EXHIBIT A-1

REDACTED - PUBLICLY FILED VERSION OF DOC. 151-1
PURSUANT TO COURT ORDER,
DATED MARCH 21, 2023 (DOC. 178)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAT BROOKS and RASHEED SHABAZZ, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

THOMSON REUTERS CORPORATION,

Defendant.

Case No. 3:21-cv-01418-EMC

EXPERT REPORT OF PROF. JANE BAMBAUER

Judge: Hon. Edward M. Chen

TABLE OF CONTENTS

Page

I. Qualifications 4

a. Background and Experience 4

b. Publications 4

c. Prior Expert Witness Work 6

d. Compensation 6

II. Scope of the Report 6

III. Summary of Opinions 6

IV. Privacy Does Not Require Absolute Control 6

a. Prof. Turow's Suggestion that Unconsented Collection and Use of Data Is Always a Violation of Privacy Is an Extreme and Untenable Position 7

b. Privacy Principles Take Context and Social Necessities Into Account 8

c. Privacy Theories and Laws Recognize Some *Per Se* Legitimate Data Practices, Some *Per Se Illegitimate* Data Practices, and Many Practices That Are Ambiguous and Context-Dependent 10

d. Factors to Consider in Context-Dependent Privacy Assessments 12

e. A Responsible Data Steward Can Avoid Creating Privacy Harm, Even if Individuals Do Not Have Full Control Over their Data, by Securing Data and Limiting Its Access and Use 15

V. The Limited Set of Permissible Uses that CLEAR Allows Create Benefits, not Harm, for Californians 16

a. For the Direct Benefit of the Data Subject 17

i. Use by a Person Holding a Legal or Beneficial Interest Relating to the Consumer 17

ii. Administering a Transaction that a Consumer Requests or Authorizes 18

b. For the Protection of Others (and Often for the Indirect Benefit of the Data Subject) 18

i. Complying with Legal Requirements and Legal Process 19

ii. Protecting Against or Preventing Fraud 20

iii. Use by a Law Enforcement Agency on a Matter Related to Public Safety....21

iv. Resolving a Consumer Dispute or Managing Institutional Risk....22

c. The Individual and Collective Benefits for Californians Are Highly Dependent on the Particulars of the Data Subject, the Purpose of the Search, and the Quality of the Data Relative to Other Available Options....23

d. Analysis of Benefits and Harms to the Named Plaintiffs....27

VI. CLEAR Has Strong Protections Against Risks of Misuse or Mistaken Associations....28

a. CLEAR Minimizes the Risk of Misuse Using Credentialing, Training, User Interface Design, Query Logs, and Audits....29

b. CLEAR Minimizes the Risk of Overcollection and Mistaken Associations Using Data Quality Procedures, User Interface Design, and Training....31

VII. Conclusion....33

I. Qualifications

a. Background and Experience

I am the Dorothy H. and Lewis Rosenstiel Distinguished Professor of Law at the University of Arizona College of Law. I am the director of the QuantLaw program (using quantitative methods to study the effects of laws) and the co-director of the TechLaw Program at the College of Law. I am also the co-deputy director of the Center for Quantum Networks, a multi-institutional engineering research center funded by the National Science Foundation, where I facilitate research across the country on the economic and regulatory implications of emerging quantum communications technologies.

My research focuses on the social costs and benefits of Big Data and how new information technologies affect privacy, free speech, and competitive markets. I am particularly interested in the ways that new technologies can upend longstanding assumptions and intuitions about privacy, discrimination, and governance. To advance the privacy discourse, I synthesize existing experimental, statistical, and theoretical research about the real-world impact of privacy laws or Big Data practices so that policy discussions can be grounded in empirical facts rather than speculation. I have also conducted my own empirical research on consumer preferences and attitudes related to the collection, disclosure, or repurposing of personal data. Because of my understanding and experience with data-driven research, I can apply insights from the highly technical literature produced by economists and computer scientists to the discussion of privacy, constitutional law, and public policy.

I have served as the Reporter for the Uniform Law Commission's model data privacy act (the Uniform Personal Data Protection Act), as the Director of George Mason's Program on Economics & Privacy, and as a Board Member of the TPRC Conference on Communications, Information, and Internet Policy. I am on the program committee for UNESCO's Privacy in Statistical Databases conference and journal. I have testified before the Senate Judiciary Committee on the impact of the GDPR and CCPA on competition and consumer welfare, and I have testified twice before the Federal Trade Commission on topics related to privacy. My privacy-related work has been quoted in the Wall Street Journal, the Boston Globe, the Washington Post, the New York Times, the L.A. Times, TIME, TechDirt, and Sports Illustrated. I am also the co-founder and executive editor of the Journal of Free Speech Law, the first peer-reviewed law journal on the topic of free speech. I teach courses on Information Privacy, Torts (including Advanced Torts, which covers the privacy torts), Criminal Procedure, Free Speech, and a seminar on the social consequences of the Internet. I hold a B.S. in mathematics and a J.D. from Yale.

b. Publications

My privacy- and Big Data-related work spans from highly technical papers discussing new methods for anonymizing data and measuring reidentification risk to more broad-ranging pieces related to the impact of new technologies on Fourth Amendment theory. My research has appeared in peer-reviewed journals, top law reviews, and mainstream media. I include here a selection of work. My complete resume is attached as **Exhibit A**.

