughts on privacy from an architect’s viewpoint. This will be a great contribution to the book.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 10

Healthcare Privacy in an Electronic Data Age

D. Micah Hester

INTRODUCTION

While Chapter 2 explores the philosophical underpinnings of the concept of privacy in detail, it is important to revisit an observation about life: there is a fundamental ontological gap among individuals. Whether philosophers conceive of us as fundamentally connected social beings or radically atomic beings, we recognize that each of us is a unique part of the experiences we have, perhaps even those we share. The “private,” then, is one way of expressing that realm of experience that each of us uniquely possess, in which others only partake when we choose to share it with them. Even then, the very act of sharing transforms that private realm into something else, as the experience is changed in the very act of sharing.

Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.

D. M. Hester (✉)

University of Arkansas for Medical Sciences, Little Rock, AR, US
e-mail: DMHester@uams.edu

—Hippocratic Oath

The sharing of our private realm occurs frequently throughout our lives, with every relationship or connection with others demanding that we express what we might otherwise keep to ourselves. This chapter explores relationships that occur between patients and providers within the realm of healthcare in the United States (US). Healthcare is a professional domain primarily dedicated to helping individuals (and sometimes, by extension, the public) to live healthily (Hester, 2001). People seek assistance from healthcare professionals (HCPs) referred to as patients, and the act of someone assuming the role of a patient is, even if in a small way, an act of trust in what HCPs can do that the patient themselves cannot do on their own. Consequently, a fundamental obligation that arises for HCPs is to demonstrate *trustworthiness* in how to collaborate with and serve patients.

Privacy, as it has been treated in healthcare, signifies a patient's entitlement to maintain control over the personal, both mundane and intimate, details of their life. This entitlement is placed firmly under the authority of the patients themselves. What follows for healthcare, then, is an obligation, which arises for the professionals and personnel working in medicine (referred to as HCPs). This obligation is typically labeled *confidentiality*, and requires that HCPs safeguard certain identifying information within the protective confines of the healthcare relationship. This principle has been recognized as an integral part of medicine for a considerable time, at least since the days of Hippocrates. In this context, the patient, as Richard Zaner aptly describes, has always possessed "peculiar vulnerabilities" (Zaner, 1988), and the "secrets" of their lives should not be "spoken of abroad" by the professional.

Privacy and confidentiality, then, are two sides of the same coin, though the former functions as a right in light of a particular kind of vulnerability experienced by patients, while the latter is a responsibility to be fulfilled by providers *and* the institutions for/in which they work. The expectation of privacy should be upheld through the trustworthy actions of HCPs in holding private patient information in confidence.

Expressed in this way, the conceptual relationship and expectations surrounding privacy and confidentiality may appear straightforward on the surface. However, this apparent simplicity is based on an overly simplistic view of healthcare as a bidirectional and exclusive collaboration between an individual patient and a specific healthcare provider. In reality,

these relational rights and obligations are not absolute. The complexities of modern healthcare and the interconnectedness of today's electronic age confound this traditional model, making the preservation of privacy and the fulfillment of confidentiality difficult, if not impossible, to maintain.

Over 40 years ago, clinician and bioethicist Mark Siegler (1982) examined the state of medical practice and declared confidentiality a "decrepit concept." In his well-known work, Siegler argues that the supposed dual relationship between physician and patient is a myth, as numerous people inevitably have access to intimate patient information. It is worth noting that this declaration preceded the advent of Health Maintenance Organizations (HMOs), Accountable Care Organizations (ACOs), electronic health records, social media, 24-hour news cycles, and many other factors both within and outside the medical culture that have significant implications for privacy and confidentiality. Given these developments, one might wonder how much more "worn-out" and "useless" the concept must be today.

It is the case, of course, that medical information about a patient is accessed by many people and shared with many institutions. The federal government, confronted by the challenge of sharing personal information in healthcare, even recognized the need to address concerns that such sharing raises when it produced the Healthcare Information Portability and Accountability Act (HIPAA) regulations, passed in 1996. And while all this seems to continue to support Siegler's argument, his concern (and others who have raised similar issues) simply miss the point. Privacy, as an expectation (even a right) of patients, and confidentiality as an obligation of providers, provide moral parameters that set the tone and tenor of medical relationships. Within the relationship, patients should have confidence that the intimacies of their lives can be expressed and exposed openly in order to receive the support they need to live healthily. Thus, clinicians must operate with the understanding that the release of patient information—intended or accidental—fails to fulfill a duty they hold to the patient. It is a moral *wrong*—be it about a trivial condition or momentous disorder. But this is not the only moral transgression that might occur. Moral harm can follow from revelations that impact patient lives through exposure that leads to loss of work, tensions in or dissolution of relationships, stigmatization, and even avoidance of future medical care.

As highlighted by Ken Goodman (2022), the challenges that healthcare faces in light of the use of electronic medical records bring into stark relief concerns regarding both moral wrongs and harms,

In the clinical setting, a patient can be wronged, harmed, or both by incautious and unguarded conversations, by failures to follow basic electronic health record (EHR) hygiene (do not share your password, log off, do not make copies), and by efforts to trick users or attack systems.... Breaches of any kind or size can erode trust and undermine universal values that shape the clinician-patient relationship.

Clinical medicine (as well as medical research) operates as a professional space precisely because the relationship between patients and providers comes with expectations that the relationship is a special kind—not one of family or friendship nor of a simple business transaction or “mechanical” service. It is a space devoted to helping human beings live healthily, meeting their own individual vision of what living healthily means to them (Hester, 2001). That requires an understanding among all the parties that the personal intricacies of individual lives “ought not to be spoken of abroad.”

LIMITATIONS AND THE SCOPE OF PRIVACY

While it is clear that privacy is important, even fundamental, to health-care relationships, it is not without its limits. From logistical to public health to criminal to moral reasons there are times when a patient’s privacy must give way to other forces and the confidentiality that providers protect must be abandoned. We have already noted that the essential flow of information within healthcare institutions often necessitates that numerous people whom patients would not otherwise have considered to be within the scope of healthcare practice gain legitimate access to intimate details of a patient’s life. That is, not just the physician or nurse knows medical details about a patient, but respiratory therapists, social workers, chaplains, and even clinical ethicists may see a patient’s chart—not to mention medical transcriptionists, medical records clerks, insurance providers, and many more. Again, this is all falls within the scope of medical privacy, even if patients are not fully aware of it.

Beyond the general scope of medical privacy, there are instances when the confidentiality inherent in medicine may be intentionally breached for the sake of public health. States have laws, for example, requiring that certain communicable diseases—such as Tuberculosis, Ebola, and HIV—be reported to state agencies. These requirements are born out of a concern for the common good, and often these same laws also impose

limitations on what personal information state agents can disclose, and to whom. The range of state-based concerns expands even further when other safety and protection factors come into play. For instance, healthcare providers are mandated reporters, legally obligated to report reasonable suspicion of child or elder abuse. Similarly, injuries suspected to be the result of criminal activity often have to be reported. These exceptions to typical privacy protections balance individual privacy with broader societal interests in safety and public health.

Wider legal factors may burst open the privacy bubble, as well. Courts may require medical records to be disclosed or healthcare providers to testify in court. Cases regarding workers' compensation require that medical records be examined by insurance providers, lawyers, and others. Such circumstances demonstrate that while medical privacy is a principle in healthcare, it is not inviolable and can be overridden by a number of broader societal concerns.

Some of the harder cases for patients and providers, however, are so-called "duty to warn" situations. The paradigmatic legal case, known as the Tarasoff case in California, emerged from mental health practice in the 1970s. The case arose after the tragic death of Tatiana Tarasoff who was murdered by her ex-boyfriend, Prosenjit Poddar. A few months earlier, Poddar told a psychotherapist at the University of California at Berkeley that he intended to kill Tarasoff. Seven years later, the Supreme Court of California Supreme Court ruled that in some cases the provider has an obligation to break confidentiality, specifically when there was a clear threat of imminent harm to an identifiable third party. Subsequent to this ruling, many states have passed "Tarasoff" laws, and even where no such law exists, many legal experts and ethicists believe that the Tarasoff ruling does identify a limit to privacy and confidentiality in healthcare relationships.

This "duty to warn" has, at times, been expanded upon by ethicists, courts, and state legislatures to include other forms of medical danger. The most prominent example arose in the 1980s and 90's with HIV and AIDS. Due to concerns about the communicable nature of HIV—especially before the development of effective antiviral treatments that could reduce or eliminate viral loads—states passed laws requiring either practitioners or state agencies to contact known, or even just potential, intimate partners of individuals testing positive to HIV.

Whether or not we agree with each category or instance of supported breaches of privacy and confidentiality, the point of all this is that privacy

does have limits. Consequently, providers may confront moments in their practice when they are required to forego keeping patient information confidential because of some other, more pressing (and typically social, legal) obligation. One ethical framework to understand better when breaching confidentiality may be acceptable includes the following criteria:

1. There is strong reason to believe that a serious threat of physical harm exists to an identifiable individual.
2. After careful consideration, there is a strong likelihood that a tangible and true benefit will result from breaking confidentiality.
3. The breach is a last resort, pursued only after other alternatives have been considered and deemed inadequate.
4. It would be reasonable to support a breach of confidentiality by a healthcare provider in any case involving a patient under relevantly similar conditions and circumstances.

A NOTE ON HIPAA

We now see how the law plays into delimiting the scope of privacy in medical practice, but as alluded to earlier, the law also seeks to constrain the use of private information in order to protect patients' personal information as much as health systems can allow. The primary instrument for achieving this has been the Health Insurance Portability and Accountability Act (HIPAA) developed in 1996 but not fully implemented until 2003. As the title suggests, HIPAA was developed to facilitate the transfer of information among the many institutions, companies, and providers that require access to a patient's health information. But this "portability" also brings with it the risk of information being easily accessible to others who do not need access to it. To address this issue, the "accountability" side of HIPAA is manifest in the HIPAA Privacy Rule. This rule provides guidelines and restrictions on how health information should be shared among the various stakeholders involved. The Privacy Rule targets individually identifiable health information, details about a person's mental or physical health, treatment history, or payment for healthcare services. This is known as "protected health information" (PHI), and PHI not only includes health information but also "common identifiers" such as name, address, birth date, and so forth.

Important requirements from HIPAA's Privacy Rule include:

- Patients should have easy and secure access to their own health information, and have the right to request an accounting of who has accessed their health records. HECs should work to foster improved ease of access to electronic health record (EHR) information.
- The sharing and exchange of health information should be guided by the “minimum necessary standard.” This means that one should not share more information than needed for a particular purpose.
- Institutions must establish policies to govern interactions between people or organizations that provide or pay for health care (“covered entities”).

Breaches of HIPAA confidentiality requirements—where Protected Health Information (PHI) is disclosed to parties who do not have a legitimate need for it—can lead to both institutional and individual penalties. In cases of serious negligence or willful disregard for HIPAA regulations, criminal charges may even be filed. Such consequences underscore the importance of safeguarding patient privacy and maintaining the integrity of healthcare systems.

TECHNOLOGY AND DATA: THE PROMISES AND PERILS TO PRIVACY

HIPAA regulations underscore the importance of and concern for the sharing of health data within and across complex healthcare, insurance, and legal systems. And while this data can be provided on paper, through hardcopies handed directly to individuals or delivered by human carriers, the reality is that in contemporary healthcare, all information is digitized. From lab values, to point-of-care testing, to online mental health forms, and more, information by and about patients resides in servers, computers, chips, and drives. Wearable devices monitor heart rate, blood pressure, glucose levels, and electronic health records (EHR) store demographic information alongside the results of MRIs, serum tests, and digitized consent forms. And while digitizing this data supports ease of use in a variety of ways, it also introduces new risks concerning the maintainability of personal privacy.

Digitized data is pervasive in healthcare, and there are any number of ways such data can be captured—both by those who need access and those who simply want access (authorized or unauthorized). Consider, for example, telehealth “visits” that are streamed over the Internet. Aside from the simple logistics of understanding who is participating in the encounter real-time—with the possibility of people standing “outside the frame”—the medium used for streaming must be properly encrypted to mitigate the risk of the feed being hacked or hijacked.

To address challenges that monitoring devices, EHRs, telehealth encounters, and more create, all systems should utilize HIPAA-compliant software to safeguard patient information and maintain the integrity of the virtual healthcare environment. But as importantly, humans developing and using such technologies must do so in ways that mitigate, if not eliminate, the possibility of unauthorized exposure of private data.

EHRs, PHRs, AND PORTALS

Of course, records captured for long-term use, like the information in an EHR, can be all the more challenging to protect. The widespread use of EHRs has been of great benefit to healthcare providers, offering convenient and searchable access to extensive patient information. This data can also be organized, analyzed, and cross-referenced using tables, lists, and values drawn from evidence-based sources. Of course, any online data is at some risk of technological breaches through hacking or mistaken data-dumping, and along with good security must exist good policies for how any unauthorized access would be handled.

But further, most EHR systems have made personal health records (PHRs) available, making the task of securing EHR data increasingly complex. Particularly, with the Twenty-first Century Cures Act of 2016 (finalized in 2022), there is widespread access to PHRs through patient portals. A clear challenge, for example, is the records of minors or those of patients’ deemed to lack decisional capacity.

For minors, parents may have ready access to their child’s patient portal, and restricted access to the child’s information should follow legal and ethical norms, requiring purposeful programming of the EHR/PHR systems. For example, some states do protect minor privacy when minors are legally allowed to consent to certain treatments for conditions like sexually transmitted diseases (STDs). Professionally, the American

Academy of Pediatrics (AAP) has recommended, as well, that “Adolescents should have the right to exclude parents from their PHRs when law dictates that they may be treated without parental consent. When these features are used, health care professionals need to know that these exclusions are in place” (AAP, 2009). However, ready access to PHRs with no systematic thought regarding exclusion criteria for parental access means that parents may learn about a child’s STD or birth control prescription (and so forth) when the child would otherwise wish this information to remain private.

Similarly, when an adult patient lacks decisional capacity, often family members are granted access to their information, even if those family members are not the legally identified surrogate decision maker. And even when they are legal decision makers, once granted access, this usually includes access to all records within the chart, not just those relevant to the current illness or injury.

Of course, these access issues are not unique to EHR data, but having ready access from almost anywhere through a patient portal magnifies the risks to privacy compared to that of paper-only copies of medical records. The AAP itself notes, “most systems are not capable of allowing ...restrict[ions] to different portions of a patient’s electronic health information,” (AAP, 2012). As such, patient information not germane to current conditions may be accessible to parents of minors, surrogates of adults, or even just family granted temporary access by the patient for a specific purpose and timeframe.

BIOBANKING AND THE SPECTER OF DATAMINING

Though there are a great deal of ways in which technology in medicine can undercut personal privacy and professional obligations to confidentiality biobanking serves as a particularly illustrative example. Originally established as storage facilities for human blood and tissue, biobanks have become crucial for medical research largely due to the data associated with these materials. A large amount of data can be garnered from a wide variety of banked materials, but genetic data, in particular, demonstrates well the risk to patient/participant privacy, because while much of the stored material is purposefully “deidentified” before it is made available to researchers, it remains possible to reconnect PHI with some of those banked materials. This vulnerability arises from several forces at play.

Given the growing use and importance of biobanking, in 2018 the US federal government finalized a revision of what is known as The Common Rule—the federal regulations governing much of the human subjects research done in the United States. The updated regulatory language explicitly permits the extensive use of biobanked materials in research without the need for consent, so long as the material is deidentified. While this change has been hailed as a major advancement for research, facilitating smoother compliance with regulations, it also has the consequence of easing the passing of genetic material around the globe in the service of research while the individuals whose material is being used know nothing of its use.

Since the material is deidentified, it might be reasonable to suggest that little-to-no risk exists for the people whose genetic material is being used. But the technical reality is that each individual's privacy is at risk. In 2013, using the data from the biobanking project known as the 1000 Genome Project (launched in 2008), bioinformatics researchers used the genetic markers in the databank and publicly available records—from genetic databanks within the US National Institutes of Health (NIH) to local public health and city director records—to reidentify roughly 5% of the genomes in the project (Gymrek et al., 2013). Subsequently, new techniques (grounded in new AI and machine learning technologies) have been developed that indicate that the vast majority of material stored with genetic markers can be re-identified. And while research consent forms do indicate the risk of privacy breaches when participating in biobanks, the language hardly describes the possibilities of identification accurately, revealing limitations in our current systems to safeguard individual privacy in medical research.

Of course, careful security measures and strict protocols can mitigate the risks to privacy in cases like these, but hacking is a reality in our culture, and mistakes can also occur. The digital nature of our personal information simply makes identifying individuals in clinical and research settings possible, even if not probable. It is important that institutions, investigators, and providers are vigilant in their attempts to eliminate breaches while being transparent to patients and participants about the real possibilities of losing privacy because of the technologies employed by healthcare.

CONCLUSION

In the years to come, the ubiquity of technology will only increase across various areas and practices within healthcare institutions and among personnel—from the application of data-driven artificial intelligence to the expansion in the use of implantable devices for monitoring, and even adjusting, aspects of our physiology. All this technology relies on and feeds into stores of data—data that originates from specific individuals and often retains enough markers to identify uniquely the sources from which it came. As such, the privacy of these individuals will always be at some risk. Therefore, it remains imperative for healthcare to foster a culture of confidentiality, even if it cannot guarantee it. Only by championing a culture of confidentiality will institutions and providers practice in ways that deliberately and effectively mitigate the very real risks to the privacy of the patients, participants, and people they serve.

