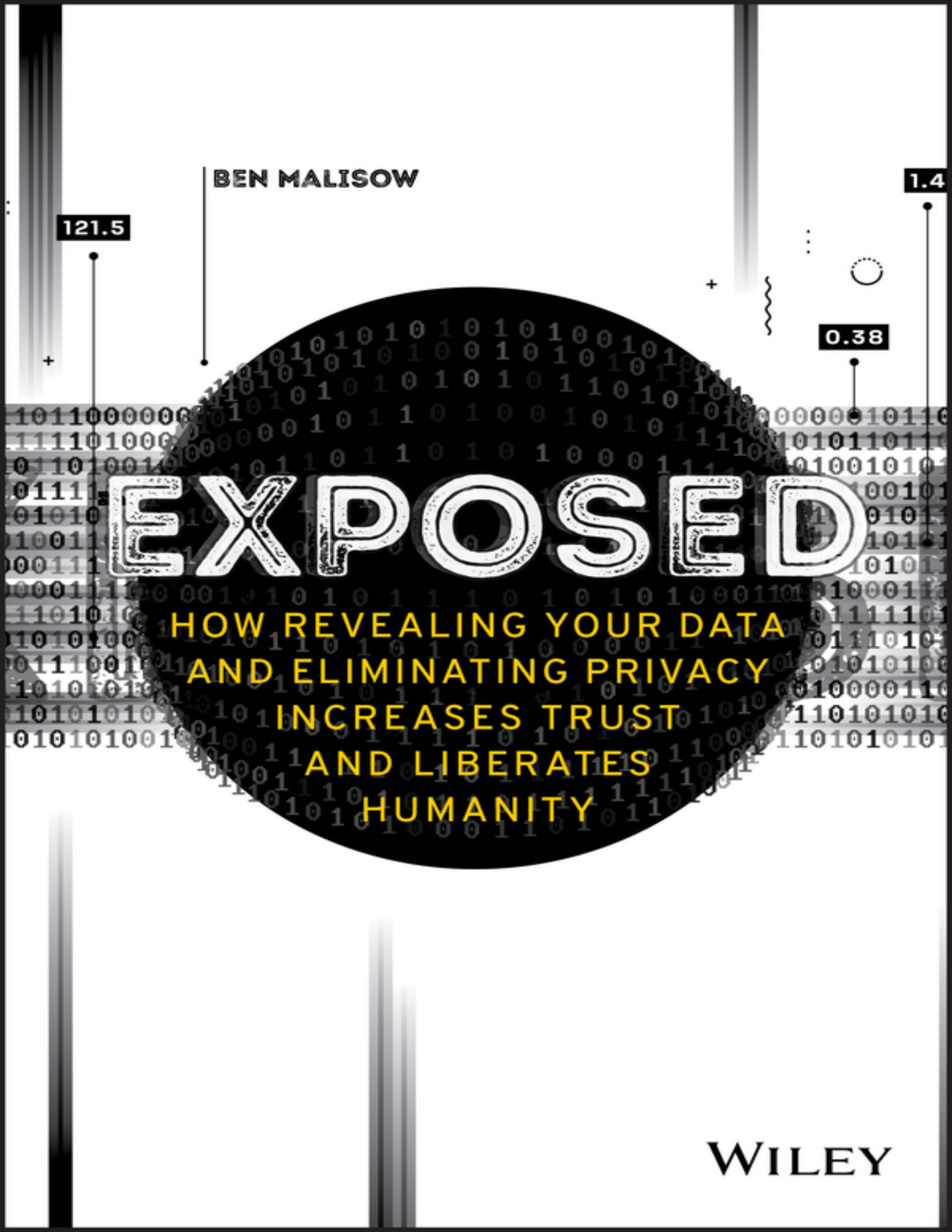
BEN MALISOW
121.5
1.4
0.38
EXPOSED
HOW REVEALING YOUR DATA AND ELIMINATING PRIVACY INCREASES TRUST AND LIBERATES HUMANITY
WILEY