Articles

Reckless Associations, 36 HARVARD JOURNAL OF LAW & TECHNOLOGY __ (forthcoming 2023) (with Saura Masconale and Simone Sepe)

Plausible Deniability, 2020 PRIVACY IN STATISTICAL DATABASES 91 (2020) (peer-reviewed) (co-authored with David Sidi).

The Algorithm Game, 94 NOTRE DAME L. REV. 1 (2018) (with Tal Zarsky).

Other People's Papers, 94 TEXAS LAW REVIEW 205 (2015).

Is Data Speech?, 66 STANFORD LAW REVIEW 57 (2014).

The New Intrusion, 88 NOTRE DAME LAW REVIEW 205 (2012).

Tragedy of the Data Commons, 25 HARVARD JOURNAL OF LAW & TECHNOLOGY 1 (2011) (published as Jane Yakowitz).

Books

BUBLICK, BAMBAUER & ARELLANO, DOBBS ADVANCED TORTS: ECONOMIC AND DIGNITARY TORTS (2d Ed.) (2022).

Book Chapters

Sober and Self-Guided Newsgathering, invited chapter in MEDIA AS A GOVERNANCE INSTITUTION (Gus Hurwitz et al., eds., Cambridge University Press, forthcoming 2023).

Conceptions of Fairness in Artificial Intelligence, invited chapter in THE PHILOSOPHICAL FOUNDATIONS OF IT LAW (David Mangan, ed., Oxford University Press, forthcoming 2022).

Privacy Versus Research in Big Data, in THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Evan Selinger et al., eds., Cambridge University Press, 2018).

Essays and Letters

Reinventing Cambridge Analytica One Good Intention at a Time, LAWFARE (2022).

Facial Recognition as a Least Bad Option, HOOVER INSTITUTE REPORT (2021).

COVID Apps Are Terrible. They Didn't Have to Be. LAWFARE REPORT (2020) (with Brian Ray).

Are Privacy Disclosures Informational or Ideological?, 65 DEPAUL L. REV. 503 (2017) (Clifford symposium issue).

Assessing Data Intrusion Threats, SCIENCE (letter) (with D. Barth-Jones et al.) (2015) (peer-reviewed).

How the War on Drugs Distorts Privacy Law, 64 STAN. L. REV. ONLINE 131 (2012).

Op-Eds

Bills Meant to Check Big Tech's Power Could Lead to More Disinformation, WASHINGTON POST (June 6, 2022) (with Anupam Chander).

Letting Police Access Google Location Data Can Help Solve Crimes, WASHINGTON POST (March 28, 2022).

c. Prior Expert Witness Work

I have served as an expert witness in one other case—*Sander v. Regents of the University of California,* in support of plaintiffs seeking public records.

d. Compensation

My hourly rate is $700. My compensation does not depend in any way on the substance of my opinion or the outcome of this matter.

II. Scope of the Report

I understand that plaintiffs in this case seek class certification in their lawsuit against Thomson Reuters stemming from its CLEAR platform. I have been retained to become familiar with the CLEAR platform—how it works, what purposes it is used for, and what precautions it takes against unauthorized access or use—and to assess the analysis and conclusions of plaintiffs' expert, Professor Joseph Turow. I have limited my report to an analysis, critique, and response to Prof. Turow's opinions as set forth in his report dated June 1, 2022 ("Turow Report") and deposition testimony. In order to fully respond to the Turow Report, I have provided a methodology to assess privacy harms as a corrective to the methodology that the Turow Report and Prof. Turow's testimony puts forward.

In authoring this report, I considered the documents listed throughout the report and in **Exhibit B**. The opinions contained in my report are based on the information and documents available to me as of the date of this report. If additional information or documents become available, I reserve the right to modify or supplement the opinions expressed in this report based on that newly available information.

III. Summary of Opinions

The Turow Report wrongly insists that any unconsented collection, disclosure, or use of personal data constitutes a privacy harm. Prof. Turow's conception of privacy harm as any loss of control, no matter how trivial, and no matter how beneficial the data practice may be to the data subject or others, is much too rigid and is well outside the bounds of scholarly consensus. In part because of his absolutist definition of privacy, the Turow Report fails to account for socially valuable and desirable uses of data (even without data subjects' consent) and therefore cannot illuminate a means of reconciling privacy with competing individual and collective interests. When the particular uses of the CLEAR platform are analyzed, it becomes obvious that Prof. Turow's conclusions that CLEAR is harmful to Californians—and is harmful to all Californians in exactly the same way and to the same degree—is detached from any context or real-world consequences. My report provides a corrective by taking into account the specific uses for which the CLEAR platform is allowed to be accessed, the safeguards by which Thomson Reuters prevents and detects misuse, and the highly variable and fact-dependent nature of the impact of CLEAR on each individual California resident.

IV. Privacy Does Not Require Absolute Control

The Turow Report wrongly claims that every unconsented collection or use of personal information is a privacy injury. In his opinion, the only question that needs to be answered in this case in order to understand the extent of privacy harm is whether CLEAR interferes with a data subject's control of their data. (Turow Report at 13). This is not correct; while consent and data subject control have a major influence over whether privacy has been respected, avoiding privacy harms has never required absolute control to be vested in the data subject. To the contrary, scholars and lawmakers

have understood that the broader social contract requires individuals' interest in controlling information about them to be balanced against, and sometimes overcome by, other interests and needs.

a. Prof. Turow's Suggestion that Unconsented Collection and Use of Data Is Always a Violation of Privacy Is an Extreme and Untenable Position

Prof. Turow concludes that Californians suffer harm because "no Californian has control over the information in or use of dossiers about them" (Turow Report at 13). According to Prof. Turow, the only legitimate test for determining whether privacy has been respected is whether a person has consented. (Turow Report at 14).