REFERENCES

- American Academy of Pediatrics. (2009). Policy statement—Using Personal Health Records to Improve Quality of Health Care for Children. *Pediatrics*, 124(1), 403–409.
- American Academy of Pediatrics. (2012). Policy Statement—Standards for Health Information Technology to Ensure Adolescent Privacy. *Pediatrics*, 130(5), 987–990.
- Goodman, K. (2022). Confidentiality and Privacy. In D. M. Hester & T. S. Schonfeld (Eds.), *Guidance for Healthcare Ethics Committees* (2nd ed., pp. 85–94). Cambridge University Press.
- Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying personal genomes by surname inference. *Science*, 339(6117), 321–324.
- Hester, D. M. (2001). *Community as Healing*. Rowman & Littlefield.
- Siegler, M. (1982). Confidentiality in Medicine—A Decrepit Concept. *New England Journal of Medicine*, 307, 1518–1521.
- Zaner, R. M. (1988). *Ethics and the Clinical Encounter*. Prentice Hall.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 11

Privacy Considerations in Archival Practice and Research

Katrina Windon and Joshua Youngblood

INTRODUCTION

Archives exist to preserve and promote cultural heritage and history. In keeping with the goal of supporting research and reuse, the archival mission is inherently bound to the idea that archival records are meant to be used. Privacy, to archivists, may be seen as a right, a restriction, a privilege, a protection, and a shield. It is interwoven throughout all aspects of archival practice, from discussions with potential collection donors to the appraisal and description of archival records to the provision of records to researchers. At each stage, archivists seek a balance between sensitivity to the rights and well-being of creators and subjects and responsibility to researchers and the access mission.

K. Windon (✉) · J. Youngblood
University of Arkansas, Fayetteville, AR, USA
e-mail: windon@uark.edu

J. Youngblood
e-mail: jcyoungb@uark.edu

The Society of American Archivists' Dictionary of Archives Terminology defines privacy as “n. 1. the quality or state of being free from public scrutiny 2. the quality or state of having one’s personal information or activities protected from unauthorized disclosure by another” (2023). Archivist Elena Danielson, however, defines privacy not as a passive quality or state, but as an ability imbued with agency: “the ability to control personal data—how it circulates in society, in archives, in publications, and on the Internet” (2010).

Statutes regarding information privacy proliferate, as do institutional policies and decision-making frameworks. There is no single, unified framework for determining what precisely constitutes a privacy concern in archival records, even for entities operating under the same legal frameworks. The archival conception of privacy is not particularly unique from that of other disciplines—it is, in fact, deeply shaped by the disciplines of records creators—but the archival approach toward privacy is distinct in that access rather than privacy is the end goal. One notable exception is grounded in the fact that archives are not merely record holders. They are also records creators, and archivists’ approaches toward archival patron records are grounded in the broader library principle that the privacy of patron circulation data is an absolute right (albeit one challenged by the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, also known as the USA PATRIOT Act and other legislation in the United States).

Types and components of archival records that might be considered private are multiform and range from the mundane to the esoteric, including (but not limited to):

- Personally identifiable information (PII)
- Health information
- Educational records
- Financial information
- Records containing passwords and security information
- Personal confessions and discussions of vulnerable topics
- Documentation of immigration status
- Legal materials intended to be covered by attorney-client privilege
- Trade secrets and confidential business information
- Culturally sensitive or taboo materials.

The privacy issues of all other fields can find their way into an archivist's domain, where they intertwine with each other and complicate an access-focused mission.

Danish archivist Eric Ketelaar identified five layers of privacy protections for private records held in public archives: (1) Legislation; (2) Transfer conditions; (3) Researcher agreements and ethics; (4) Repository access and security policies; and (5) A two-part "human dignity" test, to occur before the records are even acquired, asking, "[W]hich risk accrues to human dignity through the disclosure of confidentially imparted data?" and "Is that risk acceptable in the light of an identifiable advantage for the individual or for society?" (1995). These layers span all aspects of the archival process, often overlapping.

Archivists' roles as preservers and providers of access to information and to the protection of privacy have important consequences for society at large; as archivists Richard Cox and David A. Wallace have argued, "[p]rivacy and access to information may be the distinctive hallmarks of the modern Information age, and as a result, archivists and records managers should have pivotal roles to play" (2002).

The archival profession is guided by best practices from its professional organizations; in the United States, this is primarily the Society of American Archivists (SAA), and internationally, it is the International Council on Archives (ICA). These bodies set best practices, but do not enforce them; it is up to individual practitioners to apply the principles to their own professional contexts, and up to their co-workers and peers to serve as checks and balances.

The ICA Principles of Access to Archives and the SAA Code of Ethics and Principles are very similar in their core messaging, and that similarity is extremely significant in a field where practice and standards vary widely internationally. Even Canada and the U.S., which both have graduate programs accredited by the American Library Association (ALA), do not share a descriptive content standard. There are also wildly varying regulatory contexts. For instance, in the European Union, the General Data Protection Regulation (GDPR) offers more stringent personal data protection regulations than are present in the United States, and many nations around the world have nothing comparable to the United States' Freedom of Information Act (FOIA) laws, or even the principle that a government should be accountable to its citizens. Yet among international archivists there are agreements on these common principles—that

access is the primary goal, but that privacy must be respected—even as interpretation and application may vary.

The weighting of privacy versus access has not been a constant. As recently as 1986, archivist Alice Robbin's survey of state archivists found that most prioritized personal privacy over access considerations (Robbin, 1986). However, professional attitudes have evolved in the decades since, and the modern archival access mission means that personal privacy, even when respected and protected, is never the sole criterion when considering how to handle archival records.

Scholars such as Michele Caswell, Marika Cifor, Anna Culbertson, and Amanda Lanthorne have advocated for an approach based on an ethics of care (Caswell & Cifor, 2016; Culbertson & Lanthorne, 2021). This approach to privacy in archives involves thinking of issues as person-focused rather than institution- or issue-focused. For a particular collection, a particular set of records, the idea of the potential for harm is not abstract or anonymous. If it was, there wouldn't be a personal privacy issue. There are real people or real communities that may be impacted, and good intentions alone aren't enough for responsible stewardship.

This chapter provides an overview of privacy considerations and conceptions in archival practice, but a variety of other scholarship explores this topic and many related sub-topics in further depth. The most extensive works on the subject to date are Heather MacNeil's *Without Consent. The Ethics of Disclosing Personal Information in Public Archives* and the Menzi L. Behrnd-Klodt and Peter J. Wosh-edited *Privacy and Confidentiality Perspectives: Archivists & Archival Records* (Behrnd-Klodt & Wosh, 2005; MacNeil, 1992). Both volumes are now out of date with regard to many specific laws and policies but remain deeply relevant in their discussions of ethics and practical considerations. The archival literature establishes privacy's status as a deeply relevant but unsettled theoretical and practical territory—one whose terrain is continually changing in response to new laws and shifting perceptions.

PRIVACY CONSIDERATIONS DURING ACQUISITION AND APPRAISAL

Privacy considerations in archival practice begin long before a researcher ever asks for records, and even before records enter an archival repository. The choices made during the acquisition and appraisal stages serve as a key foundation for future decision-making and include considerations

regarding creator intent, third-party privacy, donor restrictions, legal and statutory restrictions, and ethical considerations.

Record Creation, Creator Intent, and Donor Responsibility

Privacy considerations may vary depending on how and when records are acquired by an archival repository. Unlike records managers, who typically work with records once they may have already served their primary function but are still in active use by the creating or commissioning entity, archivists typically manage records later in the lifecycle, often once they've left their originating institution and context. By the time they have reached an archival repository, records have typically lost any urgent sensitivity related to business or trade secrets. That is not always the case, however. Particularly in community archives, but also sometimes in cases where traditional organizations are trying to collect documentation of an event as or right after it happens, such as after a local disaster or tragedy, archivists and information professionals may be involved in the creation of a collection. When those doing the archiving are also active participants in the creation of records, there are additional considerations—the aspects of privacy determination that are typically left to the creators are now also vested with the archivists.

In recent decades, archivists have looked to web archiving as a way to preserve a record of under-documented groups and movements, as well as of contemporary events. However, such collecting initiatives can bring ethical challenges and raise questions about user privacy. Several researchers have noted that even when posting on public platforms, creators may have certain expectations of privacy. Ethical issues in preserving such content, often originally intended to be ephemeral or expected to be seen by a limited audience, may be compounded in cases of documenting protest movements or other cases in which posts may be used as incriminating evidence or put an individual at risk of harassment (Breed, 2019; Custers et al., 2014; Lindstrom, 2019; McCrow-Young, 2021; Velte, 2018). Archivist Ashlyn Velte, in her investigation of emerging archival practices of social media documenting activist movements, notes that “the archival profession is struggling to document sensitive groups without unintentionally endangering communities,” and identifies a need for more refined ethical approaches when acquiring such records (2018).

Archivists balance the need to preserve historically significant content with the desire to respect creators' personal privacy and intellectual property rights. This balance can be difficult to get right, but new digital tools show promise in assisting content review. Angeliki Tzouganatou has argued that a guided approach with artificial intelligence (AI) tools could allow for greater democratization of access to born-digital collections, including those containing social media, that foreground inclusive collecting while safeguarding personal privacy ([2022](#)).

In the more typical case where archivists are not records creators or co-creators, however, there is always some degree of responsibility on the donor or transmitter to identify private materials, and then either not donate the materials or arrange for an appropriate restriction, if needed. Some transfers, particularly of organizational and government records, are guided by records retention schedules (plans identifying when certain categories of records should be retained, destroyed, or transferred to an archival repository) or legal mandates, and are not subject to the creator's desires. But with personal papers, archivists will generally note that the greatest responsibility rests with the donor, who may be the creator, their heir, their estate executor, or some other party.

A well-known case of an executor disregarding a creator's wishes is that of writer Franz Kafka, who burned many of his papers and entrusted his executor, Max Brod, to incinerate the remainder after Kafka's death; Brod instead published them, and the collection was eventually donated to the National Library of Israel, for which this subversion of creator intention is advertised on the digital collection website as an interesting bit of provenance, not a guideline for how or whether to provide access ([The National Library of Israel, 2023](#)).

In contrast to the Kafka example, estate manager Rob Wilkins did have a steamroller run over a hard drive containing the late novelist Terry Pratchett's unfinished works, per Pratchett's desires ([Haigney, 2017](#)). Archivist Sara S. Hodson recounts how novelist James Joyce's grandson, Stephen Joyce, destroyed family correspondence and unapologetically explained it as a necessary action to safeguard his family's privacy ([2004](#)). Certain professionals, such as lawyers, must also adhere to professional ethics that privilege the privacy and confidentiality of client records over information access ([Behrnd-Klodt, 2008](#); [Hobbs, 1992](#)).

In other cases where a creator's wishes may be less explicit, donors may make privacy decisions based on their own comfort levels. Within the University of Arkansas Libraries Special Collections is a collection of

correspondence between a soldier during WWII and his wife that was donated to Special Collections by their son after their deaths; neither creator nor recipient was involved. The University Libraries fully digitized the correspondence and placed it online as a digital collection that includes both innocuous, quotidian letters, and others that delve into personal tragedy. Depending on one's own personal comfort levels, the idea that this couple's story is now fully open to the public, thanks to a descendant's commitment to sharing it, may be either inspirational, or cause someone to second-guess ever passing down any of their personal papers to their family members. That's because conceptions of privacy are personal and contextual, which can make the archivist's job particularly challenging.

To some extent, the degree to which archivists rely on donors to self-identify materials that need to be restricted, and conduct their own due diligence before transferring records, is a matter of expediency. It is also an extension of the belief that those closer to the creation of records are more knowledgeable about their original context and are better equipped to make those decisions. “The third parties represented in a manuscript collection donated to a repository *may* have legitimate privacy rights,” archivist Mark A. Greene conceded—but his view was “that the archival profession is not (and to the extent possible should not be) in the best position to determine whether those rights would be violated by permitting access to the donated collection. The donor should have that responsibility, just as he/she has it up until the time the papers are donated” ([1993](#)).

Third-Party Privacy

Acquisition is also a time for information-gathering about the potential for sensitive/protected information in a collection that the donor may not personally be concerned about: that of third parties whose information is represented within the collection materials. Archivist Marybeth Gaudette calls these third parties “blind donors” and argues their rights should be a priority for archivists, just as the privacy rights of donors are ([2003–2004](#)). Third-party creators are rarely called on to provide their consent for archival materials to be donated, or offered involvement in deed of gift negotiations. Lafayette College is relatively unique in having specific workflows and policies relating to third-party privacy for its Queer Archives Project—but even it does not actually call for consulting the

third parties, just considering them and potentially imposing restrictions on their behalf (Queer Archives Project (QAP) Team 2020).

Issues of third-party privacy are particularly significant when the third parties are members of vulnerable populations, such as those who are incarcerated, are undocumented, or are victims of state-sponsored violence or genocide. Archival repositories have struggled with the best ways to sensitively handle such materials. Well-documented cases of such quandaries include the records of the Mississippi State Sovereignty Commission, which conducted invasive surveillance of Civil Rights leaders (Schwind et al., 2002; Speer, 1999), and the records of the Stasi, the East German secret police who routinely surveilled the civilian population (Beattie, 2009; Danielson, 2004; Schwartz & Cook, 2002). While these types of records may typically reside in government archives, records of vulnerable populations who had little or no agency in the creation of records involving deeply personal and potentially harmful information about them may exist in any kind of archival repository.

A particularly unique third-party privacy consideration is related to traditional knowledge (TK), or indigenous material that is believed to belong to a group or culture rather than to an individual. Archivist Lara K. Aase, writing of her stewardship of indigenous archival collections, notes that she goes against the general archival trend of providing access: “Professionally, therefore, I prefer to err on the side of caution and to restrict access for a number of reasons. I do not believe the pursuit of knowledge for its own sake trumps an individual’s or a culture’s desire for privacy” (2020). This approach is supported by the SAA-endorsed *Protocols for Native American Materials*, which call for archivists to manage Native American records differently, noting that “[p]rivacy rights extend to groups in some situations. The limited right of organizations, governments, and families to associate in confidence may apply to American Indian tribes who wish to minimize or prevent intrusion into their practices” (2007). Archivist Kay Mathiesen, in line with the *Protocols*, has also argued for Native Americans’ moral rights related to the management of their traditional cultural expressions and knowledge (2012).

Negotiating and Renegotiating Donor Restrictions

According to the Association of College & Research Libraries (ACRL) Code of Ethics for Special Collections Librarians (2020), “Special collections practitioners have a responsibility to ensure the privacy and confidentiality of users, donors, record creators, record subjects, and vendors.” In order to fulfill this responsibility, the Code of Ethics recommends that “[w]hen working with potentially sensitive information within collections, practitioners prioritize access while recognizing the need to respect confidentiality of some materials, including the possible use of time-delimited restrictions. Practitioners are transparent with donors and users about the potential legal limitations of any confidentiality promises” (2020).

In keeping with this guidance, during the pre-acquisition stage, archivists will talk with potential donors about any privacy or sensitivity considerations within the records, and whether any restrictions are needed. If restrictions are merited, then they will typically be noted in the deed of gift, a donation instrument used by archival repositories to formally document transfer and outline expectations and commitments on the part of both the donor(s) and the repository. When imposed, restrictions should be specific, time-bound, and mutually agreed upon. Moreover, restrictions must be applied equitably within the archival institution’s mission and operating framework, rather than arbitrarily or prejudicially privileging certain groups’ access over others.

The majority of advice in archival scholarship regarding deeds of gift is that they should be final about whatever transfer of ownership or rights is occurring—i.e., they should not set up an ambiguous situation in which the donor may request their materials back later on, perhaps after the repository has already invested significant resources into the collection. Some scholars have urged for more flexible approaches, however. Archivists Anna Culbertson and Amanda Lanthorne recommend including revocation clauses for consent, particularly for materials that may be digitized, as a way of ameliorating power imbalances and giving donors greater agency, although they acknowledge that such a model may be difficult for most institutions to implement (2021).

Archivists’ ability to protect privacy (and, by extension, donors’ trust in that ability) is, several scholars have argued, essential to archival collecting and the preservation of a fuller historical record, free from over-sanitization and purging by possible donors. “Confidence in the

discretion of the archives and in the enforcement of restrictions demonstrably contributes to the creation and preservation of important documentation,” claims archivist Elena Danielson, noting that, somewhat paradoxically, it is reasonable restrictions that can ultimately lead to greater access (2010). “Trust is essential to build donor confidence in the archivist’s ability, including the resolve to keep sensitive material confidential, to protect family secrets, and to ensure copyright is respected,” declares archivist Rob Fisher (2015). Pekka Henttonen argues similarly: “Public records react to exposure like photographic film. If it is known that the information will become accessible to outsiders, it starts immediately to affect the content of records. [...] Thus, protection of privacy is not only a problem for archives: it is also a tool for guaranteeing that full and frank documentation is generated in the first place and then preserved” (2017).

Some institutions may be better suited than others to care for materials that merit restrictions, such as private institutions, or public institutions in jurisdictions that provide specific exemptions for archival records from any FOIA or public records laws. Archivist Eira Tansey has argued that public institutions should reconsider accepting any private donations that come with donor restrictions, both to ensure that all promises to donors can be kept (and not undermined, for instance, by FOIA requests or subpoenas), but also in recognition of the duty those institutions have to the public that funds them (2021). Private archives may have a great deal more flexibility to offer their donors, and community archives in particular have explored donation mechanisms that sometimes look very different from a traditional deed of gift in order to ensure donors have agency and ownership over their materials. For instance, archivist Judith Schwartz describes the very granular discussions she had at the Lesbian Herstory Archives with donors about how and the degree to which they wanted their materials to be attributed, shared, digitized, and/or promoted (1992).

There is, then, broad consensus in the archival profession that reasonable donor-imposed restrictions serve a valuable and even essential function—but there is debate about when and how much they are justified.

Legal and Statutory Restrictions

Within the United States, there are four primary federal laws or legal rights governing privacy protections in archival collections.

The first of these laws is the Family Educational Rights and Privacy Act of 1974 (FERPA), which protects certain educational records.

The second is the 2000 Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) issued by the U.S. Department of Health and Human Services as part of the implementation of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and which protects certain health records.

The third is the Freedom of Information Act (FOIA), which governs which federal government records are required to be made available to the public and, most relevant in this context, also specifies which kinds of records are exempt from its provisions, for reasons that may include personal privacy. Unlike HIPAA and FERPA, which are both withholding statutes (preventing certain records from being shared), FOIA is a disclosure statute—that is, a record may be exempted under FOIA, but that only means its release is not mandated, not that it can't be released.

The fourth is the constitutional right to privacy, which is the only federal protection that applies to all archival repositories.

Laws like FERPA and HIPAA only apply to certain institutions, or covered entities (for example, FERPA applies to records maintained by educational institutions receiving federal funding, or by organizations/individuals acting on their behalf). Many repositories that are not legally bound by these laws, due to their status, will still use them as models for what reasonable privacy protections are, and so these laws do have an impact beyond the statutory one. For example, HIPAA applies to protected health information created or collected during the process of health care provision by a covered entity. Someone's personal diary in which they detail their own or family health issues is not covered by HIPAA, but some archivists may use HIPAA as a framework for thinking about how to approach access to that diary.