Table of Contents

- Cover
- Introduction
  - The Purpose of Privacy
  - Going to Extremes
  - Please Indulge Me
  - Premises
  - How to Contact the Publisher
  - Notes
- 1 Privacy Cases: Being Suborned
  - Security Through Trust
  - The Historic Trust Model Creates Oppression
  - Privately Trustful
  - Disarmed Forces
  - Missed Application
  - Harmfully Ever After
  - Open Air
  - Artifice Exemplar
  - Notes
- 2 Privacy Cases: Government/National Intelligence/Military Confidentiality
  - National Security vs. Governmental Security
  - A Government Is Not a Nation
  - Rationales
  - No Net Benefit; Possible Net Negative
  - Notes
- 3 Privacy and Personal Protection

Your Exposure
Check Yourself
Take Your Medicine
The Scene of the Crime
You're a Celebrity
Notes
4 A Case Against Privacy: An End to Shame
Cultural Shame
Location, Location, Location
Beneficial Shame, Which Might Be Harmful
Hypocrisy for Thee
Notes
5 A Case Against Privacy: Better Policy/Practices
Policy Based on Bad Data: US Police and Dogs
Policy Based on Bad Data: The DSM
Bad Data Derived from Concern for Privacy: Suicide
Notes
6 A (Bad) Solution: Regulation
Regulation = Destruction
Legitimate Fear of the Private Sector
Exceptions to the Rules
Chill Out
Power Outage
Top Cover
Now You See It ...
The Government Would Never Lie to Its Overseers, Right?
Stressing It

Notes
7 A Good Solution: Ubiquity of Access
If Everybody Knows Everything, Nobody Has an Advantage
Atomicity, Again
An End to Crime?
An End to the Need for Crime?
Power Imbalance
An End to Laws?
Lower Costs
An End to Hypocrisy
An End to Bad Policy
Speaking of Accurate Portrayals of Humanity …
Notes
8 The Upshot
Science Fiction
Molecular Level
Busting My Hump
Troll Toll?
Get Out
On the Genetic Level
Still Scared
Notes
Index
End User License Agreement

Exposed

How Revealing Your Data and Eliminating Privacy Increases Trust and Liberates Humanity

Ben Malisow

WILEY

Introduction

> *“Any sufficiently advanced technology is indistinguishable from magic.”*
>
> *Arthur C. Clarke*

The idea of privacy is that each human being should be able to decide who has information about them. It's an interesting concept: each person creating an island of data and limiting access to the island only to other entities the individual permits.

In practice, it doesn't work, meaning it's both impossible and incredibly harmful to everyone when privacy “rights” are imposed and enforced. This is true for a number of reasons, including human nature, modern technology, and the way data functions and affects interaction.

Today, many people say they want privacy—that they value control of their own information. There is an almost innate, reflexive horror at the idea that someone, anyone, could know something about us that we did not want them to know. Many of us do not feel comfortable with this idea: what if you had no privacy—what if everything you ever did or said was known to everyone else? Each of us may have a different image of the form of that discomfort. Who knows everything about me—the government? Corporations? My spouse? And what would they do with that information? Harm me? Track me? Sell things to me? When we conceive of a dystopia, fictional or real, that depiction usually includes some aspect of loss of personal privacy, from the Big Brother intrusive government of George Orwell's *1984* (the archetypical dystopia)[1] to modern North Korean governmental control of its citizens[2] to the constant and ubiquitous monitoring of our online activity by the

behemoths of the Internet, from Google to Facebook to Apple to Amazon.[3] We fear anyone that has the totality of information; if someone knows everything about me, maybe they can control me. I, myself, prize my privacy and loathe the notion that someone else knows something about me that I did not want them to know.

And yet … we want to know everything about everyone else. We are naturally curious—no, not curious: nosy. We crave gossip and innuendo and accusations; we want to know what happened and when and to whom. We have entire industries thriving on the practice of gathering, analyzing, and distributing information about other people for our consumption.[4] [5] [6] [7] [8] [9] [10] This desire runs exactly counter to our claim that privacy is important, or, at least, it suggests that we want privacy for ourselves, but nobody else.

But what if there was no privacy, for anyone or anything, at all? What if everyone knew everything about everyone else?