Regarding data access or collection, the Turow Report claims that compiling and cross-referencing data is automatically a violation of privacy irrespective of the source of the data, how the data is used, or what precautions are in place to prevent abuse:

> CLEAR's very business model is to allow companies to take for granted that huge numbers of datapoints about Californians are compiled, connected, updated (including, for certain data, in real-time) and made available for Thomson Reuters' customers at the touch of a button. . . Before the internet era, melding information from even public databases was a cumbersome process, and so the material a company could bring together about a particular individual was limited." (Turow Report at 17).

Prof. Turow concludes that any collection and organization of data, even publicly available data, "deprives all Californians of the right to control their personal data" (*Id.*).[1]

With respect to how data is used, the Turow Report claims that a service allowing personal information to be accessed for *any* reason would violate privacy unless the target of the search has provided consent.

> [W]hether a person has consented to the sale of their data has nothing to do with whether Thomson Reuters lists the use as permissible. And so, whatever the function of a customer certifying a purportedly permissible use, it does nothing to solve the privacy harms of lack of control or violation of the right to be let alone. No Californian is given any control over the uses of dossiers about them. There is no use of CLEAR profiles that is permitted *by the Californians* whose information is sold via CLEAR.
>
> Turow Report at 14.

Prof. Turow has described actual uses of CLEAR as "hypotheticals" that "get away from the main point" of his report's conclusion that unconsented collection of data is a "first order" harm that overrides all other considerations. (Turow Dep. 269-70). The Turow Report did not consider the social benefits that can come from specific collection, disclosure, and uses of data for limited purposes—like the detection of fraud or the provision of government benefits.

[1] The Turow Report also suggests that CLEAR automatically violates privacy and causes harm because Thomson Reuters is not actively engaging in a public awareness campaign and encouraging individuals to opt out or change their data. (Turow Report at 15-16). But this, too, is an overstatement of what privacy principles would require. The principle of notice is typically satisfied by providing a privacy policy on a website. Information about CLEAR is available for the privacy-concerned who seek it out. Moreover, the purpose of a data system would be undermined if, for example, would-be money-launderers were alerted and permitted to opt out of a database used for Know Your Customer due diligence, eviscerating the benefits outlined below in Part V.

This is an extreme position. Prof. Turow is correct in a general sense. Privacy theory and law has long incorporated an interest and limited right for a data subject to control information about themselves. For example, the document known as the "HEW Report" promulgated a set of "Fair Information Practice Principles" or "FIPPs" that have been tremendously influential to modern privacy law.[2] These principles include many of the themes Prof. Turow emphasizes, such as notice, consent, and a constraint on repurposing data.

However, Prof. Turow's definition of privacy (and of privacy harm) is much too broad and rigid. His capacious conception of privacy harm would render the Google search bar harmful since Google search allows scattered pieces of information to be drawn together quickly and cheaply. (Turow Dep. 198; 206-210; and 326-27 (claiming that even collecting articles that a named plaintiff published in news media or collecting information contained in public county records would be a privacy harm if done without the data subject's permission)). And by his logic, the GDPR, FCRA, HIPAA, the Wiretap Act, and every other federal privacy law cause (or at least fail to prevent) privacy harms because they permit many disclosures and uses of personal data without consent. Indeed, even the warrant process prescribed in the Fourth Amendment is inadequate since the subject of a warrant has not consented to the search that has been judicially authorized.

b. Privacy Principles Take Context and Social Necessities Into Account

The Turow Report is out of sync with generally-accepted theoretical, academic, and historical frameworks for understanding privacy violations and harms because the report admits of no exceptions to his claim that privacy requires data subject control. Nearly every privacy scholar understands that privacy ensures a personal sphere that is shielded, but not absolutely closed off, from the uses and needs of others.[3] The right of a data subject to control information has always been understood as a limited one, where a person's interest in control must be reconciled with, and sometimes superseded by, other needs of society. These include physical and financial security, the right of a free press, and compliance with a wide range of legal and ethical duties. Scholars debate how widely or narrowly to define the scope of control, but have rarely, if ever, advocated for an absolutist approach to privacy.

For example, the authors of the HEW Report, which articulated the "Fair Information Practice Principles" that have informed every modern data privacy statute, explicitly rejected formulations of privacy that required the absolute control of the data subject.[4] As it explained, "it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his record."[5] Indeed, every law that has used the FIPPs as their backbone has included exceptions in which data collection, access, disclosure, or use can occur without the data subject's consent. The Privacy Act (which governs how the federal government manages its own collections of personal data) includes exceptions for criminal law enforcement, the investigation of tax and social security fraud, for purposes of "compelling circumstances affecting the health or safety of an individual", and for "routine uses"

[2] U.S. DEPT. HEALTH, EDUCATION & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973); Robert Gellman, *Fair Information Practices: A Basic History,* (describing the numerous statutory and regulatory laws that have used the FIPPs as a basic structure) (hereinafter "HEW Report").
[3] *See* sources cited *infra* notes 5-15.
[4] The HEW Report favored the concept of "mutuality" instead. HEW Report, *supra* note 2 at 3, 40.
[5] *Id.*

without getting the data subject's consent.[6] Many other US[7] and EU[8] laws similarly describe scenarios in which data can be collected or used without the data subject's consent. All of these laws follow the very widely held conceptual framework that the data subject's control over information must yield to other interests in at least some circumstances in order to ensure that privacy rights do not lead to absurd and harmful results.