There is wide variation among data privacy laws, FOIA laws, and other privacy protections not only at the statewide level, but also sometimes at the county or municipal level. Portland, Oregon, for instance, has more stringent data privacy protections than the state of Oregon overall. This variation makes it difficult for archival organizations, even regional ones, to provide useful guidance for their members, and makes it difficult for archivists to collectively advocate for changes. Most records laws acknowledge the importance of context, which introduces further variance. A person's address as standalone information is directory information, and would generally be public under FERPA, but if it were tied to health

information at a covered entity, it might be protected under HIPAA. Considerations may also be role-dependent. The height and weight of a university student would likely be considered private by many institutions, but for student-athletes, the University of Arkansas and other institutions have identified those data points as directory information.

Archivists must follow applicable laws but must also ensure that their policies and procedures do not create a legal obligation where there isn't one if they do not have the resources to uphold it. Most archivists are not lawyers, and have limited access to internal or external legal counsel, so in many cases, archivists are left to self-educate on the laws that apply to them, and how; thus, it is perhaps unsurprising that many archivists err on the side of caution in relation to health and education records, in particular.

Another consideration in the application of privacy laws is the passage of time. In the United States, the right to individual privacy is generally understood to end with death. Notable exceptions are that FERPA provides no explicit expiration date (and in the absence of one, many university archives have set their own time frames, such as 72 (following the Census restriction period), 75, or even 100 years from the date of a record's creation, and that HIPAA extends 50 years beyond an individual's death in order to protect descendants' privacy. Although some scholars have argued for the idea of post-mortem privacy rights, particularly in the context of reputational networks, these have not yet been legislated (Buitelaar, 2017; Craik, 2009).

Similarly, time-based restrictions imposed either by donors or archivists are based either on an intent for a specific time frame to act as a proxy for a likely lifespan, or with the assumption that the relevant privacy concerns will lessen over time (for example, as someone leaves public office or retires from the workplace). However, archivists do not universally recognize these perceptions of the passage of time as a lessening force on privacy. Heather MacNeil advises that “[t]he process of establishing access guidelines requires a sensitivity on archivists' part, first, to the common law principle that rights to privacy do not diminish significantly over the lifetime of the individual to whom the information relates and second, to the common sense principle that, in some cases, these rights are not extinguished with the death of the individual” (2005).

Archivists have, with varying degrees of success, sometimes lobbied for changes to or clarification of privacy laws. In 1993 SAA, ALA, and the

ACRL successfully lobbied the FERPA compliance office to provide guidance on unpublished undergraduate theses, and the office confirmed that theses could be made available without violating FERPA, even without the author's permission (Chute & Swain, 2004). 2013 changes to the HIPAA Privacy Rule that excluded otherwise covered information of those who had been deceased for more than 50 years occurred in part because of the advocacy of archivists; two archivists testified before the committee, and SAA as an organization endorsed the change during a public comment period (Novak Gustainis & Letocha, 2015). Other laws have been enacted or changed due to the advocacy of archival users, such as through the Federation of Genealogical Societies' efforts to increase access to historic vital records (Cooke McKay, 2002).

Ethical Considerations

While all archivists are bound to follow applicable laws, and generally understand what those laws are, interpretations may vary. For all the influence they have on the archival profession and on the availability of materials for research, those laws only cover a small fraction of records and privacy considerations. As Sara S. Hodson has noted, “[t]he potential for revealing private information more often constitutes an ethical concern than a legal one” (2004).

Professional codes of ethics, such as the SAA Code of Ethics and the ACRL Code of Ethics for Special Collections Librarians, lay out some basic principles, with few specifics. Elena Danielson identifies a flawed premise of many of these codes, however, noting that “[i]t is disingenuous to write ethical guidelines saying that archivists should protect the privacy rights of data subjects. Violation is part of the process. The real question is how it can be meliorated” (2010). That is, she goes on to explain, “The violation of privacy is an intrinsic and unavoidable part of archival work because it involves the secondary use of documents, which were originally created for another, so-called primary, purpose” (Danielson, 2010). This kind of violation is related to information science scholar Helen Nissenbaum's concept of “contextual integrity”—that is, people may willingly share some information about themselves in a certain public sphere, but be dismayed to have it shared or aggregated in contexts outside of the one in which it was originally shared (1998). While such violations of contextual integrity are inherent to the archival process, they may be exacerbated in some aspects of archival work that bring records further

from their original private or quasi-private sphere into much more public ones, such as when analog collections are digitized for online access.

The ethics of care framework, as well as other ethical lenses, tend to put the greatest emphasis on the potential for harm when making decisions about ethics-based restrictions. Heather MacNeil concludes that “[r]espect for the humanity and dignity of all persons, and the self-containing sense of responsibility arising from it, are the forces that will guide archivists through the ethical dilemmas that present themselves when competing values of individual autonomy and freedom of inquiry confront each other” (1992).

Choices and Constraints

Traditionally, before archival collections are made fully available to the public, they are processed, an endeavor that includes arrangement, description, and preservation, and typically results in a finding aid, or a research guide. New strategies as some repositories try to increase access while lacking the staff time to fully process their collection backlogs mean that traditional processing may not always occur, and regardless, it will not always occur at the same level of detail for each collection. However, processing is typically when the most attention is paid by archival staff to a collection, and when the most thorough review for potential privacy issues will occur. It is thus a crucial point of assessment and intervention. A key guiding framework for privacy considerations will be any restrictions laid out in the deed of gift form. If there are none, the processing archivist’s job will be that much easier. Figure 11.1 maps out a possible decision-making workflow, demonstrating some of the considerations an archivist may take into account.

Options for implementing privacy protections, when a processing archivist has determined they are merited, can vary. Approaches include:

- Restricting materials for a set period
- Requiring that redacted access copies be created for any research request
- Proactively creating redacted access copies
- Implementing access limitations and basic screening procedures, such as a researcher application process, or limiting researchers to those affiliated with an institution
- Requiring researchers to gain approval from a third-party review board, such as an institutional review board (IRB)

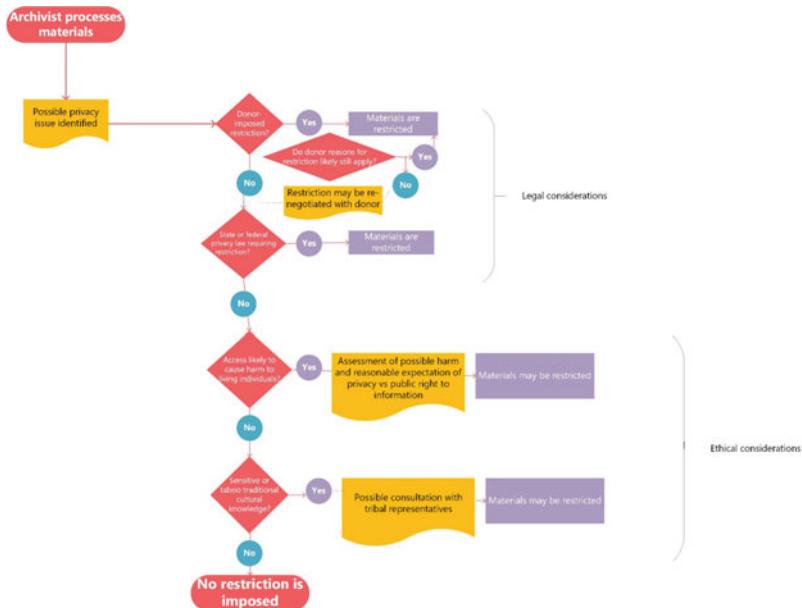


Figure 9.1: Sample decision tree for evaluating archival collection privacy issues

Fig. 11.1 Sample decision tree for evaluating archival collection privacy issues

- Requiring researchers to sign a non-disclosure agreement, an indemnification form, or some other form of waiver
- Returning materials to the donor
- “Sanitizing” materials by redacting originals
- Destroying materials.

Not all institutional staffing levels or policies may allow for all these approaches to be options; in particular, the idea of “sanitizing” records may be viewed as unethical by some. In addition to being irreversible, and removing context, such an approach may take away the possibility of someone being able to retrieve their own records (a key aspect of GDPR and of the principle of information self-determination), and potentially deny attribution.

Writing of a San Diego State University digital project that redacted correspondent names to protect the personal privacy of vulnerable individuals, Culbertson and Lanthorne acknowledge the downside—"redaction effectively turned the letters into orphan works so that anyone could potentially publish the content of a letter without the correspondent's consent. Whether intentional or not, this gave no control or agency to the very population the Library was trying to advocate for and protect" (2021). Humanities scholar Samuel Edquist, borrowing from the scholarship of Swedish archivists, has written on what he calls "ethical destruction," and notes an inherent tension in that "there are two aspects of power in documentation, where the same record can be regarded as oppressive and emancipatory. Advocates for ethical destruction argue that archival silence is for the benefit of the persons involved in records. On the contrary, archival existence is often described as a prerequisite for history writing, identity, and justice" (2021).

Privacy considerations and protections are not lump-sum. A use restriction does not necessitate a corresponding access restriction, and a decision not to digitize materials does not preclude allowing physical access or even allowing researchers to create digital copies.

While there are, as discussed, numerous meliorating options for archivists to pursue, a commonality among them is that they take time—a commodity always in short supply for archivists, who are often at understaffed repositories and working with backlogs of unprocessed collections that may have accumulated over decades. The substantial time investment required for item-level review, redaction, and other methods is not feasible for many repositories. Even for born-digital collections, where PII-screening tools may help automate some of the process, manual review is required to weed out false positives, and many privacy issues will never be caught by systems that look for patterns (such as digits in the format of a social security number), not for nuance. The time-intensive nature of the most comprehensive approaches toward considering thoughtful, reasoned privacy protections has led some archivists to advocate for largely abdicating responsibility in this area.

One of the more notable proponents of this was Mark Greene, who warned archivists against trying to apply their own judgment beyond what donor stipulations and legal frameworks required: "If we do respond by preventing access to all collections which might contain private information until all parties represented in the papers are dead, how will we explain to our publics and our resource allocators this retrogression to the

role of stingy custodians and arbiters of privacy and ‘legitimate’ research? If on the other hand we decide to shoulder the responsibility for screening collections for material which invades the privacy of third parties, then we also invite the legal consequences if despite our efforts material later deemed to be an invasion of privacy is made accessible to a researcher. Surely we need not martyr ourselves on the altar of privacy rights” (1993).

Aside from the questions of time and expertise, there is also a risk of being overly protective, to the point that measures intended to be protective may be harmful. Archivist Bill Landis warned that “when archivists talk about privacy and confidentiality issues, I think it collectively brings out our most conservative streak. I typically see what I’d characterize as downward-spiraling scenarios of privacy-violation horror into which we talk ourselves” (2009). Similarly, Hodson cautioned about “an over-active sense of ethics that may afflict some archivists” (2004). An overly conservative proactive approach to protecting personal privacy can act as a form of censorship, impeding research and undermining an archives’ mission. It may also contribute to an overly paternalistic or prescriptive approach about what is considered sensitive or shameful, potentially perpetuating prejudicial attitudes in the name of protection. Moreover, Behrnd-Klodt warns, “[a]rchivists who seek such affirmative restriction voluntarily set a high standard of conduct that may be difficult to execute,” setting themselves to a standard they cannot live up to but for which they may be accountable (2005).

ARCHIVAL PRIVACY: A RESEARCH PERSPECTIVE

Privacy is a key concern for research services and teaching as well as acquisition, accessioning, and processing. Although the restrictions and procedures research archives follow in order to service records for access are dependent upon the determinations made by acquisitions and processing archivists, the staff responsible for interfacing with the public, guiding researchers through access policies, and providing reference assistance—archivists who we will refer to here as research and reference archivists—also play an integral role. Most archivists believe that everyone should have access to records for research. They promote the democratic ideal that historical evidence should be available to anyone. In keeping with that ideal, professional best practices encourage archivists to provide equitable access to anyone with interest. However, that access must be in keeping with institutional policies in place to protect the archives or

the larger organization in which it resides from legal liability, as well as mitigate the burden on infrastructure, staffing, and other resources.

Like all areas of professional archival practice, ethical standards guide how institutions should assist researchers and ensure that their collections are both accessible and responsibly managed, including how public servicing of materials is conducted. “Ethics apply to all aspects of access, including providing physical and virtual access, producing reproductions, granting uses and permission, and adhering to restriction and legal regulations,” as archivist Cheryl Oestreicher makes clear (Oestreicher, 2020). Establishing appropriate policies with consistent and equitable service, provided by well-trained staff members is a responsibility of research archives, and privacy for patrons at every stage of their research journey is inseparable from that responsibility.

Professional Standards

As an area of concern, patron privacy is addressed in the SAA Code of Ethics. “Archivists respect all users’ rights to privacy by maintaining the confidentiality of their research and protecting any personal information collected about the users in accordance with their institutions’ policies” (Society of American Archivists, 2020). Archival ethics prioritize sustainable practices and policies that serve all of an institution’s stakeholders. Caring for collections and serving communities must necessarily involve an ongoing awareness of the impact of archival work.

As noted above, archivists must be mindful of the ways in which their professional work can function both as *harmful force* and *reparative resource*. As a potentially harmful force, archives can negatively impact the personal liberty and privacy of individuals and communities by granting access to creative works, information, or stories that were never intended by the subjects or creators to be publicly available. As a reparative resource, archives can also make political, social, and cultural information accessible for those seeking to advocate for greater rights and freedom for themselves and others and empower individuals to rewrite history by creating their own narratives (Caswell, 2021).

Archivists are always seeking to balance priorities, and in terms of privacy that means accommodating protections for donors and researchers while providing as much ease of access to and use of materials as possible. For practitioners in areas of institutional archives and research libraries

that interface with the public—research services, outreach, and instruction—it can sometimes be challenging to balance excitement and desire to promote collections with a duty to protect privacy (Oestreicher, 2020). Archival professional standards tend to emphasize the need to achieve the *broadest possible* access. While some restrictions or limitations on access because of privacy concerns may be necessary, professional practice in recent decades has sought to make available all aspects of information possible (including repository-created metadata), along with means of duplication and possible publication, within the constraints of donor agreements and the law.

The Rare Books and Manuscripts Section (RBMS) of the Association of College and Research Libraries identifies transparency about user privacy limitations as an essential duty of special collections librarians and archivists. Staff in academic archives often collaborate with classes and teaching faculty or other programs on campus. These core services to the university community complicate the goals of shielding researchers and their interests from observation or interference while facilitating learning and training less-experienced researchers in how to utilize archival records most effectively. Archivist Elizabeth Yakel noted the transformation in archivists' role in teaching at the turn of the twentieth century: "College librarians have seen their role evolve from that of passive participant in the learning process to a more active teaching role....The content of that teaching has transformed from bibliographic instruction for resources, indexes, catalogs, and materials in physical libraries to a focus on information literacy for information sources internal or external to the library" (Yakel, 2002). Yakel's "Listening to Users," along with a wide array of literature over the ensuing two decades, addresses archivists' roles in primary source learning (2002). However, the area of student privacy within those teaching environments remains understudied.

Every archive that supports research should ensure the security of its materials and users. Methods to do this, whether in the reading room or through email or other virtual channels, include registration of users and presentation of proof of identity; having protocols in place to track usage of materials; and researcher agreements to abide by policies and procedures.

Do researchers and patrons in special collections libraries desire privacy about their research topics and work? Some may as a personal preference, while others may require privacy to protect themselves from unwanted

scrutiny. The desire to preserve a scoop may be another factor—while many researchers have interests in promoting their work in archives, they would typically prefer to be able to control that promotion and its timing.

Archival research can attract scrutiny that inhibits the ability of researchers to seek truth, both in places with fewer protections for individual liberty and in places with well-established legal or constitutional protections where research may still arouse political or otherwise official suspicion or retaliation. The use of archives by researchers seeking to reveal or investigate social conditions and address social, cultural, or political issues—such as in journalism, activism, and socially-relevant scholarship—needs the shield provided by professional archival practice's commitment to patron privacy.

Privacy During Research

Privacy during research entails a balance of security measures in place for the material as well as for the patrons themselves. Reference archivists, as a specialized subset within the profession, are integral in fulfilling the mission of the archival institution and are essential to the management of privacy issues in the archives, whether regarding the origin of the research material or the privacy of researchers. Reference archivists are the intermediaries between collections and patrons, ensuring that established policies are followed (Cohen, 1997; Pugh, 2005; Oestreicher, 2020). Research archivists and others serving patrons in reading rooms will, through the course of their duties and engagement with researchers in order to better guide their requests or facilitate the use of additional services such as duplication, gain some degree of familiarity with the details of the researcher's activities. For security purposes, they will also likely track the materials used by the researcher, either in a database or via paper call slips. This type of documentation is typically disclosed to researchers as part of a researcher agreement or orientation, as documenting researchers without their consent could be considered a violation of their personal privacy. Forms used for registration sometimes provide an option for researchers to consent to be photographed for the promotional purposes of the institution. Many patrons are eager to contribute, but their willingness should not be assumed. Unless consent is explicitly given, the collation or distribution of individual researcher activity represents a potential invasion of privacy.

Personally Identifiable Information (PII) During Research

There are several times within an institution's interaction with researchers when PII might be collected. Archives often require the presentation of, and sometimes a copy of, government-issued identification as a security measure. In addition, archives that require patron registration might require a patron to provide a work or home address, other contact information, or institutional affiliation. If an institution charges fees for reproductions, then researchers requesting copies or digital scans may also need to submit financial PII.

Research services staff in publicly accessible archives have increasingly sought ways to protect PII for research and to create safeguards against accidental or intentional accessing of information for unauthorized purposes. Automated patron registration systems, as well as patron-directed duplication requests, can allow for greater protection of the records of materials being accessed or duplicated by individual researchers.