Imagine if you could view video from every camera in the world … could listen in on every microphone … could view every person's browser feed … could watch every satellite feed … in real time, unadulterated, any time. But also imagine that every other person had the same ability: your neighbor, your parents, your kids, your co-workers, your friends, and total strangers. What if we could all access every piece of data, live or recorded, at will?

In this book, I'm going to make the case that a world without privacy would be the optimum outcome: all data, everywhere, known to everyone. It's disconcerting; on a very personal level, I don't like the feeling I get when I consider this idea, and I think most people feel the same way. But, rationally, using objective reason instead of emotional reaction, it makes much more sense than the ultimate (unobtainable) goal of every individual having total

control of information, and it is absolutely preferable to the bizarre patchwork of information disparity we currently have, where certain people and institutions have access to particular information, others have access to different sets of information, and each individual person has only limited glimpses of the whole.

The Purpose of Privacy

To begin with, it's good to dissect why this idea makes us feel uncomfortable. Why do we want (or think we want or say we want) privacy? For the most part, we think privacy will give us security; the two words are often used together, sometimes mistakenly synonymously. For most of my life, I have worked in industries where the collection, distribution, and protection of information was valuable: the military, journalism, teaching, and computer security. For security practitioners, one of the fundamental premises is called the *Triad* of security goals: confidentiality, integrity, and availability.[11]

- **Confidentiality:** Only authorized people can get access.
- **Integrity:** Only authorized transactions are allowed.
- **Availability:** The asset exists when authorized people are authorized to make transactions.

From this perspective, privacy is usually perceived as an aspect of confidentiality; individual people want control of the confidentiality of information that identifies them. And confidentiality isn't used just for personal privacy; it's used to secure data and assets in all types of activities, organizations, and business. We've depended on confidentiality as part of our effort to attain security for so

long that it's hard to imagine being secure without it; it's a cornerstone of the security profession.

But it's not necessary. In fact, confidentiality often inhibits security.

For example, one of the desires we have about privacy is to protect ourselves financially—we don't want anyone else knowing our bank account information or the credentials we use to access the account (passwords, identification cards, bits of information like name and address and birthdate, etc.). Banks spend a lot of money protecting these credentials,[12] and we expend effort creating and maintaining them. All of this effort has a financial cost, which negatively impacts the financial benefit of the process and investment. Every amount the bank spends on securing the transaction is an amount charged to the customer, either through direct fees or in reduced interest on the investment—you would make more money with your account if security wasn't an additional cost of the process. This is all to prevent fraudulent transactions—someone pretending to be you in order to get your money.

But this can happen only because the *criminal* has privacy. If all of the information about all of the transactions, legitimate and fraudulent, is known to everyone, then there is no opportunity for theft. If the bank knew when someone other than you tried to take your money, the bank would not give the money to that person. *If every action of every person is known to every other person, no transaction fraud could exist*. A criminal can't engage in theft by fraud if we all know what the criminal is doing and who the criminal is.

Total transparency, then, directly counters the need for confidentiality … and improves the lives of everyone involved, because we no longer have the costs associated

with the need for confidentiality, and we can all then derive the greater benefits.

Going to Extremes

Take this to an even greater extreme and get weird with it: why do we even have banks? Again, it's a perceived need for security, based on money. We put our money in a bank so that someone else doesn't take our money without our permission. But … if everyone knows everything about everyone else, we would know if someone without permission took money from someone else. We would know if a crime was committed, and we would know who the rightful owner of the money is. The need for banks would be greatly diminished or dissipate altogether … and the cost of banking would similarly evaporate, and each individual person would get greater value from their own money.[13]

If what I'm describing is starting to make you feel uncomfortable and the idea of everyone watching your every action is creeping you out, that's understandable and completely normal. I'm not trying to describe a police state where you're being watched by law enforcement every moment of every day. Forget the *how* of this proposal for the moment; I'll get into theoretical mechanisms for achieving these goals throughout the book. (And, to be clear, I do not have a comprehensive way of accomplishing these goals. Putting these theories into practice will require the contribution and coordination of many experts, organizations, and thinkers. This book is intended to be a catalyst to start that conversation. But I think the discussion in society about privacy thus far has been overwhelmingly one-sided: everyone seems to be pursuing ways to implement and mandate more privacy, not less, as a means to ensure security. I think they're mistaken.)