Likewise, leading privacy law scholars including Alan Westin[9], Daniel Solove[10], Helen Nissenbaum[11], and Neil Richards[12] have recognized that information control is not always in the best interest of society or of the data subjects themselves, and privacy does not and should not require consent in every single conceivable case.[13] Prof. Turow cites Alan Westin repeatedly for the proposition that privacy loss automatically occurs when people lose control over their data (Turow Report at 7; Turow Dep. 28, 117), but Westin himself described control as a "central" but not *essential* factor.[14] He went on to explain that "the needs of social order may require certain levels of exposure and confession even if these are involuntary. Consent is thus to be analyzed in the specific context of the purpose of [data collection] and the use to be made of the information so obtained."[15] Prof. Turow, too, in his deposition testimony, acknowledged that the loss of control over one's information is a privacy harm "in particular contexts" and provided an example—disclosures made in the course of medical treatment, or disclosures made in order to comply with a legal requirement—in which losing control over personal data would *not* constitute a privacy harm. (Turow Dep. 101-102; 203-204).

It is telling that Prof. Turow and the named plaintiffs could not explain why people and companies are allowed to collect or use individuals' names without consent without undermining their theories that loss of control over personal information always constitutes a privacy harm In response to the question "Does the right to control one's information, that is the subject of your report in this case, extend to an individual's right to prevent a company like a court reporting company from repeating their name?" Turow replied "It's a bad question." (Turow Dep. 202). Pressed further, he explained that he would have to know:

---

[6] 5 U.S.C. § 552a.

[7] The Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g); and the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523 (2006).

[8] Europe's General Data Protection Regulation ("GDPR") allows data to be processed without consent in order to comply with legal obligations, prevent fraud, to ensure network security, and to detect possible threats to public safety. GDPR, OJ L 119, 04.05.2016, Art. 6 (2018).

[9] ALAN WESTIN, PRIVACY AND FREEDOM 418, 431-34 (1967).

[10] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1880 (2013) ("in order to advance, privacy law and policy must face the problems with privacy self-management and start forging a new direction.")

[11] HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010).

[12] NEIL RICHARDS, WHY PRIVACY MATTERS 71 (2022) ("my own definition [of privacy] excludes other ways we could talk about privacy, such as its being a right to control our personal information or to conceal disreputable information about ourselves.")

[13] Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy,* 137 J. BUS. ETHICS 551 (2016) ("Defining privacy as a state of inaccessibility is neither practical nor desirable and, ironically, renders privacy as a form of punishment. . . These social contracts around what, to whom, and for what purposes information flows are the governing rules about privacy for a given community."); Timnit Gebru et al., *Datasheets for Datasets,* MICROSOFT (2018) (encouraging database creators to ask the question "Did the individuals in question consent to the collection and use of their data?" but not requiring the answer to determine, on its own, the privacy assessment of a program).

[14] ALAN WESTIN, PRIVACY AND FREEDOM 418 (1967) ("A central aspect of privacy is that individuals and organizations determine for themselves which matters they want to keep private and which they are willing—or need—to reveal.")

[15] *Id.*; *see also id.* at 431-434 (describing exceptions to the general rule that government agencies should not share data it has collected without consent).

> [W]hy would they be doing this? Is it a legal requirement? Under what conditions? Where are the—where is the material located? Who has access to it? What can it be used for?

(Turow Dep. 203-204).

Again, this is in response to whether a company can use a person's name. When Plaintiff Cat Brooks was asked whether she has the right to control the use of her name, she responded "that's an absurd question" and "it would depend on how my name was being used in conjunction with other information." (Brooks Dep. 70).

c. Privacy Theories and Laws Recognize Some *Per Se* Legitimate Data Practices, Some *Per Se Illegitimate* Data Practices, and Many Practices That Are Ambiguous and Context-Dependent

In truth, there is no simple way to reconcile the fact that privacy principles give individuals some degree of control over their information with the fact that other private and public interests can and should override this control in some circumstances. The concept of "mutuality" from the HEW Report is the most honest and enduring account of privacy, despite its imprecision, because it treats privacy as part of a social contract—as part of a set of trade-offs and cooperation that people must engage in with each other, with industry, and with the government.[16] Prof. Turow's surveys finding that Americans are concerned about the collection and use of their personal information does not negate this inescapable trade-off. (Turow Report at 3). While it may very well be that most people prefer, in general, and all else being equal, to have control over their data, these abstract preferences say little about where legal rights and obligations should be drawn in real world contexts where personal interests in privacy may come into conflict with other pressing personal and public interests.

The HEW Report explains that a respect for privacy requires data collectors to anticipate and behave responsibly when conflicts arise between their interests and those of the data subjects. Some data uses are in the mutual interests of the controllers and the data subjects, some are in their mutual interests but are "not perceived as such," and some are in direct conflict.[17] This observation was ahead of its time and explains why privacy rules are so difficult to articulate in advance. The interests of all stakeholders sometimes run together and sometimes against each other, and a wide range of contextual factors determine whether the data subject's express consent is necessary to maintain privacy. Data subjects do not want or expect to have absolute control over their data in all circumstances.[18] And privacy should not be regarded as a rigid "procedural mechanism divorced from the particularities" of a data practice.[19]

For clarity of discussion, data practices can be organized into three categories: (1) practices that are per se privacy violations; (2) practices that are clearly warranted by public needs and the social

