Law and Policy for the Quantum Age

It is often said that quantum technologies are poised to change the world as we know it, but cutting through the hype, what will quantum technologies actually mean for countries and their citizens? In Law and Policy for the Quantum Age, Chris Jay Hoofnagle and Simson L. Garfinkel explain the genesis of quantum information science (QIS) and the resulting quantum technologies that are most exciting: quantum sensing, computing, and communication. This groundbreaking, timely text explains how quantum technologies work, how countries will likely employ QIS for future national defense and what the legal landscapes will be for these nations, and how companies might (or might not) profit from the technology. Hoofnagle and Garfinkel argue that the consequences of CIS are so profound that we must begin planning for them today.

Chris Jay Hoofnagle is professor of law in residence at the University of California, Berkeley and affiliated faculty with the Simons Institute for the Theory of Computing. He is an elected member of the American Law Institute, and author of Federal Trade Commission Privacy Law and Policy (Cambridge University Press 2016). Hoofnagle is of counsel to Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP, and serves on boards for Constella Intelligence and Palantir Technologies.

Simson L. Garfinkel is a pioneer in digital forensics, with a career in technology spanning starting a local internet service provider in 1995 to academia and government service. Garfinkel holds a Ph.D. in computer science from the Massachusetts Institute of Technology, was a tenured professor of computer science at the Naval Postgraduate School, and now is a Senior Data Scientist at the U.S. Department of Homeland Security, a part-time faculty member at the George Washington University in Washington, DC, and a member of the Association for Computing Machinery's US Technology Policy Committee (ACM USTPC). He has authored and edited 16 books, over 100 scholarly articles, and is a fellow of both the ACM and the Institute of Electrical and Electronics Engineers (IEEE). This book is written in Simson Garfinkel's personal capacity and does not reflect the views or policy of the U.S. Government, the U.S. Department of Homeland Security, the U.S. Department of Commerce, or the U.S. Census Bureau.

Law and Policy for the Quantum Age

Chris Jay Hoofnagle
University of California, Berkeley

Simson L. Garfinkel

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108835343
DOI: 10.1017/9781108883719

When citing this work, please include a reference to the DOI 10.1017/9781108883719

First published 2021

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

Library of Congress Cataloging-in-Publication Data

Names: Hoofnagle, Chris Jay, author. | Garfinkel, Simson, author.
Title: Law and policy for the quantum age / Chris Jay Hoofnagle and Simson L. Garfinkel.
Description: New York : Cambridge University Press, 2021. | Includes bibliographical references and index.
Identifiers: LCCN 2021026037 (print) | LCCN 2021026038 (ebook) | ISBN 9781108835343 (hardback) | ISBN 9781108793179 (paperback) | ISBN 9781108883719 (epub)
Subjects: LCSH: Quantum theory. | Quantum computing.
Classification: LCC QC173.96 .H66 2021 (print) | LCC QC173.96 (ebook) | DDC 530.12–dc23
LC record available at https://lccn.loc.gov/2021026037
LC ebook record available at https://lccn.loc.gov/2021026038

ISBN 978-1-108-83534-3 Hardback
ISBN 978-1-108-79317-9 Paperback

Contents

List of Figures . . . xi
List of Tables . . . xv
Preface . . . xvii
Acknowledgments . . . xix

Intro **1**

Part 01 Quantum Technologies **23**

1 Small Phenomena, Big Implications **25**
1.1 Uncertainty . . . 25
1.2 Entanglement . . . 26
1.3 Superposition . . . 27
1.4 Conclusion . . . 29

2 Quantum Sensing and Metrology **31**
2.1 First-Generation Quantum Sensing . . . 36
2.2 Modern Quantum Sensing Approaches . . . 39
2.3 Quantum Sensing Applications . . . 47
2.3.1 Measuring Time . . . 47
2.3.2 Sensing Location . . . 51
2.3.3 Sensing Gravitational Fields . . . 65
2.3.4 Quantum Illumination . . . 68
2.3.5 Quantum Radar . . . 71
2.4 From SIGINT to MASINT . . . 74
2.5 Quantum Sensing: Conclusion . . . 75