Documenting Researcher Activity

A central aspect of privacy for patrons is protecting the outcomes of research and further work. Archives should ask for consent before any publication about or photographing of researcher visits. Some archives and research facilities may attract news media, whether because of a noteworthy collection or donation, a special event, or perhaps because of a politician or celebrity visiting; these news crews should not be permitted to film researchers without permission. Management of security footage is also a concern, as well as the perception by users that they are under surveillance in the archival reading room, a circumstance Eric Ketelaar once identified as “archival temples/archival prisons” (Ketelaar, 2002). Strongly encouraging the development of a careful and transparent policy by special collections and archives staff regarding the use of security cameras, the ACRL/RBMS security guidelines make clear that as the “use of cameras involves legitimate privacy concerns for both staff and visitors,” and that this “decision should not be undertaken lightly” (2009). The guidelines suggest that institutions “create clear internal policies outlining who can access security footage, how they would view it, and under what circumstances it would be permissible” (ACRL/RBMS, 2009).

Given that researcher access and privacy are a priority, archives should reject requests from outside authorities for information on research. This

is not always possible, as laws related to freedom of information requests or issues of national security may supersede institutional policies or procedures. For this reason, archives should be cautious in both their creation of researcher documentation or surveillance footage and their retention policies of such documentation, ensuring that they collect no more than is necessary for their operations and security.

Legal Protections for Researcher Activity

Federal law provides some protections for the research process, but laws can also open up avenues for the inspection of research activity. Regulatory frameworks evolve, and changes in the United States and Europe have both restricted access to some records in favor of greater privacy for third parties and, on the other hand, allowed for intrusions upon personal privacy under the auspices of national security or fighting criminal activity. Following the beginning of the War on Terror in 2001 in the United States, the USA PATRIOT Act can be used by the federal government to obtain patron records. This development proved frustrating for many research institutions, from non-profits and public libraries to private and public universities, as it nullified well-established institutional practices and policies. As a result, efforts to further anonymize patron data, such as through new forms or automated registration systems, increased. (Oestreicher, 2020).

THE UNIVERSITY OF ARKANSAS SPECIAL COLLECTIONS AS A CASE STUDY

We can examine an established research archives division at a public university to see both how care is taken to accommodate competing needs and requirements, as well as how ongoing refinement of policies is needed to remain compliant with relevant regulations and legal frameworks. For instance, the Special Collections at the University of Arkansas Libraries has, evident on its website and in posted user research guides, detailed and evolving policies and procedures.

As a repository within a land-grant, public university serving tens of thousands of undergraduate students, Special Collections seeks to balance the university's "student first" mission with demands from researchers in the community and around the world, many of whom

are drawn to its high-profile collections related to international education, civil rights, architecture, and music. Although there is a substantial university archives, most archives available to researchers originate from non-university-affiliated sources, including governmental agencies, non-profit organizations, corporations, families, and creators from fine arts, literature, and scholarly research fields.

Before a researcher ever accesses any collection material, Special Collections is already collecting data from them through online registration forms. However, they also employ disclaimers and data usage statements addressing how data is collected and stored in order to make both the reasons for collection and the limitations of protections transparent. The current forms and systems represent an evolution of policies based on experience, lessons learned, and a growing understanding about how collecting essential information in hard copy could put researcher privacy and material security at risk. The previous paper's form-based system was vulnerable to loss of data and unauthorized access.

Like other institutions that have transitioned to digital patron management systems, the University of Arkansas now uses disclaimer language related to vendor management of data. Disclaimers also make explicit that Special Collections may need to comply with legal requirements and requests, while certain requests from outside parties, such as FOIA requests for user information, are referred to legal counsel.

Granting access to unprocessed collections is a particular challenge for protecting potential PII and other information donors may not want to be disclosed. Collections with politically relevant material, as well as archives from literary, music, or other creative fields with great public interest, can attract immediate researcher demand well ahead of an institution's processing schedule. Special Collections' Access to Unprocessed Collections policy (Fig. 11.2) thus specifies an amount of screening that Research Services staff will conduct for a given research request, as a compromise between access needs, staffing resources, and privacy protections.

An updated framework now in place at many research archives is to inform users of their responsibilities very clearly and in multiple places on websites, registration, and forms in order to establish protection for the institution and avoid overstating its role in the research, discovery, or publication processes. While the responsibility to provide access remains with the institution, the responsibility is on the user to avoid further disseminating PII once it is encountered and to act responsibly within

Libraries Home / Special Collections / Research / Access to Unprocessed Collections Policy and Procedures

Access to Unprocessed Collections Policy and Procedures

The University of Arkansas Special Collections strives to make all research materials available for research as quickly as possible, subject to university policies and guidelines detailed below. Special Collections welcomes any researcher requests to use unprocessed collections for single-use, research purposes and asks that such requests be directed to Research Services, a unit within the Special Collections Division. While Special Collections endeavor to grant access to all requests, Special Collections must weigh access against its preservation, privacy, and administrative commitments.

When a researcher requests access to an unprocessed collection, a Research Services staff member will screen* the requested materials to determine that the unprocessed collection meets the criteria to be opened for access to researchers. Research Services may restrict access to some or all of the unprocessed collection due to Special Collections' legal, institutional, and preservation responsibilities.

Criteria for making unprocessed collections accessible:

Personally-identifying Information (PII) and other types of protected information: The unprocessed collection does not contain any PII, student, medical, or employee/personnel records. If the materials containing confidential information can be safely removed from the collection in a reasonable manner and timeframe, Special Collections will consider opening access to the collection.

Research Services staff will attempt to remove any materials containing confidential information from the unprocessed collection before making it accessible for research; however, researchers should note that this may not always be possible.

Preservation: Many unprocessed collections present preservation concerns, some of which can be hazardous to human health, our facilities, and other materials in Special Collections. Therefore, all materials must undergo a preservation review before Special Collections can make them accessible to researchers. If it's possible to reasonably separate materials that require preservation treatment from the rest of the collection, Special Collections staff will make every effort to do so to allow access to the collection. In some cases, Research Services may create access copies of the original to increase the accessibility of a collection.

Administrative: If an unprocessed collection is scheduled to be processed within one month of the request, Special Collections will ask the researcher to wait until after the collection has been processed to conduct their research.

Donor-imposed Access Restrictions: Some donors may impose access restrictions to some or all of a donated collection during the donation process. Special Collections will not grant access to donor-imposed access restricted materials.

Screening activities: In order for unprocessed materials to be made accessible, a Special Collections staff member must go through the requested containers to insure any legal or institutional obligations to restrict access are met and to confirm there are no environmental and human health hazards present. Special Collections also reserves the right to deny access to some or all of an unprocessed collection if the materials are deemed too fragile or unstable for handling. Special Collections provides up to 1.5 hours of screening activities AND research assistance per semester.

POLICY CONCERNING PERSONALLY IDENTIFIABLE INFORMATION

Some collections may include sensitive or confidential information protected under federal and/or state privacy laws and regulations or under donor terms of gift, including but not limited to medical, educational, or employment records; social security numbers; bank account numbers; or credit card numbers. Researchers who find sensitive information should notify a staff member and agree not to copy or disclose this information. The researcher assumes all responsibility for infringement of right to privacy in his/her use of the materials, and agrees to indemnify and hold harmless the University of Arkansas, its agents and employees against all claims, demands, costs, and expenses arising out of use of archival collections held by the University of Arkansas Libraries.

Fig. 11.2 Updated PII and Access to Unprocessed Collections Policy, University of Arkansas Special Collections (*Image source <https://libraries.uark.edu/specialcollections/research/unprocessed.php>*)

copyright and other guidelines. Some collections may include sensitive or confidential information that has not yet been identified, so Special Collections' researcher agreement form requires that researchers notify a staff member and agree not to copy or disclose such information, should

they encounter it. In this framework, the researcher assumes all responsibility for infringement, allowing the repository to be more permissive in its access policies.

CONCLUSION

Archivists are still navigating the evolving and changing relationship between communities and archives, museums, special collections libraries, and other repositories open to the public for research. Considering possible sensitive information or material communities represented in historical collections might object to having shared publicly, a mechanism to remove content (take-down notices) or respond to requests for repatriation or deaccessioning can be implemented. Archivists must remain informed regarding evolving professional practice and applicable laws and regulations, especially as the availability of archival material digitally increases along with the public demand for digital access.

In her 2022 dissertation, Allison Rae Tyler looks at the impact of recent European Union privacy regulations on social sciences data archives and suggests new conceptualizations of privacy (2022). Her title provocatively asks the question, “Can We Still Archive?” The answer is yes—but not everything, and not without applying a legal and ethical framework to decisions about acquisition, processing, and access. Archivists can rely on donors and researchers as partners and collaborators in identifying and remediating privacy issues within our collections, but we cannot offload the responsibilities we have to those donors and researchers, as well as to other record creators and third parties. Protecting privacy within archival practice is time-consuming, contextual, and a constant balancing act between competing ethical and professional demands. Yet, a greater attention to privacy considerations does not compromise the central access mission of archives—it just makes things a bit more complicated.

REFERENCES

- Aase, L. K. (2020). Censorship or Stewardship?: Strategies for Managing Biased Publications and Indigenous Traditional Knowledge in Special Collections Libraries. In M. Kandiuk (Ed.), *Archives and Special Collections as Sites of Contestation* (pp. 7–36). Library Juice Press.

- ACRL/RBMS Guidelines Regarding the Security of Special Collections Materials. (2009). Revised January 2019; revised June 2023. https://www.ala.org/acrl/standards/security_theft
- ACRL Code of Ethics for Special Collections Librarians. (2003). Revised 19 June 2020. https://www.ala.org/acrl/sites/ala.org.acrl/files/content/standards/Special_Collections_Ethics_2020.pdf
- Beattie, R. E. (2009). Poisoned Madeleine: Stasi Files as Evidence and History. *Faculty of Information Quarterly*, 1(3), 1–11. <http://jps.library.utoronto.ca/index.php/fiq/article/view/15452>
- Behrnd-Klodt, M. L. (2008). *Balancing Confidentiality Concerns and Legal Privileges with Access to Lawyers' Papers*. Navigating Legal Issues in Archives (pp. 125–131). Society of American Archivists.
- Behrnd-Klodt, M. L., & Wosh, P. J. (Eds.). (2005). *Privacy and Confidentiality Perspectives: Archivists & Archival Records*. ALA Editions.
- Behrnd-Klodt, M. L. (2005). The Tort Right of Privacy: What It Means for Archivists...and for Third Parties, pp. 53–60. In M. L. Behrnd-Klodt & P. J. Wosh (Eds.), *Privacy and Confidentiality Perspectives: Archivists & Archival Records* (p. 60). Society of American Archivists.
- Breed, M. (2019). *Capturing a Moment: The Practices and Ethics of Social Media Archiving* (Master's thesis). University of North Carolina at Chapel Hill. <https://doi.org/10.17615/p4ff-zk64>
- Buitelaar, J. C. (2017). Post-mortem Privacy and Informational Self-determination. *Ethics and Information Technology*, 19, 129–147. <https://doi.org/10.1007/s10676-017-9421-9>
- Caswell, M., & Cifor, M. (2016, May). From Human Rights to Feminist Ethics: Radical Empathy in the Archives. *Archivaria*, 81, 23–43. <https://archivaria.ca/index.php/archivaria/article/view/13557>
- Caswell, M. (2021). *Urgent Archives: Enacting Liberatory Memory Work*. Routledge.
- Chute, T., & Swain, E. (2004). Navigating Ambiguous Waters: Providing Access to Student Records in the University Archives. *The American Archivist*, 67(2), 212–233.
- Cohen, L. B. (1997). *Reference Services for Archives and Manuscripts*. Haworth Press.
- Cox, R. J., & Wallace, D. A. (2002). *Archives and the Public Good: Accountability and Records in Modern Society*. Quorum Books.
- Craik, K. H. (2008). Posthumous Reputational Networks. *Reputation: A Network Interpretation* (online edn), January 1, 2009. Oxford Academic, <https://doi.org/10.1093/acprof:oso/9780195330922.003.0009>
- Culbertson, A., & Lanthorne, A. (2021). Praxis, Not Practice: The Ethics of Consent and Privacy in 21st Century Archival Stewardship. *Across the*

- Disciplines*, 18(1/2), 6–21. <https://doi.org/10.37514/ATD-J.2021.18.1-2.02>
- Custers, B., Van Der Hof, S., & Schermer, B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies. *Policy & Internet*, 6(3), 268–295.
- Danielson, E. S. (2004). Privacy Rights and the Rights of Political Victims: Implications of the German Experience. *The American Archivist*, 67(2), 176–193.
- Danielson, E. S. (2010). *The Ethical Archivist*. Society of American Archivists.
- Dictionary of Archives Terminology*. Privacy. Accessed August 4, 2023, <https://dictionary.archivists.org/entry/privacy.html>
- Edquist, S. (2021). The Archival Paradox of Power: When are Records Menaces to Privacy or Evidence of Maltreatment? In A. Öhrberg, T. Berndtsson, O. Fischer, & Annie Mattsson (Eds.), *From Dust to Dawn: Archival Studies After the Archival Turn* (pp. 132–158). Uppsala University.
- Fisher, R. (2015, Spring). Donors and Donor Agency: Implications for Private Archives Theory and Practice. *Archivaria*, 79, 91–119.
- Gaudette, M. (2003–2004). Playing Fair with the Right to Privacy. *Archival Issues*, 28(1), 21–34.
- Greene, M. A. (1993). Moderation in Everything, Access in Nothing?: Opinions About Access Restrictions on Private Papers. *Archival Issues*, 18(1), 31–41.
- Haigney, S. (2017). Terry Pratchett's Unpublished Work Crushed by Steamroller. *The New York Times*, August 30. <https://www.nytimes.com/2017/08/30/books/terry-pratchett-steamroller-unpublished-work.html>
- Henttonen, P. (2017). Privacy as an Archival Problem and a Solution. *Archival Science*, 17, 285–303. <https://link.springer.com/article/10.1007/s10502-017-9277-0>
- Hobbs, B. (1992). Lawyers' Papers: Confidentiality Versus the Claims of History. *Washington and Lee Law Review*, 49(179), 179–211. <https://scholarlycommons.law.wlu.edu/wlulr/vol49/iss1/13>
- Hodson, S. S. (2004, Fall–Winter). In Secret Kept, in Silence Sealed: Privacy in the Papers of Authors and Celebrities. *The American Archivist*, 67(2), 194–211. <https://www.jstor.org/stable/40294276>
- Ketelaar, E. (1995, May) The Right to Know, the Right to Forget?: Personal Information in Public Archives. *Archives and Manuscripts*, 23(1), 8–17. <https://publications.archivists.org.au/index.php/asa/article/view/8465>
- Ketelaar, E. (2002). Archival Temples, Archival Prisons: Modes of Power and Protection. *Archival Science*, 2, 221–238.
- Landis, B. (2009, February 12). “Reconciling Modern Archival Practices and Ethics with Large-Scale Digitization” (notes from panel discussion at “Extending the Reach of Southern Sources: Proceeding to Large-Scale Digitization of Manuscript Collections,” Southern Historical Collection, University

- of North Carolina at Chapel Hill). <https://docsouth.unc.edu/watson/archivalmassdigitization/download/landis.pdf>
- Lindstrom, L. (2019). *Archiving in the Era of Online Activism: Challenges and Practices of Collecting and Providing Access to Activist Social Media Archives* (Master's thesis). Lund University. <https://www.lunduniversity.lu.se/lup/publication/8980793>
- MacNeil, H. (1992). *Without Consent. The Ethics of Disclosing Personal Information in Public Archives* (Society of American Archivists and Scarecrow Press).
- MacNeil, H. (2005). Information Privacy, Liberty, and Democracy. In M. L. Behrnd-Klodt & P. J. Wosh (Eds.), *Privacy and Confidentiality Perspectives: Archivists & Archival Records* (pp. 67–81). Society of American Archivists.
- Mathiesen, K. (2012). A Defense of Native Americans' Rights over Their Traditional Cultural Expressions. *The American Archivist*, 75(2), 456–481. <https://www.jstor.org/stable/43489632>
- McCrow-Young, A. (2021). Approaching Instagram Data: Reflections on Accessing, Archiving and Anonymising Visual Social Media. *Communication Research and Practice*, 7(1), 21–34. <https://doi.org/10.1080/22041451.2020.1847820>
- McKay, A. C. (2002). Genealogists and Records: Preservation, Advocacy, and Politics. *Archival Issues*, 27(1), 23–34.
- The National Library of Israel. (2023). *Franz Kafka*. <https://www.nli.org.il/en/discover/literature-and-poetry/authors/franz-kafka>. Accessed August 4, 2023.
- Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17(5–6), 559–596.
- Novak Gustainis, E. R., & Letocha, P. E. (2015). The Practice of Privacy. In *Innovation, Collaboration and Models: Proceedings of the CLIR Cataloging Hidden Special Collections and Archives Symposium, March 2015* (CLIR pub 169) (pp. 163–176). Council on Library and Information Resource.
- Oestreicher, C. (2020). *Reference and Access for Archives and Manuscripts*. Society of American Archivists.
- Protocols for Native American Archival Materials* (2007, April 9). <https://www2.nau.edu/libnap-p/protocols.html>
- Pugh, M. J. (2005). *Providing Reference Services for Archives*. Society of American Archivists.
- Queer Archives Project (QAP) Team. (2020, February 19). *Third Party Protocol for Queer Archives Oral History Transcripts, Queer Archives Project*. Lafayette College. <https://queerarchivesproject.lafayette.edu/wp-content/uploads/sites/289/2020/02/Third-Party-Protocol-QAP-Oral-History-Tranccripts-February-2020.pdf>

- Robbin, A. (1986). State Archives and Issues of Personal Privacy: Policies and Practices. *The American Archivist*, 49(2), 163–75. JSTOR, <http://www.jstor.org/stable/40292984>
- Schwartz, J. M., & Cook, T. (2002). Archives Records, and Power: The Making of Modern Memory. *Archival Science*, 2, 1–19. <https://doi.org/10.1007/BF02435628>
- Schwartz, J. (1992). The Archivist's Balancing Act: Helping Researchers While Protecting Individual Privacy. *The Journal of American History*, 79(1), 179–189. JSTOR, <https://doi.org/10.2307/2078473>
- Schwind, A., Rowe-Sims, S., & Pilcher, D. (2002). The Conversion of the Mississippi State Sovereignty Commission Records. *The Primary Source*, 24(2), 6–10. <http://aquila.usm.edu/theprimarysource/vol24/iss2/2>
- Society of American Archivists. *Code of Ethics for Archivists*. February 2005; revised August 2020. <https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics>
- Speer, L. K. (1999). Fresh Focus: Mississippi's 'Spy Files': The State Sovereignty Commission Records Controversy, 1977–1999. *Provenance: Journal of the Society of Georgia Archivists*, 17(1), 101–118. <https://digitalcommons.kennesaw.edu/provenance/vol17/iss1/7>
- Tansey, E. (2021, March/April). Part 2: Do Private Interests Override Public Obligations? *Archival Outlook*, 11.
- Tyler, A. R. B. (2022). *Can We Still Archive? Privacy and Social Science Data Archiving After the GDPR*. ProQuest Dissertations Publishing.
- Tzouganatou, A. (2022). Openness and Privacy in Born-Digital Archives: Reflecting the Role of AI Development. *AI & Society*, 37(3), 991–999.
- Velte, A. (2018). Ethical Challenges and Current Practices in Activist Social Media Archives. *The American Archivist*, 81(1), 112–34. <https://doi.org/10.17723/0360-9081-81.1.112>
- Yakel, E. (2002). Listening to Users. *Archival Issues*, 26(2), 111–27. <http://www.jstor.org/stable/41102044>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.