---

[16] The work of Helen Nissenbaum and Kirsten Martin have helped add definition to the idea of privacy as an intricate social contract where consent is just one possible route (neither necessary nor automatically sufficient) to achieving privacy. Kirsten E. Marin, *Understanding Privacy Online,* 137 J. BUS. ETHICS 551 (2016) (hereinafter "Understanding Privacy Online"); Kirsten E. Martin, *Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract,* 11 J. BUS. ETHICS 519 (2012); Helen Nissenbaum, *Privacy as Contextual Integrity,* 79 WASH. L. REV. 119 (2004); HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010); Mary J. Culnan & Robert J. Bies, *Consumer Privacy: Balancing Economic and Justice Considerations,* 59 J. SOCIAL ISSUES 323 (2003); J. (Hans) Van Oosterhout et al., *The Internal Morality of Contracting: Advancing the Contractualist Endeavor in Business Ethics,* 31 ACADEMY OF MAGMT. REV. 521 (2006).

[17] HEW Report, *supra* note 2 at 46.

[18] Martin, Understanding Privacy Online, *supra* note 13 at 555 "Allowing privacy rules to vary based on the community or relationship mirrors expectations of privacy in the world."

[19] Helen Nissenbaum, *A Contextual Approach to Privacy Online,* DAEDALUS, THE JOURNAL OF THE AMERICAN ACADEMY OF ARTS & SCIENCES 32, 35 (2011).

contract (per se non-violations); and (3) the messy middle category, where the threat to reasonable expectations in privacy will depend on controls and procedures that are in place, the sensitivity of the data, and the costs and benefits of the practice.

1. *Per se violations.* Per se privacy violations involve observations, disclosures, or uses of data that are nearly universally unwanted and disturbing and are also unnecessary for the welfare of the data subject or the community. Examples of per se privacy violations include intrusive observations or recordings of private spaces and conversations (e.g. upskirt photography or wiretapping phone lines)[20]; indiscriminate data disclosure or completely unconstrained data reuse[21]; or a clearly harmful use (e.g. using personal data to create "sucker lists" of individuals who are especially vulnerable to fraud or manipulation).[22]

2. *Per se non-violations.* Examples of well-justified data practices (per se non-violations) include the exceptions that are common in privacy statutes. These include disclosures or analyses that are required by law; data practices that address a serious public health or safety risk; practices done for the purpose of benefiting the data subject in a context where consent is impracticable; practices that are necessary for detecting fraud; and practices that are necessary for executing a transaction or the terms of an agreement that the data subject sought out.[23] In all of these cases, even if there is not universal agreement, most would agree in advance to be part of a system that allowed these trade-offs between a data subject's control over personal information and the benefits to third parties or even to themselves that can occur if data is accessed without their control.[24]

3. *Context-Dependent Privacy Violations.* Between the per-se violations and per-se non-violations is a vast middle category where a wide range of factors will have to be considered in order to determine whether a particular practice, carried out in its real-world context, will cause a privacy injury. These include the sorts of data practices that Prof. Turow describe as "lawful and common" that also diminish a person's ability to control their information, such as online tracking for the purposes of behavioral advertising. (Turow Dep. 80-82 (discussing his own NY Times op-ed)).

For practices in this middle category, which I will refer to as the "messy middle," a number of factors will be relevant to a privacy assessment, and in some cases reasonable minds will disagree on whether a data practice is appropriate. Still, most privacy experts would home in on a few factors that cut either for or against the recognition of a privacy harm. Relevant factors include over-collection (recording more data than is likely to be useful for legitimate primary or secondary purposes), security and probability of misuse, the transparency of a system, the expectations and preferences of individual data subjects, the costs of obtaining consent (both financial costs and the costs to the utility of the data for the particular purpose), and the actual and perceived costs and benefits to the individual, to the data controller, to third parties, and to society. Identifying a privacy

[20] Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. Ct. App. 1970); The Wiretap Act, 18 U.S.C. §§2510-20; The Video Voyeurism Prevention Act, 18 U.S.C. §1801.

[21] Rest. (2d) of Torts §652D: Publicity Given to Private Life

[22] Maddy Varner & Aaron Sankin, *Sucker List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders*, THE MARKUP (February 25, 2020); Gema de las Heras, *Scammers Target Disaster Victims. Spot Their Traps,* FEDERAL TRADE COMMISSION (August 2, 2022).

[23] For example, a survey of privacy professionals conducted by the Ponemon Institute at Accenture found that most privacy professionals agree it is acceptable to use personal information to identify and authenticate customers, to share information with law enforcement, for fraud prevention, and for government and national security purposes. HOW GLOBAL ORGANIZATIONS APPROACH THE CHALLENGES OF PROTECTING PERSONAL DATA 23 (2009).

[24] Richard Re, *Fourth Amendment Fairness,* 116 MICH. L. REV. 1409 (2018) (proposing a contractualist approach to Fourth Amendment privacy).

violation requires consideration of the totality of these factors, and the hallmark of a violation is when the privacy risks cannot be justified by the benefits of a practice.[25]

d. Factors to Consider in Context-Dependent Privacy Assessments

When determining whether a practice violates generally accepted principles and expectations of privacy, the following factors will be relevant.