3 Understanding Computation **77**
3.1 Mechanical Calculation . . . 78
3.2 The Birth of Machine Computation . . . 80
3.2.1 Combinatorial Problems . . . 80

3.2.2 Numerical Analysis 82
3.3 Numeric Coding 83
3.3.1 Encoding Digital Information 86
3.3.2 Digital Computation 90
3.4 Computing, Computability and Turing Complete . . . 91
3.4.1 Introducing The Halting Problem 94
3.4.2 The Halting Problem Cannot Be Solved 96
3.4.3 Using The Halting Problem 97
3.5 Moore's Law, Exponential Growth, and Complexity Theory 98
3.5.1 Software Speedups 102
3.5.2 Polynomial Complexity (P) 106
3.5.3 Nondeterminism 107
3.5.4 NP-Complete and NP-Hard 110
3.5.5 NP-Complete Problems Are Solvable! 115
3.5.6 BQP, BPP, and Beyond 116
3.6 Computing Today 118
3.7 Conclusion 119

4 The Birth of Quantum Computing 121
4.1 Why Quantum Computers? 122
4.1.1 Richard Feynman and Quantum Computing . . 122
4.2 Reversibility 124
4.2.1 The Arrow of Time 125
4.2.2 The Second Law of Thermodynamics 126
4.2.3 Reversible Computation 130
4.2.4 The Landauer Limit 134
4.3 Cellular Automata and Conway's Life 136
4.3.1 Computing with CPUs, GPUs, and CA(s) . . . 136
4.3.2 Life (The Game) 140
4.4 Digital Physics 145
4.4.1 Edward Fredkin and Project MAC 146
4.5 Reversible Computing and Supercomputing 151
4.5.1 A Most Successful Term Paper 151
4.5.2 Reversible Computing Today 153
4.5.3 Defense Money 157
4.6 The Conference on The Physics of Computation (1981) 159
4.7 Russia and Quantum Computing 162
4.8 Aftermath: The Quantum Computing Baby 164
4.8.1 Growing Academic Interest 164

4.8.2 The First Quantum Computers 168
4.8.3 Coda 169

5 Quantum Computing Applications 173
5.1 Simulating Physical Chemistry 174
5.1.1 Nitrogen Fixation, without Simulation 181
5.1.2 Modeling Chemical Reactions 184
5.2 Quantum Factoring (Shor's Algorithm) 188
5.2.1 An Introduction to Cryptography 190
5.2.2 Forty Years of Public Key Cryptography 196
5.2.3 Cracking Public Key with Shor's Algorithm . . 199
5.2.4 Evaluating The Quantum Computer Threat to Public Key Cryptography 203
5.2.5 Post-Quantum Cryptography 208
5.3 Quantum Search (Grover's Algorithm) 210
5.3.1 Symmetric Ciphers: DES and AES 210
5.3.2 Brute-Force Key Search Attacks 214
5.3.3 Cracking AES-128 with Grover's Algorithm . . 218
5.3.4 Grover's Algorithm Today 223
5.4 Conclusion 226

6 Quantum Computing Today 229
6.1 How to Build a Quantum Computer 231
6.2 The Quantum Computer Landscape 235
6.2.1 Comparing Quantum Media 236
6.2.2 Five Kinds of Quantum Computers 237
6.3 Skeptics Present Quantum Computing's Challenges . . 242
6.3.1 Scientific Challenges 243
6.3.2 Engineering Challenges 245
6.3.3 Validation Challenges 248
6.3.4 Ecosystem Challenges 248
6.3.5 Quantum Supremacy and Quantum Advantage 249
6.4 The Outlook for Quantum Computing 253