CHAPTER 12

Employee and Customer Information Privacy Concerns in Supply Chain Management

Marc A. Scott, Matthew A. Waller, and Brian S. Fugate

INTRODUCTION

The COVID-19 pandemic illuminated the pivotal role of supply chain management in social, economic, demographic, regulatory, and market dynamics both nationally and globally (Arvis et al., 2023; Ferguson & Lahiri, 2021). From newsrooms to board rooms, the responsibility of supply chain management in facilitating the flow of resources, information, and products to service demand for goods or attenuate critical supply issues is conclusively evident (Henrich et al., 2022; Langley et al., 2021). Indeed, the ability of supply chain managers to design supply

M. A. Scott (✉) · M. A. Waller · B. S. Fugate
Sam M. Walton College of Business, University of Arkansas, Fayetteville, AR,
USA
e-mail: MScott@walton.uark.edu

M. A. Waller
e-mail: MWaller@walton.uark.edu

B. S. Fugate
e-mail: BFugate@walton.uark.edu

chains agile enough to absorb some of the otherwise detrimental effects of the increased volatility that characterize the contemporary marketplace is nothing short of phenomenal, if not incredible (Henrich et al., 2022; Pricewaterhouse Coopers, 2023). Much of the ability to manage the supply chain effectively has been facilitated through the use of advanced technologies that harness data that is analyzed to support decisions-making. While this data collection confers a significant competitive advantage, issues related to information privacy in supply chain management have now arisen. So, why is data collection important in supply chain management? What are the sources of information privacy issues in supply chains? Before delving into these questions, we define supply chain management.

OVERVIEW OF SUPPLY CHAIN MANAGEMENT

Supply chain management refers to the effective and efficient management of the flow of information, resources, currency, and physical products within and between organizational actants. These actants, often a collection of firms, seek to connect the demand for products and services to their sources of supply through a “chain” of activities conducted via interdependent processes. The supply chain has been described as “...the interconnected journey that raw materials, components, and goods take before their assembly and sale to customers” (McKinsey and Company, 2022). The Association for Supply Chain Management (ASCM) (2023) defines the supply chain as “the global network used to deliver products and services from raw materials to end customers through an engineered flow of information, physical distribution and cash.” Concurrently, the Council of Supply Chain Management Professionals (CSCMP) explains supply chain management as an action that:

Encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies” (CSCMP, 2023)

As noted, logistics management is a component of supply chain management. As defined by the CSCMP (2023), logistics management is “that part of supply chain management that plans, implements, and controls the efficient, effective, forward and reverse flow and storage of goods, services and related information between the point of origin and the point of consumption in order to meet customers’ requirements.” Logistics management activity typically includes inbound and outbound transportation management, fleet management, warehousing, materials handling, order fulfillment, logistics network design, inventory management, supply and demand planning, and the management of third-party logistics services providers (CSCMP, 2023). A component of logistics management, order fulfillment, is the process, which ensures that customers that are served by the supply chain receive their orders in a timely and accurate manner; ensuring customer expectations are met (Fawcett & Fawcett, 2013).

Order Fulfillment in Supply Chain Management

Customer orders, or the anticipation of them, initiate supply chain activity. Order fulfillment is therefore of central importance in supply chain operations, and involves generating, packing, delivering, and servicing customer orders (Croxton, 2003). Often the only method by which customers interact with selling firms, the order fulfillment process is a mechanism through which selling firms pursue customer service level targets, thereby directly affecting the buyer experience in various ways (Croxton, 2003; Fawcett & Fawcett, 2013). The way in which the order fulfillment process is managed can determine, among other outcomes, whether orders are picked accurately from a warehouse, whether products are in stock at a store, or whether deliveries are on time to a customer’s home. As such, a deepened understanding of customer needs and preferences when designing the order fulfillment process, can significantly enhance its effectiveness and its ability to be responsive to evolving consumer expectations (Croxton, 2003; Langley et al., 2021). Simultaneously, supply chain managers must ensure that this responsiveness is facilitated in as cost-efficient a manner as possible (Langley et al., 2021). Order fulfillment operations that are managed to be both efficient and effective can facilitate faster or more convenient deliveries to customers, as well as reduced order-to-cash cycle times for selling firms (Croxton, 2003; Langley et al., 2021). Figure 12.1 displays the relative activities that occur

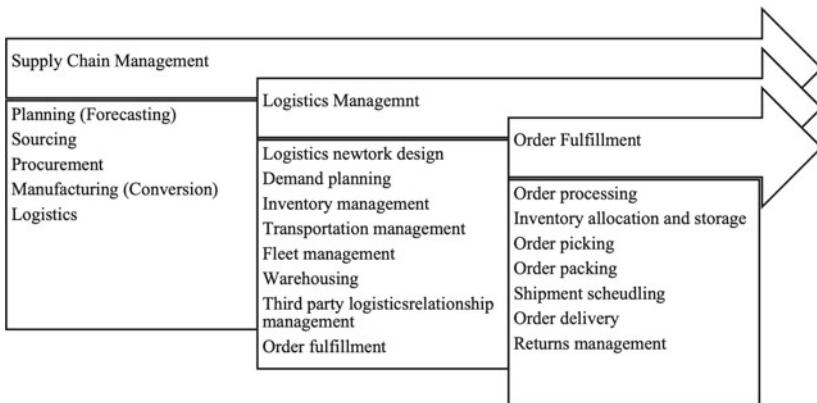


Fig. 12.1 Supply chain, logistics, and order fulfillment activities

within the areas of supply chain management, logistics management, and order fulfillment.

Well-managed order fulfillment operations can be the differentiating factor among firms in highly competitive marketplaces where customers can switch easily between sellers (Henrich et al., 2022; Langley et al., 2021). In retail markets, differences in order fulfillment operations have distinguished market leaders from other competitors (Devari et al., 2017). This distinction exists because the speed, convenience, and service levels associated with the handling of orders after they are placed with retailers are now among the primary factors that customers consider when deciding from whom to purchase (Pricewaterhouse Coopers, 2023; Tsai & Tiwasing, 2021). Further, retail market leaders must now operate order fulfillment processes that support both traditional in-store engagement and increased consumer e-commerce activity, a practice referred to as *omnichannel retailing* (Langley et al., 2021). Omnichannel retailing integrates the sales, operations, and order fulfillment processes of both online and in-store operations (Dohrmann et al., 2022). The advent of omnichannel retailing has served to increase the complexity of the order fulfillment process in retail supply chains because of the need for retailers to coordinate activities within and between channels (Fawcett & Fawcett, 2013; Pricewaterhouse Coopers, 2023). This innovation has increased the complexity associated with retail supply chains, leading to the need

to leverage the capabilities facilitated by using advanced technologies (Dohrmann et al., 2022; LaBombard et al., 2019).

ORDER FULFILLMENT IN RETAIL SUPPLY CHAINS

Urbanization, mobile technology access, product variety, and improved technology-enabled delivery services have played a role in the growth of consumer engagement in e-commerce (Wolff et al., 2020). In omnichannel retailing, customers engage with retailers and their products across a multiplicity of both digital and physical touchpoints that can include retail stores, various types of other pick-up locations, and websites (Langley et al., 2021; Pricewaterhouse Coopers, 2023).

The goal of omnichannel retailing is to provide customers with a unified and synchronized experience, allowing customers the choice of purchasing a product through any channel, thus enabling the reception and return of products through those channels (Dohrmann et al., 2022; Langley et al., 2021). An example would entail a customer purchasing a product on a retailer's website and then being presented with the option to either pick the order up at one of the retailer's store locations, or have it delivered to their home. If that same customer opted to pick the order up in the store but then changed their mind, they could return the item without ever leaving home by using the online channel.

Successful omnichannel retailing necessitates intricate planning of inventory levels across many retailer and logistics service provider facilities and assets, including stores, warehouses, and delivery vehicles. Delivery of goods must not compromise on the speed, convenience, and consistency in service levels among channels—consumers have an expectation of efficiency conducted at a high level of professionalism (Dohrmann et al., 2022; Langley et al., 2021). For example, customers' propensity to buy online and pick-up in-store (BOPIS) has now become a standard shopping behavior (Dohrmann et al., 2022; Pricewaterhouse Coopers, 2023) and requires sophisticated coordination of order processing, inventory sharing, and transportation planning activities (Langley et al., 2021). This sophisticated coordination points to the pivotal role that logistics management, through the order fulfillment process, plays in ensuring omnichannel retailing supply chain effectiveness and efficiency (Devari et al., 2017; Dohrmann et al., 2022). Notably, the coordination of the order processing, storage, and movement of physical products within and

between channels in omnichannel retailing is facilitated by technology-enabled order fulfillment (Alicke et al., 2016; Borgi et al., 2017; Dohrmann et al., 2022). These enabling technologies simultaneously provide value while engendering potential information privacy issues.

Organizational Uses of Technology in Retail Fulfillment

The advent of digitization across the supply chain has led to the availability of large-scale data sets with information on numerous dimensions of supply chain operations. These data sets can comprise information on purchase transactions, contract terms and conditions, traffic volumes, customer and facility addresses and locations, and competitor pricing for instance (Borgi et al., 2017; DHL, 2023). In retail, technology and the data management associated with its use can support order fulfillment activities in any of three ways (Dohrmann et al., 2022; LaBombard et al., 2019). First, technology can facilitate insights by generating new data sets or analyzing existing ones. An example of this system would be the generation of a data set that details the differences in the average on-time delivery performance between two different product categories offered by a retailer online. Second, technology supports fulfillment operations when applied to facilitate the automation of order fulfillment tasks and processes. Automation refers to the use of technology to automate tasks that were previously conducted manually to improve fulfillment process efficiency. An example would be the use of robots to carry out order picking in a warehouse, a task traditionally completed by human employees. Third, technology can be used to engage in the monitoring of order fulfillment activities to improve worker productivity and safety, or any of a variety of other desirable outcomes. An example of this process would be the use of advanced surveillance technologies to record employee truck loading and unloading performance in real time.

Indeed, the visibility facilitated by monitoring, tracking, and surveillance technologies has been of paramount importance in retailers and logistics service providers' ability to address the various complexities brought on by e-commerce growth and the resulting surge in omnichannel retailing activity (LaBombard et al., 2019). The ability of retail supply chain managers to have a comprehensive view of their fulfillment operations in real time and leverage that ability to make operations and resource allocation decisions speedily, with increased confidence, is enabled using advanced technologies (Cantor, 2016; LaBombard et al.,

2019). These technologies can range from applications that improve frontline worker picking operations, to those that provide decision support in the selection of optimal logistics network designs (Alicke et al., 2016; Langley et al., 2021; Winkenbach, 2018).

Given that two of the more significantly affected stakeholders in the rapid adoption of advanced technologies in retail fulfillment operations are customers and the employees engaged in the order fulfillment process, it is important to understand how technologies are leveraged during the order fulfillment process to gather data from each of these stakeholder groups.

Customer Data Collected During Order Fulfillment

As customers become more connected to retailers through digital technologies, vast amounts of consumer supply chain-related data are generated. This data is then utilized to develop more customer-centric order fulfillment operations, which subsequently facilitate the development of innovative and customized products and services (Mahoney & Dauer, 2021). Benefits can accrue to retailers through leveraging technologies to better understand the retail customer. For example, logistics service providers and the retailers they serve can have access to customer delivery addresses, their purchase history, and their web browsing activity (DHL, 2023; Winkenbach, 2018). This data is used to comprehend both human behavior and operational characteristics, which then serves as input to improve various fulfillment operations activities. These activities include customer expectations regarding delivery service features; customer product preferences as to what, where, and when they order; fluctuations in traffic conditions during delivery; and real-time transportation equipment availability (Pricewaterhouse Coopers, 2023; Winkenbach, 2018).

Retailers collect various forms of customer data which can include sentimental data, attitudinal data, behavioral data, engagement data, personal data, and demographic data. Sentimental data indicate what customers say they will do, like a customer signaling in a comment online that they will purchase twice as much of a product if it is available in a different color. Attitudinal data show customer emotions and perceptions regarding their experiences, like a feedback survey regarding package delivery or a review page discussing order delivery tracking experiences. Behavioral data reveals what customers do, like the average order value for

a newly launched product or the return rate for that product. Engagement data predicts customer behaviors across various retail channels and helps determine how customers respond to and share experiences regarding engagement with a specific retailer on social media. Personal data suggests customer-specific information that can include name, birthday, website login details, or credit card details. Demographic data describes customers by population-based factors like age, race, and sex.

Specific to retail fulfillment operations, the collection of these various forms of customer-related data can serve to facilitate improvements to both instore and online product layouts based on behavioral mapping technologies or improved target marketing using interactive voice assistant technologies, which analyze customer speech and commands (Dohrmann et al., 2022; Winkenbach, 2018). Some retailers also use internet of things (IOT) technology sensors to determine the location and status of shipped orders or to calculate the remaining number of inventory units for a product across their network of facilities, thereby ascertaining in-stock levels. In both cases, this is information that can be communicated with customers, leading to higher levels of customer service. Further, to improve their last-mile delivery operations, some retailers are leveraging customer transactions, delivery addresses, delivery routes, purchase histories, and other forms of personal information records, to improve service design and efficiency (DHL, 2023; Winkenbach, 2018). Retailers therefore use customer data to sense, motivate, and serve customers during the order fulfillment process by meeting their expectations regarding time, convenience, and place of product order and receipt (Mahoney & Dauer, 2021). The benefits of collecting the aforementioned types of customer data also include the ability of retailers to use it to identify key customer segments, attract and retain high-value customers, improve customer onboarding to increase repeat purchases, increase personalization of the online and in-store shopping experience, prevent customer churn through augmented customer engagement, and enhance responsiveness to customer expectations based on collected data (Eikelmann et al., 2023; Mahoney & Dauer, 2021).

Employee Data Collected During Order Fulfillment

Both retailers and logistics service providers are using advanced technologies to harness and assess data on various dimensions of employee's state of being and performance. Employees in fulfillment operations include

those individuals who are engaged in warehousing, transportation, and store operations activities or those who assume corporate management and analyst roles in retail distribution. Data collected on these employees is levied by employers to improve employees' state of well-being, their job performance, or fulfillment process efficiency. For instance, interactive artificial intelligence can be leveraged to automate order processing workflow components, allowing workers to pursue more complex tasks when situations require (Dohrmann et al., 2022). Performance data can also be used to reallocate or reassign tasks in real time (Dohrmann et al., 2022). Tracking technologies are also used to capture delivery vehicle driver behavior as well as data on vehicle speed, position, braking intensity, and environmental conditions (Acharya & Mekker, 2021; Winkenbach, 2018). Elements of these data can be used to send warnings to drivers in real-time, to avoid pending hazardous or unsafe incidents (Acharya & Mekker, 2021).

While from an organizational perspective, prior research has found that organizations "that are open perform better" (Tapscott & Ticoll, 2003)—*open* referring to the ability to observe various aspects of both customer and employee behavior. There are, however, developing issues regarding the collection of employee data. Indeed, there is a correlation between observability and performance, the premise being that both managers and employees need to see working activity to determine what needs to improve (Bernstein, 2012; Tapscott & Ticoll, 2003). Notably, the ability to observe, or transparency, has been shown to facilitate the presence of two key tenets of organizational productivity: *organizational learning* and *operational control* (Bernstein, 2012; Deming, 1986). Technology is a leading factor in facilitating observability through the acquisition of process and employee data. As such, technology is also a major mechanism through which privacy-related issues in the supply chain are actualized.

PRIVACY CONCERNs

In retail supply chains, the collection of the aforementioned various forms of process, employee, and customer during the order fulfillment process, using data and the widespread implementation of advanced technologies is a driver of privacy now being a central issue in supply chain management (Dohrmann et al., 2022; Eikelmann et al., 2023; Sheng, 2019). The harnessing of data at the individual level in real-time requires that retail supply chain managers be highly cognizant of the fact that both

employees and customers perceive such practices to be invasive, which can impact their workplace or shopping experience (Cantor, 2016). The collection and analysis of granular-level employee and customer-generated data that supply chain digitization and advanced technology deployment have facilitated has given rise to concerns regarding data protection, security, and privacy in omnichannel retail fulfillment operations (Cantor, 2016; Dohrmann et al., 2022; Winkenbach, 2018). Due to the multiplicity of functional areas, such as tasks, channels, customer decisions, purchase actions as well as other contextual factors, fulfillment operations must take heed of them all. The rationale is simple. There is no overarching conceptualization of privacy because the definition of the term is contingent on both individual and contextual factors (Cottrill & Thakuriah, 2015). Yet, the common theme regarding privacy that drives much deliberation revolves around concerns as to who owns the control and flow of information (Cottrill & Thakuriah, 2015).

In retail fulfillment operations, the perception of the loss of privacy can manifest itself in various forms, depending on the dimension of privacy being considered. For instance, warehouse employees may determine that employers collecting data on their order pick rates is reasonable, but then find that the harnessing of data regarding their health conditions is invasive. Likewise, retail customers may find the collection of their browsing behavior while shopping online to be admissible but deem the analysis of their shopping related driving patterns to be intrusive. While both retailers and logistics service providers make the case that the harnessing and analysis of customer and employee data can confer benefits to both individuals and the fulfillment process, trade-offs exist concerning the privacy loss-related cost individuals or firms may bear associated with the collection of that data. Table 12.1 displays several of the advanced technologies being used in retail fulfillment operations, describes them, and then provides examples of some of the potential privacy implications associated with their use.