Actual and Perceived Benefits of a Data Practice: When it comes to the benefits of data use, privacy expectations and preferences often operate as a sliding scale: the more benefit the data subject derives from data use, the less invasive the practice. The economic literature on the "privacy paradox" provides a glimpse into the tradeoffs between privacy and benefits. The privacy paradox is the frequently replicated phenomenon where individuals report concern about their privacy but are also willing to give up control of their personal data for small payments or perks.[26]

While there are several theories that could explain the paradox, the most parsimonious explanation is that whatever respondents say about privacy in the abstract, their concerns about privacy are adjusted up or down depending on a large range of factors specific to each individual and each data practice.[27] The intrinsic or deontological value of privacy in real-world contexts is fairly low for most people, and so their context-specific concerns about a data practice can be outweighed by the context-specific benefits.[28] My own experimental research has found that most Americans primarily

---

[25] The FTC explains the sliding scale like this: "the level of transparency, access, and correction should be tied to the significance of the benefit or transaction in question." FEDERAL TRADE COMMISSION, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY ix (2014) (hereinafter "FTC Data Brokers Report").

[26] Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk,* NBER WORKING PAPER NO. 23488 (2017); Kai-Lung Hui et al., *The Value of Privacy Assurance: An Exploratory Field Experiment,* 31 MIS QUARTERLY 19 (2007); Jan H. Schumann et al., *Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance Among Users of Free Web Services,* 78 J. MARKETING 59 (2014). Consumers rarely alter the defaults in privacy settings (Adam S. Chilton & Omri Ben-Shahar, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. LEG. STUD. 41 (2016); Eric J. Johnson et all., *Defaults, Framing and Privacy: Why Opting In-Opting Out,* 13 MARKETING LETTERS 5 (2002)) and the drafting of privacy notices has almost no effect on behavior (Lior J. Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEG. STUD. 569 (2016); Adam S. Chilton & Omri Ben-Shahar, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. LEG. STUD. 41 (2016)). In my own work, I have found that privacy-related notices are often wasteful and do not change consumer choices. Dramatic just-in-time disclosures have the best potential to change behavior, but they also run the risk of exaggerating a sense of threat and distorting the consumer's evaluation of other criteria. Jane Bambauer et al., *A Bad Education,* 2017 IL. L. RE V. 109 (2017). Even when consumers are paying attention to privacy options, they rarely forego a service or benefit that they would otherwise want in order to protect their privacy. Lior J. Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEG. STUD. 569 (2016); Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk,* NBER WORKING PAPER NO. 23488 (2017); Alessandro Acquisti, *Privacy and Human Behavior in the Age of Information,* 347 SCIENCE 509 (2015) (providing a summary of related scholarship).

[27] Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables,* 18 COLUM. SCI. & TECH. L. J. 176 (2017). *See also* Kirsten Martin & Helen Nissenbaum, 31 HARV. J. L. & TECH. 111, 130-38 (2017) (describing some of the contextual factors that appear to matter when public data is disclosed to different entities).

[28] Long Chen et al., *The Data Privacy Paradox and Digital Demand,* NBER WORKING PAPER NO. 28854 (2021) (finding that individuals who have the greatest concern for privacy also get the greatest value from data-sharing); Culnan & Bies, *supra* note 16; Tamara Dinev & Paul Hart, *An Extended Privacy Calculus Model for E-Commerce Transactions,* 17 INFO. SYS. RESEARCH 61 (2006); Hui et al., *supra* note 26; Heng Xu et al., *The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services,* 26 J. MGMT. INFO. SYS. 135 (2009); Susanne Barth & Mennode Jong, *The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review,* 34 TELEMATICS AND INFORMATICS 1038 (2017); Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms,* 30 BUS. ETHICS QUART. 65, 72 (2019) (summarizing this literature) ("Uses of information

value privacy for its instrumental purposes—to avoid concrete risks to themselves and others—*and will therefore perceive less of a threat to privacy when the benefits of a data practice outweigh those risks.*[29]

Cat Brooks' deposition testimony illustrates the privacy paradox very well. On one hand, she states "I believe that any personal information about me that I do not disclose myself that is collected, stored, given, sold, whatever, to anybody else is an invasion of my privacy." (Brooks Dep. at 74-75). And yet, she also explains that if another person *does* redisclose information that they have learned about her, the question of whether a privacy invasion has occurred "depends on who they're parroting it to. …. And for—not just who, but for what purpose." (Brooks Dep. at 77-78). For example, her Wikipedia page, which collects information about her from multiple sources and discloses her birth name, would seem to violate the definition of privacy she offered in the abstract since she did not create the page herself. (Brooks Dep. at 96, 99-100). But she did not object to it and is ok with its existence. (Brooks Dep. at 96; 99-100). She also does not make use of her rights, as a Californian, to opt out of the sale of her data through any websites other than CLEAR even though this is a form of control she could exercise right now. (Brooks Dep. at 146; 84). Ultimately, Brooks recognized that her philosophy about her right to control her personal information "depends on the conditions around how that information is being repeated" and "if that information is repeated with the potential to impact my life or the peoples whose lives are associated with mine in a negative way." (Brooks Dep. at 121). In other words, even in Brooks' view, her right to control information depends on the consequences of subsequent data disclosures and uses. This is consistent with her explanation that she conducts cost-benefit analyses when deciding how much she will reveal about herself and in what context. (Brooks Dep. at 77; 120; 138).

The Turow Report makes no attempt to balance, or compare, the harm from lost control over personal data to the potential benefits either to the data subjects or to others. In deposition, Prof. Turow explained that while he understood a court will weigh the harm to Californians against the utility of a data practice, his report does not offer any opinion about the utility of the CLEAR product or how the magnitude of benefits compares to the magnitude of harms. (Turow Dep. 112). Prof. Turow did not offer an opinion about where the balance should be struck. (Turow Dep. 114-15). In Prof. Turow's opinion, "my mandate is to discuss the—the first order privacy harms, which override" any analysis of benefit. Thus, his working definition of privacy harm is incomplete, accounting for social losses alone without any accounting of social gains.