7 Quantum Communications 257
7.1 Information-Theoretic Security 260
7.1.1 An Easy Math Problem 260
7.1.2 A Hard Math Problem 261
7.1.3 An Impossible Math Problem 262
7.2 Golden Ages: SIGINT and Encryption Adoption . . . 264

7.2.1 The Golden Age of SIGINT 264
7.2.2 The Golden Age of Encryption 270
7.3 Quantum Random Number Generation (QRNG) . . . 271
7.4 Quantum Key Distribution 276
7.4.1 BB84 277
7.4.2 How QKD Works 279
7.4.3 Why QKD Is Secure 283
7.4.4 QKD Gains Momentum 286
7.4.5 QKD Commercialized, Miniaturized 289
7.5 Quantum Internet 293
7.6 Conclusion 300

Part 10 Shaping the Quantum Future 303

8 Quantum Technologies and Possible Futures 305
8.1 Do Quantum Artifacts Have Politics? 305
8.1.1 Threat Modeling 307
8.1.2 Future Quantum Technology Scenarios 308
8.2 Scenario 1: Government Superior and Dominant . . . 309
8.2.1 Winner Take All 310
8.2.2 Strategic Surprise: Cryptanalysis 315
8.2.3 Forged Signatures and Our Legal Realities . . . 322
8.2.4 Attacks on Passwords and Other Authentication Systems 325
8.2.5 Strategic Surprise: Nuclear Weapons 331
8.2.6 Quantum Strategic Surprise: Chemical, Biological, and Genetic Weapons 332
8.2.7 Strategic Surprise: Remote Sensing 335
8.2.8 Quantum Strategic Surprise: QKD and Quantum Internet 339
8.2.9 Quantum Strategic Surprise: Secrecy and Leakage 341
8.2.10 Countermeasures in a Government-Dominant Scenario: Disruption, Denial, Degradation, Destruction, and Deception 344
8.3 Scenario 2: Public/Private Utopia 347
8.3.1 How Quantum Technologies Could Change Governance and Law 350
8.3.2 Implications for Human Primacy 355

8.4 Scenario 3: Public/Private, East/West Bloc 361
8.5 Scenario 4: Quantum winter 366
8.6 Conclusion 372

9 A Policy Landscape 375
9.1 Quantum Technology's Policy Impact 376
9.1.1 Game-Changers: Code-Breaking and Possibly Machine Learning 378
9.1.2 Quantum Technology Dominance 379
9.2 Industrial Policy 380
9.2.1 National Quantum Investments outside The US 380
9.2.2 US Quantum Technology Industrial Policy . . . 383
9.2.3 Industrial Policy: Options and Risks 385
9.2.4 Innovation and The Taxpayer 392
9.2.5 The Risk of Choosing Poorly 397
9.3 Education Policy 401
9.3.1 Graduate Training in QIS 401
9.3.2 The Human Capital Challenge 407
9.3.3 Faculty Research Incentives 408
9.4 National Security and Quantum Technologies 411
9.4.1 Export Controls 413
9.4.2 Quantum Technology and Space Law 422
9.4.3 Quantum Technology and Cybersecurity 424
9.5 Quantum Technology and Privacy 426
9.5.1 Secrets and Their Time Value 427
9.5.2 Regulation of Decryption 428
9.5.3 Challenges of Government Power 433
9.5.4 The European Approach to Privacy Rights . . 437
9.6 Quantum Prediction 440
9.6.1 Product development 441
9.6.2 Fairness 443
9.7 Measuring Quantum's Research Output 446
9.7.1 Academic Publications 446
9.7.2 Quantum Technology's Patent Output 451
9.8 Conclusion 454

10 The Quantum Age: Conclusions 457
10.1 Quantum Computing Winter Is a Probable Scenario for 2030 458
10.1.1 Public/Private Scenario 459

10.2 Assessing the Next Decade of Quantum Technologies . 460
10.2.1 Prospects for Quantum Sensing 460
10.2.2 Prospects for Quantum Computing 461
10.2.3 Prospects for Quantum Communications 462
10.3 Law and Policy Priorities for the Quantum Age 464