These examples are just several among a plethora of potential privacy scenarios that can exist across the vast array of activities and processes that characterize retail order fulfillment operations (Dohrmann et al., 2022; Eikelmann et al., 2023; Fawcett & Fawcett, 2013; Sheng, 2019). Yet, among various dimensions of privacy, *work environment privacy* and *information privacy* are highly salient in retail order fulfillment operations

Table 12.1 Privacy implications of technology use in retail fulfillment

<i>Technology</i>	<i>Description</i>	<i>Privacy implication in retail fulfillment</i>
Artificial Intelligence	Computer programs can learn through completing or observing human-like tasks. Learning facilities digital computers or computer-controlled robots being able to perform tasks commonly associated with intelligent beings	Retail customer information about preference of personal hygiene, contraception, or medical product preferences, along with shipment addresses of choice being collected during their engagement with AI-enabled ordering or virtual assistant systems Machine learning algorithms duplicate undesirable human biases regarding hiring seasonal warehouse workers or drivers, expected pick rate performance, or overtime pay opportunities during the holiday season
Autonomous Vehicles	Vehicles capable of driving themselves due to automated technology utilizing each combination of advanced computer programs and sensors	Retail customer are concerned with connected vehicle technology being able to share their shopping trip or travel behavior data with third parties, more so without authorization
Bionic Enhancements	Enhancement of human physical and cognitive capabilities through machine-human interactive technologies. These technologies facilitate exceeding the current human physical or cognitive limits associated with a task	Fulfillment employees are being concerned about the leakage of biometric data used to encrypt access to individual-specific exoskeletal suits or the collection of data used to determine whether there is a need to recommend the use of one to an employee in a warehouse environment or not

(continued)

Table 12.1 (continued)

<i>Technology</i>	<i>Description</i>	<i>Privacy implication in retail fulfillment</i>
Blockchain	A digital ledger comprised of immutable records, referred to as blocks, with each record representing a transaction. A decentralized cluster of computers manages these records so that no one entity solely owns information rights to the data	The unintended or intended leakage of retail customer financial, location, behavioral, or other personal information to a third party The risk of a supplier's costing information being observable by a retailer who in turn uses this information to apply pressure during pricing negotiations
Drones	Also referred to as unmanned aerial vehicles (UAVs), these vehicles carry no human pilot no passengers, and often human pilots control them remotely	Customer concern over the monitoring capability of drones during package deliveries to their homes, or fulfillment employee anxieties over drone surveillance of behaviors at the wrong times (e.g., during break time at fulfillment facilities)
Internet of Things	Computing devices embedded in physical objects are interconnected via the Internet. Each of these devices has the capability to transfer data within a network of connected devices, with no need for human intervention	Retail customers' apprehension over the collection, directly or through a breach, and sharing of personal information generated at self-checkout points in stores or the collection of behavioral and product consumption patterns through connected devices in their homes
Robotics and Automation	Robotics refers to machines controlled by an internal or external computer capable of executing complex series of movements and tasks automatically. Automation describes the use of software to complete computer-based tasks commonly performed by humans	The concern of both fulfillment employees and retail customers regarding robots using camera recording and data collection capabilities to harness sensitive or personal information during delivery or fulfillment task completion activity

(Bhave et al., 2020). In the following sections, we will focus our discussion on the implications of these dimensions of privacy, as applicable to either employees or customers in retail order fulfillment operations.

EMPLOYEE PRIVACY IN RETAIL SUPPLY CHAIN ORDER FULFILLMENT

Collecting information on employees can significantly benefit employers. These benefits can accrue in recruiting and hiring efforts, in supporting effective and efficient operations performance, and in minimizing exposure to risk and legal issues. Employers such as retailers and third-party logistics service providers presuppose it to be advantageous to maintain extensive sets of information on their employees (Bhave et al., 2020). Indeed, corporations do have the right to amass information about their workforce, such as data pertaining to employee capability, performance, and ethics. They may do so to implement programs that reduce counterproductive or undesirable work behaviors (Bhave et al., 2020). Managerial visibility, or transparency, to such information, has proven to be accretive to retail order fulfillment performance, as employees of varied levels of experience and capabilities engage in increasingly complex fulfillment process tasks at stores, distribution centers, and transportation depots. These tasks are essential to realizing customer service level targets and operating efficiency goals.

Transparency, or the ability to accurately observe fulfillment operations activities, procedural approaches, work behaviors, and task performance at a granular level, can result in improved organizational learning and operational control for retailers and logistics service providers alike (Bernstein, 2012; Deming, 1986; Miller, 2018). Extant literature indicates that transparency has been found to improve a work unit's access to expertise, experience, and stored knowledge, thereby increasing the propensity for knowledge transfer and shared understanding. Transparency is also an antecedent to accelerated organizational learning curves as well as to increased strength in the ties that govern knowledge exchange between networks of actors (Bernstein, 2012; Miller, 2018).

The ability to observe can also enable operational control through the availability of more detailed, comprehensive, accurate, and real-time data on employees and processes across the retail supply chain, thus, improving both hierarchical and peer control of fulfillment operations (Bernstein,

2012; Dohrmann et al., 2022). The value proposition of increased transparency across retail supply chains has resulted in supply chain managers engaging in process and facility redesign aimed at facilitating increased observability, most often supported through using advanced surveillance and data capturing technologies in stores, distribution centers, and transportation depots (Bernstein, 2012; Dohrmann et al., 2022; Sheng, 2019). Surveillance and data collection significantly contribute to the ensuing privacy issues that employees bring attention to and, at times, engage in litigation to address. Indeed, in retail order fulfillment operations, the importance of ensuring that employee and customer data are safe is paramount now, making privacy one of the central points of interest in omnichannel retail and order fulfillment operations (Dohrmann et al., 2022; Pricewaterhouse Coopers, 2023).

Employers such as retailers and third-party logistics service providers presuppose it to be advantageous to collect extensive sets of information on their employees (Miller, 2018). Indeed, corporations do have the right to collect information about their workforce, such as data pertaining to employee capability, performance, and ethics. They may do so to implement programs that reduce counterproductive or undesirable work behaviors (Bhave et al., 2020). In retail order fulfillment operations, the benefits discussed above can be realized through (1) a retailer or logistics service provider conducting psychometric analysis on job applicants to determine their cognitive fit with the responsibilities associated with a high-intensity role within a fulfillment center; (2) a retailer or logistics service provider collecting data on the individual performance rates of employees that load and unload containers at a transloading facility, being intent on using that data to identify constraints to improving its cross-docking operations speed; and (3) a retailer or logistics service provider using an inward-facing camera to record a truck driver during a traffic accident and thereafter use the footage as evidence to avoid punitive actions in litigation proceedings (see Fig. 12.2).

Employees themselves can also profit from the collection of their personal data. Among these benefits include the ability for job performance-related data to be used in the allocation of economic incentives, career advancement opportunities, and other related rewards (Miller, 2018). Personal data can also be used to improve health and safety conditions, like the monitoring of biologically vital information to preempt medical hazards or the suggesting of task-related movement best practices to improve the personal safety of workers (Guillot, 2019).



Fig. 12.2 Inward-facing camera monitors an employee (*Image credit* Alamy Stock Photo/Olaf Doering)

Further, recorded data can be used as material to support employee claims or cases during litigation proceedings (Wendt, 2023). While each of these examples points to the use of data for purposes that appear to be accretive to both the employer and its employees, the appearance of the sensor, surveillance, voice recognition, and other technologies to track, listen to, and record workers in real time while on the job has led to employees and other stakeholders to voice concern over the privacy implications of corporate surveillance programs (Sheng, 2019).

Indeed, industry research has found that most employees in distribution facilities have both reservations and concerns about these tracking and monitoring technologies despite understanding the benefits they confer (Dohrmann et al., 2022; Miller, 2018). While the use of these tracking and monitoring technologies has indeed led to efficiency gains in order fulfillment operations, an unintended consequence of their implementation is a growing concern regarding both corporate and individual privacy in the workplace (Bhave et al., 2020; LaBombard et al., 2019). Given the fact that these large-scale datasets are susceptible to data

breaches, they can be distributed to third parties, especially in instances where employers fail to adequately document or notify employees that data collection activity is occurring (Bhave et al., 2020; Iyer, 2023). This dynamic has resulted in growing tensions regarding workplace privacy because employers require information on employees who are increasingly cognizant of their individual rights (Bhave et al., 2020; Iyer, 2023).

Work environment privacy refers to perceptions of control over sensory stimuli in the work environment (Bhave et al., 2020). These stimuli can be visual, spatial, acoustic, or olfactory in nature. Work environment privacy addresses dimensions pertaining to control over employees' interpersonal interactions in a workspace or access to employees' presence. More definitively, and as detailed by Bhave et al. (2020), *visual privacy* refers to an employee being independent of optical stimuli and undesired notice by others. *Acoustic privacy*, which deals with auditory and sound-related dimensions of privacy, indicates the degree to which employees are isolated from noise, and whether they perceive that their verbal conversations or other forms of speech in the workplace are private. *Spatial privacy*, or privacy regarding personal space, notes the extent to which an employee perceives others entering the physical area surrounding them as being invasive. Though deliberated less regularly, *olfactory privacy* touches on the absence of undesired smells in the workplace. Much of the work in extant literature that addresses work environment privacy does so from the perspective of workspace layout and design, often integrating elements of visual, acoustic, and spatial privacy as well. The aforementioned dimensions of *work environment privacy* are applicable to the retail fulfillment context, and Table 12.2 provides some examples of the work environment privacy implications for employees that are associated with each of these dimensions.

Information privacy pertains to control over the acquisition, storage, use, and sharing of employee data, and addresses if and how this information is made available to others (Bhave et al., 2020). An issue of significance to employees in this arena centers on whether they are informed as to the purpose of data collection and its intended use. The nature of data being collected by firms varies and can include social media information mined for use during the recruitment and employee selection process. Most firms are weary of this dynamic because it can adversely impact firm reputation and subsequent recruiting efforts. Dependent on corporate policy, firms can also stockpile employee e-mail-related information or share performance and appraisal information beyond the focal

Table 12.2 Work environment privacy dimensions in retail fulfillment (Adapted from Bhave et al., 2020)

<i>Work environment privacy</i>		
<i>Privacy dimension</i>	<i>Description</i>	<i>Application in retail fulfillment</i>
Visual Privacy	Employee independence from optical stimuli and undesired notice from others	Warehouse or transportation workers not being exposed to lighting, facility signage, or the public display of pick rate or loading performance information; any actions deemed as either invasive or having a negative impact on the ability to perform well
Acoustic Privacy	Employee isolation from noise, and their belief that conversations and speech in the workplace are private	Warehouse workers are concerned over the impact that conveyor belt or assembly and kitting equipment noise has on their ability to perform. Truck driver discomfort with vehicle inward facing cameras being able to record personal conversations
Spatial Privacy	Employee perception that others entering the physical area surrounding them is invasive	Warehouse workers are uncomfortable with the proximity of supervisors to the workspace or truck drivers worry about the close proximity between camera and driver inside their vehicles
Olfactory Privacy	The absence of undesired smells in the workplace	Warehouse worker's concern over the scent of spoiled or obsolescent produce at the facility or truck driver anxiety over the scent of vehicle-based chemicals or emissions

employee and their immediate supervisor (Bhave et al., 2020). Further, the growing use of electronic performance monitoring and tracking systems by employers facilitates the collection of data that can include information on individual task performance or employee location in real time (Bernstein, 2012; Bhave et al., 2020). Differing perspectives between employees and employers exist regarding information privacy (Iyer, 2023). Employees are desirous of having control over their personal information and the level of access an employer has to that information. Conversely, employers expect to be able to have comprehensive information on their employees, in addition to a growing desire to have knowledge of their employees' whereabouts at any given point in time (Bhave et al., 2020; Iyer, 2023).

Corporations leverage tracking and monitoring technologies to pursue safety, customer service, efficiency gains, and risk-management objectives. In contrast, their employees perceive the existence of significant privacy-related tradeoffs regarding the use of these technologies. From a safety perspective, working conditions are of paramount importance in order fulfillment operations activities. For example, during the COVID-19 pandemic, companies deployed computer vision technologies to ensure that employees in distribution centers and processing facilities adhered to the use of personal protective equipment stipulations (Dohrmann et al., 2022), an action that some employees found to be invasive and infringe on their personal rights. In another instance, various retailers, desirous of addressing working condition issues, directly or confidentially engage with the employees of their suppliers to collect information on the working conditions at those suppliers' facilities. Moreover, those employees use mobile technologies to record the conditions in which they work (Sanders et al., 2019). This focus on human rights is of course commendable, but some employees at those facilities, and the companies for which they work, determine these actions to infringe on their privacy rights.

Additionally, numerous retailers and logistics service providers utilize surveillance cameras and artificial intelligence technologies to record and detect if employees in their facilities are adhering to ergonomic best practices to minimize the risks associated with personal injuries, in-facility vehicle speed violations, and non-compliance to stipulated walking paths within distribution and production facilities (Dohrmann et al., 2022). Indeed, musculoskeletal disorders (MSDs) occur due to ergonomic-related hazards in fulfillment operations facilities. In response, companies are equipping workers with wearable devices to record and observe employee performance patterns to minimize MSD occurrence risk through either workplace redesign or employee training programs that are based on the observed recorded behavior of employees (Dohrmann et al., 2022).

Of note, wearable technology devices, along with other sensor technologies, are also being used to collect and track employee biometric information. Companies are outfitting retail store, warehouse, and transportation employees with sensor technologies that can detect vital body data, including fatigue and stress levels, heart rates, alcohol levels, and other measures of physical fitness that display how employees are physically responding to the tasks that their respective roles demand. For example, a large retailer recently received a patent for an ultrasonic

bracelet that would be able to detect warehouse workers' locations within a facility and then monitor their interaction with task equipment using ultrasonic sound pulses (Sheng, 2019).

Additionally, employers are utilizing facial recognition and text analysis tools to identify employee emotions and sentiments when completing their tasks (Iyer, 2023). For example, a large retailer recently patented a system that facilitates listening in on both workers and customers to determine their sentiments and preferences (Sheng, 2019). The above scenarios represent only a handful of cases in which advanced technologies track and monitor employee behavior in various aspects of retail order fulfillment operations (Dohrmann et al., 2022).

While employers note that the use of these technologies can warn employees about, and even preempt, pending hazards and medical conditions, unsurprisingly employees across the various facets of order fulfillment operations have expressed an aversion to the use of some of these surveillance and tracking technologies (Wendt, 2023). These employees argue that these technologies can infringe on their privacy rights and often put them at risk of being the recipients of unfair, and sometimes unwarranted, punitive actions. Of note, employees and other stakeholders are anxious about how employers will collect and use biometric data (Guillot, 2019; Sheng, 2019) or use data that presents employee performance at a more detailed level. Further, there is substantial concern over the autonomous decision-making authority that these technologies will have in order fulfillment operations as they become more advanced and pervasively used (Dohrmann et al., 2022; Iyer, 2023). As these technologies proliferate, it is of utmost importance to understand how employee responses to their employers' increased surveillance and monitoring activity will impact supply chain and order fulfillment operations.

Extant research on the response of employees to electronic performance monitoring in the workplace has determined that though the characteristics of the technologies themselves are important in influencing the reaction of individuals, context, personality, and other individual characteristics also influence the response to surveillance activity (Ravid et al., 2020). These individual characteristics can include locus of control, perception of control, trust in management, task difficulty, task complexity, individual skill, and aptitude (Ravid et al., 2020). Additionally, Ravid et al. (2020) found that personality, values, goal orientation, occupational and work characteristics, and organizational culture and

climate each moderated the effect of electronic performance monitoring on employee responses. Differences in *personality* moderated the effects of monitoring and surveillance systems on individual reactions, such that individuals with lower levels of extraversion and emotional stability were less likely to have positive attitudes toward monitoring and surveillance activity. Individuals with higher levels of neuroticism were also less likely to perceive surveillance and monitoring activity in the workplace as being procedurally fair or legitimate.

Next, *values* also mitigated the effects of electronic performance monitoring on employee reactions. In studying whether individuals' ethical orientations influenced their sensitivity toward potential privacy breaches within surveillance and monitoring systems, researchers found that ethical orientation influenced the perception of the invasiveness and appropriateness of such systems. One of these studies demonstrated that individuals with high levels of formalism had the strongest negative relationship between perceived privacy invasion and appropriateness of surveillance and monitoring systems (Alder, 2007). Of interest, individuals with high levels of utilitarianism were found to exhibit the strongest positive relationship between the perceived usefulness of surveillance and monitoring systems and organizational trust (Ravid et al., 2020).

Goal orientation was yet another moderator of the effect of electronic performance monitoring systems on employee response. Employee responses varied depending on the type of goal they found motivating (Ravid et al., 2020). For example, mastery goals, where the focus is on learning and personal improvement, differ significantly from performance goals, where the objective is to prove one's ability and actively avoid the judgment of others. Interestingly, research focused on performance goal orientation found that employees with higher levels of avoid-performance goal orientation had more anxiety about evaluation apprehension and lower skill attainment when they believed their performance data would be reviewed at a future time. Alternatively, the study found that employees with higher levels of prove-performance orientation had increased levels of evaluation apprehension and lower skill attainment when they understood that their performance data would be reviewed in real time (Watson et al., 2013).

Occupational and work characteristics were other moderators of the effect of monitoring systems on employee response. Indeed, recent studies have shown that occupational types moderate the relationship between surveillance and monitoring systems and an employee's trust in

their management. Of note, those employees who engaged in jobs that were more manual in nature associated less trust in management with more surveillance and monitoring, while no such relationship existed for those employees in non-manual jobs. Another study found that individuals who reported having more empowering jobs were more likely to respond negatively to monitoring than those employees who perceived their jobs to have less autonomy.