It's worth noting that some jurisdictions (some cultures, some populations) value privacy in different ways. For instance, the European Union, right now, has decided that personal privacy is a human right, tantamount to living; this is codified and mandated by the General Data Protection Regulation (GDPR), which gives some power to individuals in terms of imposing who can or cannot disseminate their personal data.[14] This law also gives an even greater amount of power to the governments of the European Union, as enforcers acting on behalf of the individuals they supposedly protect. This law is mimicked around the world; similar statutes exist in countries such as Japan,[15] Switzerland,[16] Australia,[17] Canada,[18] Argentina,[19] Singapore,[20] Israel,[21] and others, as well as the American states of California[22] and New York.[23]

> **NOTE** In government, healthcare, technology, and other fields, personal data is often referred to as *personally identifiable information* (PII). PII generally includes each person's name, address, date of birth, mobile phone number, the logical and physical addresses of their computer/device (the IP and MAC addresses), government-issued ID numbers (such as social security, driver's license, and passport numbers), and more. Privacy laws vary by jurisdiction, so what is defined as PII in one location may not be considered PII in another.

Other jurisdictions, on the other hand, have laws and practices that are in direct opposition to personal privacy. China, for instance, has laws that require that the government have access to all online activity, including the ability to monitor the action/communication of each individual.[24] In the same vein as the European Union's justification for the GDPR, China's rationale for monitoring

is to protect the citizenry. But unlike the EU, which purports to protect individual privacy, China's stated intent is a different excuse for police powers: Chinese authorities want to protect society from criminals who operate in secret or prevent disruption of society that might result because of “bad” information or influence.

Meanwhile, in the United States, prevailing national law runs exactly counter to the very idea of privacy: instead of each individual having an absolute right to privacy, each individual has an absolute right to free expression. This is codified in the US Constitution and in the First Amendment (twice, in fact, as both the freedom to say what you want and the freedom to distribute/publicize what you say—freedom of speech and freedom of the press).[25] So instead of you telling me what I can say about you, I can say anything I want about you, to anyone or everyone. That applies regardless of whether “you” means an individual, a government, or a corporation. Perhaps not surprisingly, this approach of freedom of speech, combined with transparency, will be most in line with the argument for improving the human world I'll make throughout this book.

Please Indulge Me

I'm going to ask for your indulgence as you read the rest of the book. It might seem, in a few places, that I'm suggesting that a police state is somehow preferable to personal privacy—that is definitely not the case. In fact, I think it is much more likely that privacy laws create a situation for a police state to grow and flourish. I prefer personal, individual freedom over all other things. It might also seem like what I'm describing is science fiction—that what it would take to achieve total transparency is impossible. I ask you to momentarily suspend your disbelief for the purpose of this discussion and examine the topic

objectively, from the perspective of the desired end-state, and not the complications of the possible implementations.

Finally, it's probably best we all agree that there is no actual privacy (or that there probably never really was): someone knows everything about you. Not that any one person knows all the things—but all the people who know things about you could get together and assemble all that data and nothing you've done or said would be private anymore. Someone, somewhere, singly or collectively, has all of it—whether that someone is the government, corporations, or trusted loved ones, you have no privacy. You have an illusion of privacy, or the faux privacy of anonymity. These are not worth the expense and cost that the false benefit of “privacy” supposedly provides.

Premises

Secrecy is not security; confidentiality is only one leg of the Triad. If other legs of the Triad are violated/abrogated, we can lose security just as easily as if we lost confidentiality. Privacy is not security—but we often think privacy will give us security. Privacy requires secrecy; if you cannot enforce confidentiality, you have no privacy.