Appendices **469**

A Introduction to the Quantum Realm **471**
A.1 The Quantum World: A Brief Introduction 472
A.2 Terminology, Size, and Frequency 473
A.2.1 The Atom 474
A.2.2 Quantum Sizes 475
A.2.3 Light 477
A.2.4 Quantum Speeds 479

B Introduction to Quantum Effects **483**
B.1 Wave Mechanics 483
B.1.1 Quantum Swirls 484
B.1.2 Light: Newton Thought It Was a Particle . . . 488
B.1.3 Light: It Acts Like a Wave 488
B.1.4 Light: How Can It Possibly Be a Wave? 492
B.2 Quantum Effects 1: Uncertainty 501
B.3 Quantum Effects 2: Polarization 505
B.3.1 Six Experiments with Quantum Polarization . 509
B.4 Quantum Effects 3: Entanglement 513
B.5 Quantum Effects 4: Superposition 517
B.6 The Cat State 522
Bibliography 525

Index **567**

Colophon **577**

List of Figures

1.1 Superposition is like a coin toss 28

2.1 A superradiant laser 33
2.2 NMR of ethanol 37
2.3 Micrometer-sized, single-photon emitters. 44
2.4 Rydberg atoms used to detect radio frequency across the entire spectrum 49
2.5 NIST's ytterbium ion clock 50
2.6 US Navy Quartermaster Seaman Delaney Bodine uses a sextant. 56
2.7 Detecting the gravitational quadrupole of a simple submarine model. 62
2.8 Engine room in an Ohio class nuclear submarine. 62
2.9 A ghost image of a toy soldier. 69
2.10 Ghost images under turbulence and time separation . 70
2.11 The Coherent Hard X-ray Scattering (CHX) beamline at the National Synchrotron Light Source II. 71
2.12 The Lockheed HAVE BLUE stealth proof of concept. . 72
2.13 Quantum radar 73

3.1 Using a slide rule to compute that $2 \times 3 = 6$ 84
3.2 A simple AND gate and its "truth-table." 91
3.3 A simple NOT gate and its truth table. 91
3.4 Full adder 92
3.5 Four-bit adder 92
3.6 An illustration of the complexity classes 114

4.1 Feynman diagram 125
4.2 Exercise in entropy 129
4.3 The value of each variable as the program `SORT_NUMBERS` runs 132

4.4 An electron bucket . . . 133
4.5 Rules for John Conway's "Life" . . . 141
4.6 The Fredkin gate (CSWAP) . . . 153
4.7 The Toffoli gate (CCNOT) . . . 153
4.8 Ed Fredkin's course on digital physics . . . 154
4.9 Attendees at the Physics of Computation Conference . 160

5.1 The possible energy states of two electrons in a hypothetical quantum system. . . . 176
5.2 Alice and the Cheshire Cat . . . 186
5.3 A locked suggestion box . . . 193
5.4 The perfluorobutadienyl iron complex IBM used to factor the number 15 . . . 204
5.5 A locked safe . . . 214

6.1 2-bit quantum carry circuit. . . . 234
6.2 2-bit quantum sum circuit. . . . 234
6.3 Four-bit quantum adder . . . 235
6.4 Four-bit quantum adder, optimized. . . . 236
6.5 An ion trap built by the Air Force Research Lab . . . 241
6.6 The Jiuzhang Quantum Computer. . . . 243
6.7 A closeup of the Jiuzhang Quantum Computer . . . 250

7.1 Using a LED for QKD . . . 277
7.2 The NSA's DIANA one-time pad system. . . . 279
7.3 The BB84 Key Exchange Process . . . 282
7.4 Quantum submarine communication . . . 287
7.5 Air Force Research Laboratory quantum key distribution rig . . . 290
7.6 Analysis of Russian intelligence on the US Manhattan Project . . . 291
7.7 xkcd #465: Quantum Teleportation. . . . 298