The strength of the effect of electronic performance monitoring systems on employee response was also found to vary based on *organizational culture and climate*. Researchers found that the shared values and beliefs on which organizational culture is based can lead to the establishment of behavioral norms and expectations. Therefore, any corporate intervention that appears to not align with those shared values conjures negative reciprocity from employees. For instance, in highly bureaucratic cultures that are defined by clearly defined lines of authority and systems-based work, surveillance and monitoring systems were more welcomed. Further, it was also determined that the caring climate of a company moderated the relationship between the effect of electronic performance monitoring systems and employee response. For employees who perceived that they worked in a strong caring climate, the relationship between their attitude toward surveillance and monitoring systems and their intention to resist such systems was less negative than that observed for those employees who reported working in uncaring work climates (Ravid et al., 2020).

CUSTOMER PRIVACY IN RETAIL SUPPLY CHAIN ORDER FULFILLMENT

Retail customers can help improve order fulfillment process design by disclosing elements of their personal information and by agreeing that other forms of information about them can be collected. In retail fulfillment operations, retailers can utilize various forms of customer data to better manage inventory through enhanced demand forecasting and determining optimal inventory levels to hold based on extracted customer preferences. Additionally, customer demographic and behavioral data, like location and willingness to pay, can help develop optimal pricing strategies for value-add services like product put-away or assembly inside customer homes during delivery. Further, customer demographic and

behavioral data can assist in designing more efficient delivery operations by segmenting customers by delivery speed, drop-off time window, and delivery vehicle type preferences, generating immense value for customers (Eikelmann et al., 2023; Mahoney & Dauer, 2021). Therefore, understanding retail customers' propensity to disclose information is of paramount importance to retail order fulfillment operations. However, the scale to which technologies collect and share customer data can result in significant levels of customer concern (Dohrmann et al., 2022; Eikelmann et al., 2023).

Prior research has discovered that retail customers generally express concern around four factors related to privacy: *unauthorized access*, *secondary use*, *errors*, and *collection* (Aloysius et al., 2018). Researchers describe each of these factors. *Unauthorized access* refers to the extent to which customers are concerned about their personal information being available to unauthorized persons. *Secondary use* highlights the extent to which customers are concerned about the unjustified use of their information for purposes other than that for which it was initially intended. *Errors* are defined as the degree to which customers are concerned about both intentional and non-intentional errors that occur in the handling of their positional information. *Collection* describes the measure to which customers are worried about the amount of their personal information being collected by retailers (Aloysius et al., 2018). Indeed, the advent of advanced technologies able to capture significant volumes of consumer data bears significant information privacy implications for retail customers.

Retail customers' perceptions of technology have a substantial effect on those technologies' outcomes and use (Aloysius et al., 2018). Specific to retail stores, studies have found that customers do not always prefer the personalized services that advanced technologies facilitate due to their *privacy concerns* (Aloysius et al., 2018; Chellappa & Shivendu, 2010). Of note, retail customers' privacy concerns adversely impact the wide-scale adoption of advanced retail and fulfillment technology (Aloysius et al., 2018; Venkatesh et al., 2017). Some of this concern is amplified when retail customers consider the data-harnessing capabilities inherent in the mobile devices on which they consistently conduct transactions (Cottrill & Thakuriah, 2015). Specific to online engagement, retail customers have expressed anxiety regarding data security in online shopping contexts, which has had an adverse effect on their willingness to disclose personal information (Aielloa et al., 2020). A study by Ingram (2017) revealed that 85% of consumers were unwilling to share their

personal information if they had a concern about the use of that information by retailers and, further, 71% of these customers indicated that they would stop purchasing from a retailer if their information is gathered without their consent. This consumer sentiment is in no small way exacerbated by the continual and frequent news of data breaches and the mishandling of consumer data by large companies as of recent (Aiello et al., 2020). While Chapter 6 discussed privacy concerns, the willingness to disclose personal information, the privacy paradox, and privacy calculus on users in general, this section applies these concepts to consumers in the omnichannel retail order fulfillment process.

Retail customers' *willingness to disclose* information is a central concept in the study of customer privacy implications in the e-commerce and omnichannel retail contexts (Cottrill & Thakuriah, 2015; Eikelmann et al., 2023). Given this, various researchers have studied customers' propensity to disclose information across a variety of retail contexts, understanding the significant effect it can have on order fulfillment process design and operations. These studies have found that customers' *willingness to disclose* information can vary due to individual differences, consumer–company relationships, and retail setting contextual differences (Belk, 2013; Markos et al., 2017; Mothersbaugh et al., 2012; Li et al., 2015; Markos et al., 2018; Phelps et al., 2000). As retail customers determine which, and how much, information they are willing to share when engaging in the online purchasing journey, they make decision tradeoffs regarding the benefits and costs of doing so.

Privacy calculus theory conceptualizes the drivers and influences on how individuals compare the perceived risks and anticipated benefits associated with them divulging private data, or the collection and distribution of sensitive information. As a theory, privacy calculus has been utilized as a lens to interpret customers' adoption or use of technologies in e-commerce social networking, and location-based mobile applications contexts (Leon et al., 2023). The theory posits that the trade-offs customers make in their privacy calculus can be contingent upon their cognitive resources, their attitude, cultural values, social norms, and various other situational and contextual factors (Leon et al., 2023). Privacy calculus theory is highly salient in omnichannel retail and order fulfillment operations. Retail customers do not only make decision tradeoffs when deciding the type and amount of personal information to disclose when engaged in the online purchasing journey; they also do so when deciding on order delivery modes and delivery service options.

The decision outcomes based on retail customers' privacy calculus can impact order delivery operations in two substantive ways. First, the information that customers are willing to share while engaging in the online purchasing journey can determine the service levels offered by delivery service operations. For example, aggregated purchase frequencies, preferred delivery locations, channel preferences, delivery speed preferences, and various other forms of personal data captured online can be used to design distribution networks that deliver on customer expectations regarding, delivery time window, number of days to delivery, the frequency of delivery service, and the level of return services to offer. Second, given each of the aforementioned delivery service features is often enabled by various forms of customer-facing advanced distribution and mobility technologies, customers' propensity to assess either high or low levels of information-related or spatial-related privacy concern is also a central dynamic in retail delivery operations.

Advanced technologies in delivery operations can take the form of autonomous delivery vehicles, autonomous ground vehicles with lockers, parcel lockers, droids, and drones, each mode resulting in varied levels of *perceived privacy*-related issues, which in turn have implications for delivery service planning and operations.

Smart lockers. Research on the use of smart lockers in retail fulfillment operations by Tsai and Tiwasing (2021) found that *privacy security* was an integral factor and service attribute in alleviating customer privacy concerns regarding control over their financial and personal information when using parcel lockers to access their delivered orders. Interestingly, prior studies also indicated that a benefit consumers associate with the use of smart lockers is the removal of human interaction during delivery transactions which facilitates the prevention of potentially sensitive information being collected and distributed by retail or delivery service provider personnel (Featherman & Pavlou, 2003; Tsai & Tiwasing, 2021; Wang et al., 2020).

Vehicle delivery. Extant research has found that customers can have varied levels of *perceived data privacy* the degree to which an individual is concerned about the collection and use of their data—when it comes to the use of connected, autonomous, or recording capability-equipped vehicles that are used in order delivery (Acharya & Mekker, 2021; Bridget, 2017). Further, customers have expressed levels of concern regarding the collection and use of shopping trip data generated by their personal vehicles or mobile devices, and that data being shared with retailers or other

third parties (Acharya & Mekker, 2022a, b; Schmidt et al., 2016). This issue has recently come to the fore more vividly due to the growing practice of crowd-sourced delivery or “social transportation-driven” delivery services, where customers become temporary delivery service providers by picking up and dropping off the orders of other customers within the same social media network (Devari et al., 2017).

Drones. Of note, the use of drones (see Fig. 12.3) has garnered relatively more focus on privacy issues in fulfillment and last-mile delivery operations (Dohrmann et al., 2022; Scharf, 2019).

In the context of drone delivery, retail customers have expressed privacy-related concerns regarding the risks associated with drones being able to collect and record highly sensitive information regarding the personal lives of customers, often without the customers’ knowledge or consent (Iyer, 2023; Leon et al., 2023). Drone anxiety can be compounded by the fact that this technology is relatively new compared to other forms of order delivery technologies, and this adds an additional dimension to customer perceptions of potential privacy-related issues (Dohrmann et al., 2022; Leon et al., 2023). *Privacy concern*, which refers to the context-specific fears regarding the misuse, voluminous collection, unsecure storage, and unauthorized distribution of personal information, is highly salient in retail drone delivery operations (Dinev & Hart, 2006;



Fig. 12.3 Drone surveillance (*Image credit* Alamy Stock Photo/Wavebreak Media)

Lankton et al., 2017). Yet, extant research has unveiled that the *perceived usefulness* of drone technology impacts what consumers comprehend to be the potential privacy harm associated with interactions with drones (Roca et al., 2009). *Perceived usefulness* refers to the degree to which a customer believes that using a particular system will enhance their performance in some way (Davis et al., 1989). In the context of drone technology, studies have revealed that customers can be more willing to overlook the perceived privacy risk associated with drone deliveries once they understand the benefits of those deliveries to be higher (Roca et al., 2009). *Perceived privacy risk* illustrates a combination of the perceived likelihood and impact of privacy harm (Choi et al., 2018; Li et al., 2016). Researchers have noticed that higher levels of *perceived privacy risk* negatively affect the drone delivery adoption intentions of retail customers (Leon et al., 2023; Yoo et al., 2018). Another highly salient concept in the context of order fulfillment by drone delivery is that of customer's *trust*, defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (McKnight et al., 2002; Roca et al., 2009). In last-mile delivery operations *trust* becomes highly important in the perceived mitigation of privacy and safety risks as retailers and logistics service providers make deliveries to customers' places of residence (Leon et al., 2023). Specific to drone delivery, prior studies have reported that higher levels of *trust* positively impacted customer intent to adopt drone delivery services (Leon et al., 2023; Zhang et al., 2019).

SUMMARY

This chapter commenced by defining supply chain management, of which logistics management is a constituent, and then described order fulfillment activities within logistics activities. The focus was on the *order fulfillment* component of supply chain management, especially due to its central importance and high salience in omnichannel retailing. Noting that the effective and efficient management of retail customer orders through fulfillment operations is of central importance due to the rapid growth of e-commerce activity and the resulting emergence of omnichannel retailing, the analysis described how the increased complexity introduced by omnichannel retail supply chains is managed using advanced technology-enabled order fulfillment operations. The

chapter detailed how the use of these advanced logistics technologies allows both retailers and logistics service providers to harness and analyze large-scale data sets that provide information on various human and process dimensions of retail fulfillment operations. Subsequently, this study surveyed the role that observation and *transparency* play in facilitating *organizational productivity* through facilitating increased *organizational learning* and *operational control*, describing their applicability in retail fulfillment operations. Importantly, the use of these technologies to gain transparency and operational efficiency gives rise to both employee-based and customer-based privacy issues in retail order fulfillment operations.

The chapter also discussed the applicability of *work environment privacy* and *information privacy* for both employees and customers engaged in retail order fulfillment operations and processes. As noted, several dimensions of *work environment privacy* exist, and they include *visual*, *spatial*, *acoustic*, and *olfactory* forms of privacy, each having ramifications in retail fulfillment operations contexts. The discussion also defined and debated *information privacy* and indicated its applicability to both employees and customers in retail fulfillment operations. For retail fulfillment operations employees, their propensity to accept tracking, surveillance, or monitoring technologies in the workplace can be contingent on their individual characteristics. These characteristics can be identified as *personality*, *values*, *goal orientation*, *occupational and work characteristics*, and *organizational culture and climate*.

In discussing *information privacy* as it relates to retail customers, the chapter singled out the four factors related to privacy that customers generally expressed concern over. These factors are *unauthorized access*, *secondary use*, *errors*, and *collection*. Additionally, privacy concerns impact customers' *willingness to disclose* information to retailers. Various factors affecting customer *willingness to disclose* information include individual *differences*, *consumer-company relationship*, and retail setting *contextual differences*. Additionally, *privacy calculus theory* is applicable to retail customer information privacy perceptions regarding order delivery activity within retail fulfillment operations. There are two key impacts in this area, the first being that customer willingness to share information with retailers while engaging in the purchasing journey online can directly affect the knowledge retailers have and can use to customize and design delivery services that align with customer preferences. Second, the novelty of several advanced technologies used to deliver packages can be the source

of customer privacy concerns. Among these technologies are smart parcel lockers and drones. This chapter concluded with thoughts about how *perceived data privacy*, *privacy concern*, *perceived usefulness* of technologies, *perceived risk*, and *trust* all play a role in the way retail customers apprehend privacy risk as it pertains to them interacting with advanced technologies in retail fulfillment delivery operations.

REFERENCES

- Acharya, S., & Mekker, M. (2021). *Public perception of the collection and use of connected vehicle data* (No. MPC-21-439).
- Acharya, S., & Mekker, M. (2022a). Measuring Data Sharing Intention and Its Association with the Acceptance of Connected Vehicles. *Transportation Research Part F: Psychology and Behaviour*, 89, 423–436.
- Acharya, S., & Mekker, M. (2022b). Public Acceptance of Connected Vehicles: An Extension of the Technology Acceptance Model. *Transportation Research Part F: Psychology and Behaviour*, 88, 54–68.
- Aielloa, G., Donvitoa, R., Acuti, D., Grazzinic, L., Mazzolia, V., Vannuccia, V., & Viglia, G. (2020). Customers' Willingness to Disclose Personal Information throughout the Customer Purchase Journey in Retailing: The Role of Perceived Warmth. *Journal of Retailing*, 96(4), 490–506.
- Alder, G. S. (2007). Examining the Relationship Between Feedback and Performance in a Monitored Environment: A Clarification and Extension of Feedback Intervention Theory. *The Journal of High Technology Management Research*, 157–174.
- Alicke, K., Rachor, J., & Seyfert, A. (2016). *Supply Chain 4.0—The Next-Generation Digital Supply Chain*. McKinsey and Company.
- Aloysius, J., Hoehle, H., Goodarzi, S., & Venkatesh, V. (2018). Big Data Initiatives in Retail Environments: Linking Service Process Perceptions to Shopping Outcomes. *Annals of Operations Research*, 25–51.
- Arvis, J.-F., Ojala, L., Shepherd, B., Ulybina, D., & Wiederer, C. (2023). *Connecting to Compete 2023: Trade Logistics in an Uncertain Global Economy—The Logistics Performance Index and Its Indicators*. The World Bank.
- Association for Supply Chain Management. (2023). *Supply Chain Management*. Accessed July 29, 2023. <https://www.ascm.org/scm/>
- Belk, R. W. (2013). Extended Self in a Digital World. *Journal of Consumer Research*, 477–500.
- Bernstein, E. S. (2012). The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control. *Administrative Science Quarterly (Johnson Cornell University)*, 57(2), 181–216.

- Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management*, 46(1), 127–164.
- Borgi, T., Zoghlami, N., Abed, M., & Saber Naceur, M. (2017). *Big Data for Operational Efficiency of Transport and Logistics: A Review*. 2017 6th IEEE International Conference on Advanced Logistics and Transport (ICALT).
- Bridget, C. (2017). Autonomous Cars, Big Data, and the Post-Privacy World| DMV. ORG. DMV. ORG Articles. <https://www.dmv.org/articles/self-driving-vehicles-privacy-concerns>
- Cantor, D. E. (2016). Maximizing the Potential of Contemporary Workplace Monitoring: Techno-Cultural Developments, Transactional Memory, and Management Planning. *Journal of Business Logistics*, 37(1), 18–25.
- Chellappa, R. K., & Shivendu, S. (2010). Mechanism Design for “Free” But “No Free Disposal” Services: The Economics of Personalization Under Privacy Concerns. *Management Science*, 56(10), 1766–1780.
- Choi, H., Park, J., & Jung, Y. (2018). The Role of Privacy Fatigue in Online Privacy Behavior. *Computers in Human Behavior*, 81, 42–51.
- Cottrill, C. D., & “Vonu” Thakuriah, P. (2015). Location Privacy Preferences: A Survey-Based Analysis of Consumer Awareness, Trade-off and Decision-Making. *Transportation Research Part C*, 56, 132–148.
- Council of Supply Chain Management Professionals. (2023). *CSCMP Supply Chain Management Definitions and Glossary*. Accessed July 29, 2023. https://cscmp.org/CSCMP/Educate/SCM_Definitions_and_Glossary_of_Terms.aspx
- Croxton, K. L. (2003). The Order Fulfillment Process. *The International Journal of Logistics Management*, 14(1).
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 35(8), 982–1003.
- Deming, W. E. (1986). *Out of the Crisis*. Center for Advanced Engineering Study, Massachusetts Institute of Technology.
- Devari, A., Nikolaev, A. G., & He, Q. (2017). Crowdsourcing the Last Mile Delivery of Online Orders by Exploiting the Social Networks of Retail Store Customers. *Transportation Research Part E*, 105, 105–122.
- DHL. (2023). *Data Protection and Its Legal Implications on Logistics*. Accessed August 4, 2023. <https://lot.dhl.com/data-protection-and-its-legal-implications-on-logistics/>
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-commerce Transactions. *Information Systems Research*, 17(1), 61–80.
- Dohrmann, K., Toy, J., Pitcher, E., Selders, J., & Garuf, T. (2022). *The Logistics Trend Radar*. DHL.