In the rest of this book, I’m going to describe ways that privacy and secrecy hinder actual security, or how security (whether attained through confidentiality, integrity, or availability) can harm people. It’s important to understand that what we say we want, or what we think we want, is not something that is actually beneficial or useful (or at least as not as beneficial/useful as we think, especially compared to other choices). Privacy is not a magical solution to perceived problems, and privacy might actually cost each of us more than the potential benefits it provides. We might all benefit more, as individuals, from security methods other than limiting access to our own data islands. And

other approaches would not incur the costs privacy requires.

Another premise: to properly discuss privacy, we need to discuss adult topics, because we, as people, usually want privacy for adult reasons (financial, sexual relationships/activity, death, business, etc.). This book will deal with those topics in frank and adult terminology—if you're uncomfortable with adult conversation, you may find parts of the book uncomfortable.

Finally, while reading the rest of the book, try to imagine that each person on the planet has a magical capacity to view and hear everyone else on the planet: a television set that can be instantly tuned to any other person, anywhere, that not only displays real-time data, but all prior activity—all historical actions and speech of every other person.

I'm not using this premise because I'm excited about the potential; from the perspective of someone who was raised in a culture that respected privacy and someone who has been engaged in the practice of security in one way or another for most of my adult life, this premise seems awkward, intrusive, dangerous, and makes me very uncomfortable.

But my personal feelings/biases don't matter: I also realize that the future I'm describing is almost here, and that it is inevitable. While I'm not relishing its arrival, I'm trying to view it as objectively as possible, and I anticipate the pitfalls and predict the opportunities. I know the situation that brings me discomfort is upon us, and I know that we can exacerbate the danger and difficulty of the transition from a private world to the post-privacy world, if we approach it with obsolete tools and philosophies.

And that magical TV set is just a step away from what we have right now—and it's only magical in Arthur C. Clarke's

sense of technological sophistication. It would be better if we could start figuring out how to use our next magical tool instead of pretending it will never arrive.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line “Possible Book Errata Submission.”

Notes

1 Orwell, G. (1955). 1984. New York: New American Library

2 www.hrw.org/world-report/2019/country-chapters/north-korea#

3 abcnews.go.com/Technology/ceos-amazon-apple-facebook-google-face-congressional-antitrust/story?id=72034939

4 www.tmz.com

5 people.com

6 starmagazine.com

7 marketingplatform.google.com/about/enterprise [formerly DoubleClick]

8 www.cambridgeanalytica.org

9 www.lexisnexis.com/en-us/products/public-records.page

10 www.equifax.com/personal

11 www.elsevier.com/books/the-basics-of-information-security/andress/978-0-12-800744-0

12 www.americanbanker.com/articles/financial-firms-to-further-increase-cybersecurity-spending

13 Granted, banks provide services other than protecting savings, such as commercial/residential loans and currency exchange.

14 General Data Protection Regulation, OJ L 119, 04.05.2016 § (EU) 2016/679 (2018)

15 iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information

16 www.admin.ch/opc/en/classified-compilation/19920153/index.html

17 www.oaic.gov.au/privacy/the-privacy-act

18 www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda

19 servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

20 www.pdpc.gov.sg

21 www.gov.il/en/Departments/the_privacy_protection_authority

22 leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

23 www.dos.ny.gov/coog/pppl.html

24 www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html

[25] www.law.cornell.edu/constitution/first_amendment

1
Privacy Cases: Being Suborned

“Well … how did I get here?”

—David Byrne, “Once in a Lifetime”

To discuss the relative merits of personal privacy, it's worth reviewing historic rationales and justifications for security processes and programs. Privacy and security have become linked to the point where the ideas are almost inextricable, and it is valuable to understand how this came to happen.

Security Through Trust

One of the concepts that relates to privacy is security through trust— an institution, government, or company is considered more trustworthy if the personnel working in or for it are themselves trustworthy. To determine whether a person is trustworthy, it's important to learn certain things about the person: their behavior, tendencies, condition, mindset, and so forth. Trust is established based on past performance; we tend to believe that someone will act more or less in a manner similar to how they already have. The assumption is: a lying junkie will continue to be a lying junkie; a person who has worked diligently and honorably for their entire adult life will continue to behave diligently and honorably. There are, of course, outliers and changes in circumstance where predictions are wildly unhinged from the past; the junkie might change overnight and become a paragon of virtue and a hard worker, whereas the model employee might turn into a depraved murderer in a moment. Human beings are fickle, unpredictable, irrational creatures. But if you have to trust someone, you will

generally tend to use their past actions as an indicator for what you expect of them in the future.