8.1 A military quantum technology fever dream . . . 311

9.1 Major science, technology, and military projects . . . 394
9.2 Graduate research output in QIS . . . 402
9.3 Patents concerning qubits or quantum entanglement . 452

B.1 Swirls in a soap bubble . . . 485
B.2 Demonstration of wavelength . . . 485

B.3 The photoelectric effect 487
B.4 Newton's rings 490
B.5 Thomas Young's dual-slit experiment 491
B.6 Thomas Young's notebook showing light rays. 491
B.7 Michelson interferometer 496
B.8 Fifth Solvay Conference, Brussels, 1927 503
B.9 Light is a transverse wave 506
B.10 Enhancing a photograph with a circular polarizer. . . 509
B.11 Unpolarized, linearly polarized, and circularly polarized light 510
B.12 Two linear polarizing filters not-overlapping and overlapping 511
B.13 Two overlapping linear polarizing filters aligned 0°, 90° and 0°, 45° 512
B.14 Three overlapping linear polarizers aligned (0°, 90°, 45°) and (0°, 45°, 90°) 512
B.15 Diagram of white light from a candle blocked by colored filters 520
B.16 Diagram of white light from a candle partially blocked by polarizing filters 522
B.17 Diagram showing white light from a candle passing through three filters 522

List of Tables

2.1 Satellite navigation systems 52

3.1 The first 17 presidents of the US. 104

5.1 Decrypting a message encrypted with the Data Encryption Standard by trying all possible keys 215
5.2 Using Grover's algorithm to crack an encryption key. . 219

7.1 A sampling of the intelligence gathering disciplines . . 265

9.1 Subjects associated with QIS graduate theses and dissertations (limited to subjects with more than 100 works) 403
9.2 Nations and number of QIS theses and dissertations . 404
9.3 Nations and number of QIS theses and dissertations . 404
9.4 Institutions with more than 100 dissertations and theses published on QIS 405
9.5 Fields associated with quantum technology 410
9.6 Support for publications on quantum technologies . . 448
9.7 Affiliations listed by authors on quantum technology publications 449
9.8 National affiliation of QIS authors 450

A.1 The electromagnetic spectrum. 480
A.2 The visible electromagnetic spectrum. 480

Preface

THIS book is the result of a chance meeting between the authors in the summer of 2019 on a 12-hour international flight. This was not a case of quantum superposition, but it certainly demonstrates the power of chance.

The *Oxford English Dictionary* defines *quantum* as "A discrete quantity of electromagnetic energy proportional in magnitude to the frequency of the radiation it represents."[1] In this book, we use the term *quantum technologies* to mean tools that use those discrete quantities of energy to provide some utility. Classical technologies are indeed made of those discrete quanta of energy, but when we use a hammer, or fly in an airplane, or even use a computer, we do not concern ourselves with quanta-level energy or effects. Quantum technologies focus on the smallest quanta of energy and their effects, and this focus is what makes quantum technologies so surprising: mastering the physics of the small, has surprisingly large implications. We classify quantum technologies into quantum sensing and metrology, computing, and communications.

In the chapters on computing we distinguish the words *calculation* and *computation*. We use the word calculation to describe rote mathematical processes that are data independent – that is, that can be performed without concern to the numbers being acted upon. We use the word computation to describe all other processing of information, be it mathematical or otherwise. Calculation, such as doubling a number, or determining the number of days in a year by fetching the value from an almanac, can be performed with a simple device. Computation requires a more complex device that can read, execute, and modify its own program. In the academic literature the terms *finite state machine* and *pushdown automata* are used to describe

[1] "quantum, n. and adj.", definition A.5.a, OED Online, Oxford University Press, December 2020.

devices that perform what we call calculation, and *Turing machine* to describe what we call computation.

In this book we use the `courier typewriter font` to present computer code and pseudocode, as well as specific base-10 numbers used in computer algorithms. We use the stylized numbers `0` and `1` when we are referring to binary digits. Thus, `13` = `1101`. Occasionally we may indicate the base using a subscript following the number, or use the Python programming language convention for hexadecimal numbers, such that `1101` $= 1101_2 = 0D_{16} =$ `0x0D`.