- Eikelmann, S., Schlemmer, M., & Langkammer, J. (2023). The ROI of Customer Data in Retail ‘Highway to Hell’ or ‘Stairway to Heaven?’ *Strategy*, April 27.
- Fawcett, S. E., & Fawcett, A. M. (2013). *The Definitive Guide to Order Fulfillment and Customer Service: Principles and Strategies for Planning, Organizing, and Managing Fulfillment and Service Operations*. Pearson Education.
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474.
- Ferguson, R. W., & Lahiri, U. (2021). *How to Fix Global Supply Chains for Good*. Council on Foreign Relations, November 23. <https://www.cfr.org/article/how-fix-global-supply-chains-good>
- Guillot, C. (2019). Wearables in the Warehouse Bring Privacy Concerns to the Forefront. *Supply Chain Dive*, May 21.
- Henrich, J., Li, J. D., Mazuera, C., & Perez, F. (2022). *Future-Proofing the Supply Chain*. McKinsey & Company.
- Ingram, S. (2017). *Protect.me: How Consumers See Cyber Security and Privacy Risks*. December 4. Accessed October 20, 2023. <https://www.pwc.com.au/digitalpulse/report-protect-me-consumerscybersecurity.html#:~:text=The%20vast%20majority%20of%20consumers,doing%20more%20about%20data%20protection>
- Iyer, C. (2023). *Workplace Monitoring and Employee Data Privacy Are on a Collision Course*. April 28. Accessed August 4, 2023. <https://www.reworked.co/employee-experience/workplace-monitoring-and-employee-data-privacy-are-on-a-collision-course/>
- LaBombard, M., McArthur, S., Sankur, A., & Shah, K. (2019). *The Human Side of Digital Supply Chains*. McKinsey & Company.
- Langley, C. J., Novack, R. A., Gibson, B. J., & Coyle, J. J. (2021). *Supply Chain Management: A Logistics Perspective* (11th edn). Cengage.
- Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook Privacy Management Strategies: A Cluster Analysis of User Privacy Behaviors. *Computers in Human Behavior*, 76, 149–163.
- Leon, S., Chen, C., & Ratcliffe, A. (2023). Consumers’ Perceptions of Last Mile Drone Delivery. *International Journal of Logistics Research and Applications*, 26(3), 345–364.
- Li, K., Lin, Z., & Wang, X. (2015). An Empirical Analysis of Users’ Privacy Disclosure Behaviors on Social Network Sites. *Information & Management*, 882–891.
- Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining Individuals’ Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective. *International Journal of Medical Informatics*, 88, 8–17.

- Mahoney, K., & Dauer, R. (2021). Consumer Connectivity: Creating Customer-Centric Supply Chains. *Consumer connectivity Using Consumer Data to Enable Breakthrough Products, Services, and Business Models*. Deloitte.
- Markos, E., Labrecque, L. I., & Milne, G. R. (2018). A New Information Lens: The Self-Concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information. *Journal of Interactive Marketing*, 46–62.
- Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *Journal of Public Policy & Marketing*, 79–96.
- McKinsey & Company. (2022). *What is Supply Chain?* August 17. Accessed October 20, 2023. <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-supply-chain>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for E-commerce: An Integrative Typology. *Information Systems Research*, 13(3), 334–359.
- Miller, J. A. (2018). Why 70% of Facilities May Deploy Wearables in 5 Years. *Supply Chain Dive*. August 7.
- Mothersbaugh, David L., William K. Foxx, Sharon E. Beatty, and Sijun Wang. 2012. "Disclosure antecedents in an online service context: The role of sensitivity of information." *Journal of service research* 76–98.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 27–41.
- Pricewaterhouse Coopers. (2023). *February 2023 Global Consumer Insights Pulse Survey*. PWC.
- Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. *Journal of Management*, 46(1), 100–126.
- Roca, J. C., José García, J., & José de la Vega, J. (2009). The Importance of Perceived Trust, Security and Privacy in Online Trading Systems. *Information Management & Computer Security*, 17(2), 96–113.
- Sanders, N., Boone, T., Ganeshan, R., & Wood, J. (2019). Sustainable Supply Chains in the Age of AI and Digitization: Research Challenges and Opportunities. *Journal of Business Logistics*, 40(3), 229–240.
- Scharf, R. L. (2019). Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy. *Indiana Law Journal*, 94, 1065.
- Schmidt, T., Philipsen, R., Themann, P., & Zieffle, M. (2016, June). Public Perception of V2x-Technology-Evaluation of General Advantages, Disadvantages and Reasons for Data Sharing with Connected Vehicles. In *2016 IEEE Intelligent Vehicles Symposium (IV)* (pp. 1344–1349). IEEE.

- Sheng, E. (2019). *Employee Privacy in the US is at Stake as Corporate Surveillance Technology Monitors Workers' Every Move*. April 15. Accessed August 1, 2023. <https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html#:~:text=A%202018%20survey%20by%20Gartner,over%20this%20invasion%20of%20privacy>
- Tapscott, D., & Ticoll, D. (2003). *The Naked Corporation: How the Age of Transparency Will Revolutionize*. Simon and Shuster.
- Tsai, Y.-T., & Tiwasing, P. (2021). Customers' Intention to Adopt Smart Lockers in Last-Mile Delivery Service: A Multi-Theory Perspective. *Journal of Retailing and Consumer Services*, 61.
- Venkatesh, V., Aloysius, J. A., Hoehle, H., & Burton, S. (2017). Design and Evaluation of AUTO-ID ENABLED SHOPPING Assistance Artifacts in Customers' Mobile Phones. *MIS Quarterly*, 41(1), 83–114.
- Wang, Y., Wang, S., Wang, J., Wei, J., & Wang, C. (2020). An Empirical Study of Consumers' Intention to Use Ride-Sharing Services: Using an Extended Technology Acceptance Model. *Transportation*, 47, 397–415.
- Watson, A. M., Foster Thompson, L., Rudolph, J. V., Whelan, T. J., Behrend, T. S., & Gissel, A. L. (2013). When Big Brother Is Watching: Goal Orientation Shapes Reactions to Electronic Monitoring During Online Training. *Journal of Applied Psychology*, 642–657.
- Wendt, R. (2023). *Research: Truck Drivers Mistrust Driver-Facing Cameras*. April 28. Accessed August 4, 2023. <https://www.truckinginfo.com/10197665/research-truck-drivers-mistrust-driver-facing-cameras#:~:text=Around%206%25%20of%20drivers%20consider,drivers%20with%20proven%20safety%20records>
- Winkenbach, M. (2018). The Analytics Revolution in Last-Mile Delivery. *Supply Chain Management Review*, May/June.
- Wolff, C., Sahay, R., Klin, C., Heid, B., Huber, A., Hannon, E., & Deloison, T. (2020). *The Future of the Last Mile Ecosystem*. World Economic Forum.
- Yoo, W., Yu, E., & Jung, J. (2018). Drone Delivery: Factors Affecting the Public's Attitude and Intention to Adopt. *Telematics and Informatics*, 35(6), 1687–1700.
- Zhang, T., Tao, D., Qu, X., Zhang, X., Lin, R., & Zhang, W. (2019). The Roles of Initial Trust and Perceived Risk in Public's Acceptance of Automated Vehicles. *Transportation Research Part c: Emerging Technologies*, 98, 207–220.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



INDEX

A

- access management, 76, 77
- accounts and passwords, 9, 112, 121–123
- acoustic privacy, 250, 251
- ACRL Code of Ethics for Special Collections Librarians (2020), 213
- anonymity, 27, 37, 40, 77, 83, 121, 149, 171
- architectural design
 - ennobling the prosaic, 12, 183
 - light, 12, 183
 - primary, secondary, and tertiary spaces, 11, 183
- privacy and comfort in design, 184
- sound, 12, 183
- archival practice, 12, 205, 208, 209, 222, 224, 229
- artificial intelligence (AI), 4, 5, 42, 79, 87, 112, 150, 160, 170, 203, 210, 243, 245, 252
- Association for Information and Image Management (AIIM), 89

Association for Supply Chain

Management (ASCM), 236

Association of College & Research Libraries (ACRL), 213, 217, 225

attack vectors

- denial of service (DoS) attack, 8, 74
 - man in the middle (MitM) attack, 8, 74
 - phishing, 92
 - social engineering, 92
 - spoofing attack, 8, 74
- autonomy, 39, 51, 90, 100, 101, 104, 218, 255

B

biobank, 201, 202

Bitcoin, 9, 113, 114, 126, 172

blockchain, 5, 9, 114, 160, 170, 172, 174, 176, 246

bodily privacy, 2, 15

breaches, 8, 12, 73, 87, 91–95, 106, 118, 196, 200, 202, 254, 257

- C**
- California Consumer Privacy Act (CCPA), 172
 - Canada, 72, 207
 - Children's Online Privacy Protection Act (COPPA), 16, 105
 - Colorado Privacy Act (CPA), 105
 - communication privacy, 2, 15
 - confidentiality, 11, 12, 27, 40, 77, 84, 91, 134, 194–199, 201, 203, 210, 213, 221, 222
 - Connecticut Data Privacy Act, 106
 - consent, 3, 4, 37, 40, 41, 76, 77, 82, 102, 199, 201, 202, 211, 224, 225, 257, 259
 - controls, 7, 12, 16, 18, 26, 35, 39, 41, 42, 65, 73, 76, 77, 80–82, 88, 97, 98, 102, 113, 118, 122, 124, 131, 134, 173, 206, 224, 244, 246, 247, 250, 251, 253, 260
 - administrative controls, 80, 81
 - technical controls, 80, 81
 - Council of Supply Chain Management (CSCMP), 236, 237
 - Cures Act of 2016, 200
 - customer privacy, 11, 255, 257, 258
 - cybersecurity, 7, 8, 10, 15, 71, 72, 75, 77, 80–82, 84, 112, 113, 115
 - cybersecurity attacks
 - denial of service (DoS) attack, 8
 - man in the middle (MitM) attack, 7
 - phishing, 92
 - social engineering, 92
 - spoofing attack, 7, 8
- D**
- data ethics, 89, 98, 106
 - data governance, 8, 16, 87–90, 95–97, 99, 102–106
 - Data Governance Institute (DGI), 89
 - Data Management Association (DAMA), 89
 - data privacy, 8, 88–90, 100–103, 105, 106, 118, 171–173, 215, 262
 - data protection officer (DPO), 103, 104
 - decentralized finance (DeFi), 129, 130
 - democracy, 5, 37, 51, 101
 - denial of service (DoS), 7, 92
 - dichotomies
 - public/private, 52, 59
 - public/private dichotomies of information, 51
 - public/private dichotomies of spaces, 50
 - public/private dichotomies of the human body, 48
 - digital wallet, 9, 114, 115, 121, 123, 124, 126, 128, 129, 132–134
 - dignity, 32, 37, 38, 93, 94, 100, 207, 218
 - disclosing personal information, 9, 113
 - distributed ledger, 9, 114, 115, 124, 126, 133, 175
 - donor responsibility, 209
 - duty, 15, 195, 214, 223
 - duty to warn, 197
- E**
- East Central Europe, 64
 - educational records, 173, 206, 215
 - Egypt, 6, 54, 56, 58
 - electronic medical records, 195
 - employee privacy, 247
 - employees, 11, 14, 17, 80, 82, 97, 112, 142, 174, 240, 242–244, 246–255, 261
 - employee concerns, 14, 15
 - employee data collection, 14

Ethereum, 9, 114, 115, 128, 132, 176
 ethics of privacy, 4
 Europe, 5, 6, 13, 17, 106
 European Union's General Data Protection Regulation (GDPR), 8, 16, 103, 106, 207

F

Family Educational Rights and Privacy Act of 1974 (FERPA), 215–217
 fractal recursivity, 64
 freedom, 36, 37, 42, 53, 66, 94, 100, 101, 148, 149, 218, 226
 Freedom of Information Act (FOIA), 207, 214, 215, 227

G

governance, 88, 96, 98, 122, 126, 129, 132
 Gramm-Leach-Bliley Act (GLBA), 16, 105

H

Health Insurance Portability and Accountability Act (HIPAA), 12, 16, 95, 171, 190, 195, 198–200, 215–217
 homomorphic encryption, 10, 169

I

identity theft, 35, 112, 113, 115
 ideology, 64
 information privacy, 2, 7, 9, 11, 14, 26, 113, 116, 117, 120, 134, 206, 236, 240, 244, 250, 251, 256, 261
 institutional safeguards, 119, 120
 instrumental value, 33, 34

intellectual property rights, 210
 International Council on Archives (ICA), 207
 International Standards Organization (ISO), 89
 ISO/IEC TS 38505-3:2021—Information technology—Governance of data, 89
 ISO/IEC TS 38505-3:2021 - Information technology — Governance of data, 89
 Internet-of-Things (IoT), 73, 84, 173
 Internet Protocol (IP), 116, 122
 intrinsic value, 32–34
 inviolate personality, 5, 30

K

K-anonymity, 77–79, 84
 know your customer (KYC), 170, 174

L

lack of choice, 113, 117, 120
 liberalism, 36, 37

M

man in the middle (MitM) attack, 8, 74, 75
 meritocracy, 114
 metaverse, 17, 115, 127, 130–132, 134
 Middle East, 5, 184
 moral harm, 195
 moral wrong, 195
 multi-party computation (MPC), 7, 10, 16, 142, 144, 148–154, 174

N

National Institute of Standards and Technology (NIST), 8, 80–82, 84, 163

non-attributable networks, 8, 82

normative dimensions of privacy, 31

O

olfactory privacy, 250, 251

ownership, 25–27, 30, 33, 37, 171, 213, 214

P

password, 81, 91, 92, 121–123, 125, 132, 196, 206

personally identifiable information (PII), 7–9, 72, 77, 82, 84, 116, 119, 121–123, 131, 134, 170, 206, 225, 227, 228

phishing, 92

physical worlds, 1–3, 7

pluralism, 25, 30

primary, secondary, and tertiary spaces, 12, 183, 186, 187

Privacy Act of 1974, 105

privacy and comfort, 11, 183–185

privacy and commodification, 35, 41

privacy and democratic society, 35, 36

privacy and security, 3, 25, 35, 38

privacy and the self, 35, 39

privacy and transparency, 35, 36

privacy calculus, 9, 113, 116–118, 120, 134, 257, 258, 261

privacy concerns, 14, 15, 71–73, 78, 80, 102, 116–119, 134, 173,

206, 223, 225, 256–259, 261, 262

privacy controls, 8, 79, 80, 99

privacy fatigue, 9, 113, 117, 118, 134

privacy paradox, 9, 113, 116, 117, 120, 134, 257

privacy rights/rights to privacy, 11, 14, 24, 26, 31, 32, 35, 38, 40, 41, 72, 211, 216, 217, 221, 222, 252, 253

privacy-specific operating system (OS), 83

private domain, 26, 27, 29, 35

private key, 75, 114, 123–125, 171

professional societies

ACRL Code of Ethics for Special Collections Librarians (2020), 213

Association for Information and Image Management (AIIM), 89

Association of College & Research Libraries (ACRL), 213

Association of Supply Chain Management (ASCM), 236

Council of Supply Chain Management (CSCMP), 236

Data Governance Institute (DGI), 89

Data Management Association (DAMA), 89

International Council on Archives (ICA), 207

Project Management Institute (PMI), 89

Society of American Archivists (SAA), 217

Project Management Institute (PMI), 89

protected health information (PHI), 198, 199, 201, 215

pseudo-anonymity, 121, 134

public key, 123, 124, 126, 128, 163, 166, 171

Public Key Infrastructure (PKI), 75

R

reductionism, 33

regulations, 7, 16, 43, 65, 103, 106, 141, 157, 158, 199, 202, 226, 229. *See also* United States regulations on privacy

European Union's General Data Protection Regulation (GDPR), 106, 207

right to be let alone, 29

S

scalability, 169, 175, 176

smart contract, 154, 174, 175

social behaviors, 8, 83

social engineering, 92

socialism, 65, 188

social transportation-driven order fulfillment, 259

Society of American Archivists (SAA), 206, 207, 212, 216, 217, 222

spatial privacy, 17, 250, 251

spoofing, 75

standards, 7, 28, 30, 32, 47, 48, 55, 57, 61, 62, 65, 80, 95, 97, 99, 122, 147, 149, 162, 207, 221, 223, 239

standards making bodies

European Union (EU), 207

International Standards

Organization (ISO), 89

National Institute of Standards and Technology (NIST), 8, 80, 82

supply chain, 4, 5, 10, 11, 14, 15, 17–19, 142, 174, 235–240, 243, 248, 253, 260

surveillance capitalism, 112, 113, 126

symbolic acts, 52

T

territorial privacy, 2

The California Privacy Rights Act, 105

The Onion Router (TOR), 8, 82, 83

third-party privacy, 209, 211, 212

token economics, 126, 130

transparency, 5, 36, 82, 95, 102, 103, 128, 163, 168, 173, 223, 243, 247, 248, 261

trust, 9–11, 36, 39, 40, 56, 62, 63, 94, 113, 117–120, 125, 131, 133, 134, 167, 169, 173, 176, 194, 196, 213, 253–255, 260, 262

types of privacy

acoustic privacy, 250

bodily privacy, 2

communication privacy, 2, 15

data privacy, 100, 215

information privacy, 2, 113, 120, 244

olfactory privacy, 15, 261

spatial privacy, 14, 15, 261

territorial privacy, 15

visual privacy, 14, 250, 261

U

United States regulations on privacy, 72, 103, 106, 207

California Consumer Privacy Act (CCPA), 172

Children's Online Privacy Protection Act (COPPA), 105

Colorado Privacy Act (CPA), 105

Connecticut Data Privacy Act, 106

Family Educational Rights and Privacy Act of 1974 (FERPA), 215

Freedom of Information Act (FOIA), 207

Gramm-Leach-Bliley Act (GLBA), 105

Health Insurance Portability and Accountability Act (HIPAA), 190, 195, 199

Privacy Act of 1974, 105

- The California Privacy Rights Act, [105](#)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), [226](#)
- Virginia Consumer Data Protection Act, [105](#)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), [206](#), [226](#)
- user access, [122](#)
- V**
- value of privacy, [3](#), [5](#), [24](#), [30](#), [32–35](#), [40](#)
- instrumental privacy, [38](#), [40](#)
 - instrumental value, [32](#), [33](#)
- Virginia Consumer Data Protection Act, [105](#)
- virtual worlds, [2](#), [3](#), [7](#), [17](#), [115](#), [130–132](#)
- visual privacy, [15](#), [250](#), [251](#)
- W**
- Web2, [9](#), [112](#), [113](#), [115](#), [121](#), [122](#), [125–127](#), [131](#), [132](#), [134](#)
- Web3, [7](#), [9](#), [113–115](#), [121–127](#), [129](#), [130](#), [132–134](#)
- West, [18](#), [185](#)
- willingness to disclose personal information, [119](#), [256](#), [257](#)
- work environment privacy, [14](#), [244](#), [250](#), [251](#), [261](#)
- Y**
- Yemen, [184](#), [185](#)
- Z**
- Zero-knowledge proofs (ZKP), [10](#), [158](#), [162–165](#), [168](#), [170–177](#)
- Zero-Knowledge Scalable Transparent Argument of Knowledge (zkSTARK), [10](#), [168](#)
- Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK), [10](#), [163](#)
- zero-sum game, [142](#)