The Historic Trust Model Creates Oppression

Not so long ago, many organizations had some rather bizarre criteria programmed into their trust models—metrics that we would find ridiculous, offensive, stupid, and/or downright evil today. These have included gender, race, religion, ethnicity, and national origin.

For instance, at the outset of World War II, American President Roosevelt considered people of Japanese descent, including American citizens with Japanese parents and grandparents, untrustworthy, to the point where he believed they might aid Japan in its war against the United States. He therefore ordered them to be forced into concentration camps.[1] The rationale was: this would make the United States more secure. Personal privacy, in that circumstance, was not an aspect of the trust model; significant physiognomic traits, combined with birth and immigration records, allowed the US government to enforce this horrible decision. There was not much room for question as to the ethnicity of the prisoners.

Privately Trustful

Another awful aspect of the personnel trust model was, however, larger a facet of what is generally considered "private" life: whether that person engaged in same-gender sexual activity.

NOTE For purposes of discussion in this book, I'll use the term *gay* to mean the full spectrum of what we now often call LGBTQ—lesbian, gay, bisexual, transgender, queer—sometimes with additional descriptors.

There were two main (ugly and horribly flawed) rationalizations for this type of policy.

- Gay people are untrustworthy because of their very nature; sexual orientation is a choice, gay people engaging in sexual acts is an indicator of character, and only depraved people would choose to do so.
- Gay people are untrustworthy because they are susceptible to coercion; anyone learning of a person's sexual interactions or desires could use that knowledge against the person—a gay person could be blackmailed for being gay.

The first “reason” is so tragically stupid that it's hard for people today to realize that people in the past actually believed ideas like this. It almost certainly had origins in religious and cultural biases and misanthropic tendencies tantamount to evil. The second rationale is insidious in a different way and is a perfect of example of how privacy and security can become conflated to the point of causing true harm to the very things they purportedly are meant to protect.

NOTE At the time the laws/policies discussed in this chapter were created/implemented/enforced, there were other terms used to describe any sexual activity that did not conform to heteronormative standards, typically *unnatural acts* and *sodomy*, when included in statutes or other written mandates.

The historical personnel trust model is based on some simple premises: institutional trust is linked to personal trust, personal trust is based on using past behavior to predict future action, and personal behavior outside the workplace (such as sexual activity) is linked to personal behavior in the workplace. For the institution to trust the individual for a particular job, the institution must learn and know about the person's behavior outside the workplace, in their personal life. That's the institution's perspective.

Generally, from the individual's perspective (instead of the institution's), we like to think of a person's home life and work life as two separate, distinct contexts: I act in accordance with my employer's needs during the hours I'm working, because that's what I'm getting paid for, but when I am not working, I am free to live my life in the manner I see fit, without my employer's oversight. I might wear a uniform in the workplace, but I take it off when I'm not working; I associate with colleagues and customers while I'm working, but I might have a totally different set of friends and acquaintances when I'm not working, and I might not interact with the workplace colleagues/customers until I'm back in the workplace.

In reality, this construct often breaks down in actual practice. Colleagues and customers share information about their nonwork activities in workplace discussions, and actions a person takes outside the workplace can

seriously affect their employment, be it acquiring a college degree or running someone over with a car while driving drunk. Even so, we often like to think of ourselves as having a bifurcated existence.

In order for the dated trust model, which discriminated against gay people to have existed, the institution had to breach the employee's private life—sex is generally (with very, very few exceptions) an activity that happens outside the workplace. This intrusiveness was seen as necessary in order to ensure that the person placed in a position of trust by the institution was, indeed, trustworthy.