We endeavor to list companies, countries, people, and other proper nouns in alphabetical order unless there is a specific reason to list them otherwise. When order is meant to convey importance, we make this clear. So if we write that China, Russia, and the United States are all world powers, we are sorting the countries alphabetically. If we say that the world's most populous countries as of January 1, 2021 are China, India, the United States, Indonesia, and Pakistan, you can assume that China's population is the largest, Pakistan ranks fifth, and you should expect us to cite our source.[2] When numeric order is relevant, we will number using hash-marks, such as when Step #1 is followed by Step #2.

We have a few chemical formulas in this book, and when we present a molecule, we will include the hydrogen atoms and attempt to present the formula in a manner that conveys its structure. That is, ethanol is CH_3CH_2OH and not C_2H_5OH.

Currencies, unless otherwise stated, are in US dollars. When comparing spending across time, we convert to inflation-adjusted US 2020 dollars using the US Labor Department's Bureau of Labor Statistics Consumer Price Index (CPI) and the calculator at www.usinflationcalculator.com.

[2] US Census Bureau, "US and World Population Clock" (2021).

Acknowledgments

Law and Policy for the Quantum Age has been a fascinating and challenging book to research and write. We went long on the history of technology, as we believe that experience with the introduction of previous game-changing technologies offers important context for making decisions about such technologies today. We believe that good technology policy can only be made with a rough-and-accurate understanding of the underlying technology. We are determined to correct much of the misinformation that is present in the popular literature of quantum information science today.

Quantum technologies was a new topic for both authors. Author Hoofnagle decided to research the field after conversations with Lily Lin (Berkeley MIMS 2019), whose narrative made clear that quantum sensing was much more interesting than cryptanalysis. Then, the good folks at Delta Airlines seated author Garfinkel together with Hoofnagle on a long flight back from Tel Aviv in the summer of 2019. Together we discussed the national security implications of quantum technologies and formed plans to write this book.

As part of researching this book, the authors downloaded and reviewed over 1500 scientific articles, popular articles, and books pertaining to the topics discussed herein. We purchased sheets of polarizing material, 3D glasses, and large optical grade calcite crystals so that we could experience first-hand the mysteries of superposition at the macro scale. We haunted online forums, emailed with a Nobel Laureate, and tried the very best we could to make up for the fact that neither of us had studied quantum physics in college.

This book would not have been possible without the thoughtful engagement from many experts in quantum information science, who gave generously of both their time and counsel. We owe many thanks to those who helped us with difficult material, and acknowledge that any mistakes remaining are our own.

We would like to explicitly thank those who answered questions about technology and history while working on this project, including Scott Aaronson, Ross Anderson, Syed Assad, Holger Axelsen, Philip Ball, Charles Bennett, Scott Bradner, Steve Crocker, Nike Dattani, Peter Denning, Edward Fredkin, Joyce Fredkin, Michael Frank, Shohini Ghose, David Grier, Aram Harrow, Marco Lanzagorta, Seth Lloyd, Chao-Yang Lu, Norman Margolus, Henry Minsky, Margaret Minsky, Christopher Monroe, Jian-Wei Pan, Daniel Polanic, Peter W. Shor, Adam Shostack, Bill Silver, Tommaso Toffoli, Rainer

Weiss, and Stephen Wolfram. Tom Slee reviewed our section on chemistry and found several errors, which we attempted to correct; those that remain are ours, not his.

Mark Horowitz at Stanford worked with us to resolve several lingering questions regarding the National Academies report on the potential of quantum computing. Overall, we found the report useful as an initial, highly technical introduction to this complicated topic; we strongly recommend the report to anyone looking for a description of quantum computing that is more technical than the one we present here.