Person-Specific Privacy Preferences: Prof. Turow concludes that the CLEAR platform causes the exact same privacy harm to all Californians. (Turow Report at 13). However, not only does he fail to consider offsetting benefits, he does not explain why all Californians would be harmed in the same way and to the same degree. In fact, he specifically did not consider individual differences among class members: in deposition, he testified that he was *not* asked to evaluate the harm or objections that might apply at "the individual level." (Turow Dep. 148-150 ("The issue is not an individual class member. The issue is the larger class of Californians.")) But a complete evaluation of privacy harm must take into account differing levels of sensitivity and preferences (as well as differences in the impact of potential benefits). The risks and harm associated with a data practice is interpreted, at least to some degree, through an individual's experience of loss of dignity, loss of a sense of control, and upset expectations.[30] These will vary not only by data practice, but also by person. Some people

---

deemed privacy violations in consumer surveys may be better judged after taking into consideration the benefits of sharing information online.")

[29] Jane Bambauer, *Privacy Tradeoffs: Who Should Make Them, and How?,* working paper available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3905024; Jane Bambauer et al., *A Bad Education,* 2017 U. ILL. L. REV. 109 (2017).

[30] Daniel Solove, *A Taxonomy of Privacy,* 154 U. PENN. L. REV. 477, 507 (2006) describing the harms from data aggregation. Note that Solove also describes significant economic benefits as well and does not take a position on whether or when privacy harm occurs from aggregation and reuse.).

are much more privacy-sensitive than others[31], and even individuals who have the same average privacy sensibilities may still have different expectations and dignitary losses depending on who is accessing data or for what purpose.[32] The "messy middle" category includes data practices where some individuals are willing to relinquish control and others are not. For example, some consumers prefer to disclose information for the purpose of content personalization or to access free services while others do not.[33]

Actual and Perceived Benefits of Privacy Controls: Just as data practices in the middle category will be seen as beneficial to some and less so to others, the benefits of privacy controls are similarly mixed and individualized. While individuals who are privacy-sensitive will prefer having consent-based control over their information, others who are privacy pragmatists could see data subject control as a cost in some circumstances because it creates an imposition on them to manage requests and opt-ins for services that are, in their mind, clearly worth it.[34] Some individuals might perceive consent procedures as getting in the way of the usefulness of the data. For example, as I discuss in more detail below, data practices that are designed to detect fraud would be undermined if the target of an investigation had to be consulted in advance. Also, data practices that depend on a representative sample of data in order to accomplish their goals could suffer from selection bias if only some potential data subjects opt in.[35] Consent-based privacy controls can also frustrate competition policy goals because the companies that are in the best position to collect and manage consents and to combine a larger variety of types of data are the largest companies that already dominate their markets—Google and Facebook, for example.[36]

The experience in Europe shows that there are at least some disadvantages to consent-based privacy regimes. European privacy law (the General Data Protection Regulation, or "GDPR") caused investment in research and development for new technology startups in the EU to falter, and productivity of EU firms fell as compared to US counterparts.[37] Meanwhile, the internal budgets for privacy offices at companies of all sizes (including in the U.S.) increased 29%.[38] Costs to American companies if they have to comply with GDPR-style laws are estimated to be approximately $480 per

[31] Alan Westin found that a sizable subset of individuals were privacy-unconcerned, some were pragmatists (willing to trade privacy for benefits), and some were privacy sensitive. Alan F. Westin, *Social and Political Dimensions of Privacy,* 59 J. SOCIAL ISSUES 431, 445 (2003) (describing survey work conducted in the 1990s).

[32] The same person also has different privacy preferences over time. Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns,* 102 AM. ECON. REV. 349 (2012).

[33] Xu et al., *supra* note 28; Syagnik (Sy) Banerjee & Ruby Roy Dholakia, *Mobile Advertising: Does Location Based Advertising Work?,* 3 INT. J. MOBILE MARKETING 68 (2008).

[34] Outside Facebook, where sustained attention and criticism has caused a greater proportion of users to change their privacy settings (Andrew Perrin, *Americans Are Changing Their Relationship with Facebook,* PEW RESEARCH CENTER (2018), available at http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/), the great majority of consumers do not bother to change default settings related to their privacy. This is true even in Europe, where only 12.5% of Europeans opt out of data collection despite the very prominent and easy-to-use pop-up windows providing the opportunity to do so. Guy Aridor et al., *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR,* NBER WORKING PAPER NO. 26900 (2021).

[35] Jane Yakowitz Bambauer, *Tragedy of the Data Commons,* 25 HARV. J. L. & TECH. 1, 61, 64 (2011) (published as Jane Yakowitz).

[36] James Campbell et al., *Privacy Regulation and Market Structure,* 24 J. ECON. & MGMT STRATEGY 47 (2015); Garrett Johnson et al., *Privacy and Market Concentration: Intended & Unintended Consequences of the GDPR* (2022) (draft available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686); Christian Peukert et al., *European Privacy Law and Global Markets for Data* (2020) (draft available at https://doi.org/10.3929/ethz-b-000406601); Jian Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment,* NBER WORKING PAPER NO. 25248 (2018); Ran Zhuo et al., *The Impact of the General Data Protection Regulation on Internet Interconnection,* NBER WORKING PAPER NO. 26481 (2020).