This, of course, makes absolutely no sense, when exposed to even the barest logical scrutiny. Were gay people subject to blackmail/coercion because of their same-gender sexual activity? Yes—*but only because the institutional trust model created that situation*. The person who is given employment or promotion only under the condition that they act in a prescribed manner (or, more to the point, do not act in a proscribed manner) is under the threat of losing something of value (a job, a promotion, etc.) if their unapproved behavior becomes known.

Disarmed Forces

Here's a historic example: the US military has its own laws and court system; this is known as the Uniform Code of Military Justice (UCMJ). Not too long ago, the UCMJ prohibited same-gender sexual activity; violations could be punished with demotions, dismissal, or even imprisonment.[2] The government had similar, if more vaguely worded, restrictions in Executive Order 10450, “Security Requirements for Government Employment.” In both the military and other government positions, a security clearance (the documented verification of a

person's trustworthiness) was (and still is) considered extremely valuable—a person with a security clearance could get employment and other opportunities that a person without a clearance could not. A person in the military/government service could lose their security clearance if the military/government learned that the person was gay.[3]

So, the military/government (and institutions who had similar anti-gay policies) had created a situation where certain people had something to lose (the clearance, and the benefits that come with a clearance) if information about them (personal information, from their “private” life) was disclosed. That, therefore, put those people at risk of coercion and put the institution at risk overall (a trusted person might be coerced into causing harm to the institution). If, however, the anti-gay rules/policies did *not* exist, then the entire possibility for coercion would not exist, and trust would not be in question.

NOTE Within reason, and taken in context, a person might not be subject to coercion *only* because of their employment status and situation, and that employer's policies—there might be other aspects of a person's life that could be used to coerce them into harming their employer. At the time the UCMJ had rules against same-gender sexual activity, there were also social mores and prejudices that might make someone gay subject to coercion as well; a blackmailer might threaten the target with outing them to their *family* as opposed to their employer and might therefore get the victim to do something harmful to the employer. “I will show these photos of you with your gay lover to your children, unless you steal these files from your office.” Societal and cultural dysfunction played a large part in workplace discrimination, as well. Typically, however, the employers' rules both reflected and exacerbated the cultural norms.

Missed Application

While employer-created susceptibility to coercion was bad enough, these institutions further harmed themselves by adhering to this flawed trust model in the application and enforcement of the mandates. The rules were never applied fairly, uniformly, or sensibly; there are many notorious cases where the rules were instead used to settle personal workplace grudges, by resentful lovers/spouses/friends as revenge, for political damage, to gain advantage by a competitor for a position/promotion, or even simply by small-minded bureaucrats insistent on following the law regardless of sense or harm to the “lawbreaker.”

Here's one example of lack of uniformity/sense in applying the rules (and the trust model) regarding personal (private) behavior: a group of British men, acting as Soviet spies from the 1930s through the 1950s, known as the Cambridge Five.[4] At least two of the men were gay, and a third bisexual[5] … and almost all of them were known to regularly abuse alcohol, to the point where drinking significantly impacted their behavior (one of the KGB handlers of the spies noted that one of the Five, MacLean, may have revealed the fact that he was a spy to both a lover and a sibling while drunk). Yet none of them was prosecuted by the British government, although their behavior was presumably known to British authorities as well. This can be directly contrasted with the case of Alan Turing, another British government employee, whose cryptographic work is famously thought to have been instrumental in the Allied effort to win World War II. Turing was convicted of "indecency" in 1952, under the Criminal Law Amendment Act of 1885,[6] and was subjected to chemical castration as part of a sentencing arrangement; he lost his security clearance as well, which ended his consulting work with the British government and may have led to his suicide in 1954 (the details of his death do not rule out accidental causes).