At IBM, we would like to thank Chris Nay for working with us over the course of more than a year in both answering questions and arranging interviews with Charles Bennett, John Smolin, and Bob Sutor.

We would like to thank Diane Carr at ColdQuanta for answering our questions and providing us with overview information; Misha Rindisbacher at Launch Squad for her help in answering questions about the D-Wave computer; and Jason Freidenfelds at Google for answering our questions about Google's efforts.

We especially benefited from Bill Silver sharing with us his notes and recollections of Ed Fredkin's course on Digital Physics, and from Charles Bennett sharing with us his photograph of the 1981 Conference on Physics and Computation.

We also benefited from commentary and support from Geoff Cohen, Andrew Grosso, Burt Kaliski Jr., Darrell Long, Hartmut Häffner and Stuart Schechter..

The text benefited from workshops held by the Haifa Center for Law and Technology (with commentary by Amnon Reichman, Tal David, Shay Gueron, Michal Gal, and Orr Dunkelman); the Sandia National Laboratory (with thanks to Andrew Reddie); and the Ohio State University (with thanks to Dennis Hirschman).

In its final form, various chapters of this book benefited from in-depth reviews by Ross Anderson, Michael Grant, Ted Huffmire, and Bill Silver.

Author Hoofnagle's family, doctors Jay and Mark Hoofnagle and Cheryl Winchell, read drafts and provided commentary; Hoofnagle's father-in-law, Jon Wilbrecht, provided commentary and suggested the ultimate organization of the work. Yasemin Acar helped us with German translations.

We are grateful to our editor, Matthew Gallaway, and colleagues Cameron Daddis, Jadyn Fauconier-Herry, and Chloe Quinn of Cambridge University Press. Our copy editor, Ken Moxham, our proofreader Ian Pickett, and the TeX Support team at SPi Content Solutions, particularly Suresh Kumar, caught and fixed many problems with the text and formatting. Those that remain are ours, not theirs.

This work started as an article that received comment from Lily Lin, Evan Wolff, and Peter Swire; the participants in the Future of Cybersecurity Working Group, particularly Andrew Reddie and Kristy Cappelli; the participants of the Berkeley faculty scholarship workshop, including Jennifer Urban, Sonia Katyal, Christopher Kutz, Andrea Roth, Amnon Reichman, Mark Gergen, Nicole Ozer, Steven Sugarman, Eugene Bardach, Peter Schuck, and Christopher Slobogin; the participants of the Yale Information Society Project paper series, including Laurin Weissinger, Sam Hayek, Nikolas Guggenberger, Tiffany Li, and Mason Marks; the participants of the Privacy Law Scholars Conference including Andrea Matwyshyn, Sue Glueck, Andrew Odlyzko, Maria Brincker, Ot Van Daalen, Katherine Strandburg, Alex Deane, Ari Waldman, Aaron Massey, Pam Dixon, Jeff Brueggeman, Mary Madden, and Nick Merrill.

Special thanks are due to the contributors of *tex.stackexchange.com* who answered our LaTeX questions, as well as to our respondents on *quantumcomputing.stackexchange.com*, *chemistry.stackexchange.com*, *crypto.stackexchange.com*, and *hsm.stackexchange.com* (history of science and mathematics).

The appearance of US Department of Defense (DOD) visual information in this work does not imply or constitute DOD endorsement.

Publication with a *CC-BY-NC* license was made possible in part by support from the Berkeley Research Impact Initiative (BRII) sponsored by the University of California, Berkeley Library and by the Berkeley Center for Law and Technology. We are grateful to Timothy Vollmer, Rachael Samberg, Margaret Phillips, and James X. Dempsey for their support in making an open access version of this work available.

0	1	0	0	0	1	1	0	0	1	1	0	0	0	0	1
0	1	1	0	1	0	0	1	0	1	1	1	0	1	0	0
0	0	1	0	0	0	0	0	0	1	0	0	1	1	0	0
0	1	1	1	0	1	0	1	0	1	1	1	1	0	0	0