Arbitrary enforcement of any law is atrocious; it degrades the rule of law and overall concepts of justice. However, with these particular laws, designed specifically to control the private lives of citizens, lack of uniformity in application creates fear, mistrust, and a horrific sense of unease and anxiety among the very people the laws are supposed to protect. Anyone who might be victimized by their own legal system is naturally terrified of this possibility. To underscore the relationship of this situation to the premise of the book: *laws designed to protect privacy necessarily create situations where there are "private" lives/data*

distinct from “open” lives/data, and situations where the distinction between what is known and what is not, especially by law enforcers and the individuals affected, can cause fear, mistrust, and unnecessary hardship on individuals. Moreover, even laws created with the very best of intent (and, to give the benefit of the doubt to lawmakers, let's assume that means all laws, although I certainly think there's a great deal of room to argue that point) often have unintended consequences. With privacy laws, one of the obvious, predictable, “unintended” consequences is to create sets of data that are sensitive—giving power to those people and institutions that are allowed to transcend or abrogate those laws (such as the government and law enforcement entities). A set of data that is sensitive is a set of data that can be leveraged, often to the detriment of the very citizenry who are supposed to be protected by those laws (the individuals who the data describes). Again: by creating “protected” information, we create a potential to cause harm.

Harmfully Ever After

What harms did those obsolete laws and policies, based on the atrociously flawed trust models, cause? Aside from the personal harm to each individual affected (those like Turing who lost their jobs, prominence, and respect in their fields of endeavor, and often freedom), what harm does this cause to society at large?

The first and most obvious terrible impact is the loss of potential candidates for trusted positions that become ineligible. This might happen through self-elimination—candidates who fear being identified and punished for personal actions/behaviors/beliefs therefore do not even attempt to pursue positions where they might be considered or investigated. It also includes those people

who still attempt to take those positions but are turned away or rejected by the institutions as unsuitable. On top of these are the people who still sought those positions (knowing that they, themselves, could be identified, eliminated, or even prosecuted), actually achieved their intent and took those roles, but then were fired/removed from the positions later because their private lives and actions came to light.[7] Qualified, accomplished people have been removed from candidacy for those positions, or removed after a time of faithful service, and the negative impact is felt by both the institutions and the society as a whole that is served by those institutions.

And possibly the most terrible harm in distinguishing a “private” life from a “public” persona is creating a situation where the person in a position of trust—in a job, in their community, in their family—must always have a continuous fear, the constant knowledge that at any time their livelihood and identity could be ruined, if they were to be “outed” (that is, if someone reveals the heretofore “private” knowledge about them, without the target's consent/permission). This must be a lingering, gnawing apprehension, something that infects and degrades every success and keeps people who experience this risk from enjoying their lives fully. That is a severe cost, and a constant toll. It's one of the reasons why many laws in many jurisdictions have a statute of limitations: every perpetrator must live with the constant knowledge that they could be arrested and prosecuted at any moment, that they are hunted, and that is a form of punishment in itself.

At first pass, this might seem like a reason *for* privacy: to set up stringent distinctions between an individual's private life and their public identity. We might view as beneficial the possibility of distinguishing, for ourselves, what is revealed to others, and what is held in secret. In practice, however, this causes only opportunities for abuse,

malfeasance, and fear: anything secret and distinct lends a potential for exploitation and attack—anyone with entrée to your (supposedly) private life has power over you, even if that power can only be used to hurt you.

Open Air

How would openness and an end to privacy have served as a benefit to the gay people vilified and persecuted by laws like Executive Order 10450 and the Criminal Law Amendment Act? Wouldn't the *lack* of privacy have been more damaging to the targets of those laws, denying them any opportunities for positions of trust, by not allowing them to keep their identities and behavior secret? (That is, is there an argument to be made that *having* privacy created the only opportunity for gay people to attain those positions of trust in a hostile environment?)

The answer is: if the actions of every person were known to every other person, then same-gender sexual activity (or any activity associated with gay people) would not and could not be seen as wildly deviating from the norm, nor as inherently dishonorable or disreputable, for two reasons—the significant percentage of human beings who engage in the proscribed behavior and the existence of a large number of gay people known to be eminently trustworthy.

If everyone knows that everyone else engages in a particular activity, that activity cannot reasonably be vilified … and even if prejudices and social mores exist that attempt to vilify the particular activity, *enforcement* cannot be meted out uniformly and evenly throughout the entire population. To wit: many laws that prohibited sodomy specifically included oral sex—if every person (hetero or otherwise) who has ever received or given a blowjob were under the same threat of prosecution and punishment, then a vast majority of the population would live in continual