[37] Jia, *supra* note 36; EUROPEAN COMMISSION, 2021 DIGITAL ECONOMY AND SOCIETY INDEX (DESI) 6, 9 (2021).

[38] *IAPP-EY Annual Privacy Governance Report 2021*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP) (2021).

data subject.[39] These costs cause the prices that consumers pay to rise—a cost that may well be worth it to some people and in some contexts, but not to *every* person in every context. Thus, even in the middle category where the benefits and risks of a data practice are mixed and subject to differences of opinion, Prof. Turow is wrong to suggest consumer consent is a panacea to modern data stewardship puzzles.

All of the foregoing factors must be kept in perspective when determining whether a privacy violation has occurred with respect to practices in the middle category. In the middle category of data practices, reasonable minds will disagree and analysis of privacy is more complex and context-dependent.

e. A Responsible Data Steward Can Avoid Creating Privacy Harm, Even if Individuals Do Not Have Full Control Over their Data, by Securing Data and Limiting Its Access and Use

A company can avoid causing privacy invasions entirely if it collects or uses data only for a limited set of clearly beneficial purposes (*per se non-violations*) and if it maintains the data with adequate security and care.

Most garden variety data aggregators operate in the "messy middle" category and thus raise challenging questions for courts and lawmakers. Garden variety data aggregators are those companies that collect and sell personal data for a wide range of marketing purposes including targeted advertising, customer lists, market research, and to sell people search services to the general public.[40] CLEAR is *not* a garden variety data aggregator. It is a search tool that is accessible only for a narrow set of socially valuable risk mitigation purposes.[41] CLEAR is designed and managed in a manner that stays within the bounds of per-se non-violations of privacy because the uses it permits confer substantial benefits on data subjects individually and collectively without creating meaningful new risks.

Prof. Turow has taken an extreme position, claiming that *any* loss of any aspect of control over personal data is a privacy harm. According to Prof. Turow, the collection of publicly available information, without affording the data subject the opportunity to control it, would be a privacy harm even if the data is never subsequently used or disclosed. (Turow Dep. 163-168).

Prof. Turow may be taking this absolutist position on consent and control because he has conflated the CLEAR platform with hypothetical services that might collect every possible piece of information about individuals and sell access to "dossiers" for unlimited use. Prof. Turow claims the "breadth of information available in CLEAR, and the variety of uses for which Thomson Reuters permits business and governmental entities to access information through CLEAR, cover many aspects of Californian's lives." (Turow Report at 13). He states that "CLEAR [] provides customers the ability to coalesce large numbers of data points about individuals quickly and seamlessly" (Turow at *10) without acknowledging the strict limitations on use that are imposed. (*See also* Turow Dep. 204 (claiming that CLEAR uses data "willy nilly"). Prof. Turow draws parallels between this case and

[39] Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (ITIF) (2019).

[40] FTC DATA BROKERS REPORT, *supra* note 25 at ii-iii (describing marketing products and people search products and differentiating them from risk mitigation products).

[41] Federal Trade Commission does not consider risk mitigation data services to be engaged in an unfair business practice or to pose harm to consumers. *Id.* at iii, vii-ix. Because these types of data services are used to verify the identity or location of a data subject during a moment of vulnerability, or to assess the risk that the data subject is committing fraud or criminal activity, the FTC has all but endorsed these data products and have called for no legal intervention into their business models or practices.

his critiques of the digital behavioral advertising industry.[42] Indeed, in his deposition testimony, he describes Thomson Reuters' CLEAR platform as an example of "a company that is selling *audiences* to other companies." (Turow Dep. 51 (emphasis added); *see also* Turow Dep. 215 (equating the use of CLEAR to "a marketing context")). But CLEAR does not allow its service to be used to construct and buy audiences.

To summarize, Prof. Turow asserts that any collection or use of personal data that is done without the data subject's consent and control is a violation of privacy and causes privacy harm. This is not correct. For some highly beneficial or socially valuable purposes, data can be collected and used without consent without conflicting with any reasonable notions of privacy. And there are also some data practices that will either offend or conform to reasonable notions of privacy depending on context.

As the next Parts explain, the CLEAR platform is available only for a limited set of uses that are socially valuable and do not offend contextualized notions of privacy, and Thomson Reuters incorporates many protocols to prevent and detect misuse of the platform.

V. The Limited Set of Permissible Uses that CLEAR Allows Create Benefits, not Harm, for Californians

Prof. Turow claims that "every Californian whose information is accessible through CLEAR has suffered the same fundamental privacy harm of a lack of control and violation of their right to be let alone." (Turow Report at 13).[43] Because the Turow Report uses such an extreme definition of privacy harm, where every unconsented collection or use is automatically harmful, his report does not make clear how some of the other factors he highlights—the volume of data (Turow Report at 10), the "variety" of permitted uses (Turow Report at 13), or the lack of notice to data subjects (Turow Report at 15)—relate to his ultimate conclusion that Californians are harmed. As a result, it is not clear what type of carefully designed and thoughtfully managed data service would satisfy Prof. Turow's tests. It is not clear, in other words, that there is any possible version of CLEAR that could exist that Prof. Turow would recognize as harmless or even beneficial to Californians. Even a version of CLEAR that is restricted only to the most urgent purposes—locating an abducted child, for example—would cause harm to every person whose data is made theoretically accessible without their consent by Prof. Turow's vision for privacy. (Turow Dep. 274-77).

Thomson Reuters allows the CLEAR platform only to be used for nine permissible uses, which are the same nine permissible uses under the Gramm-Leach-Bliley Act. (TR-BROOKS013537;

---

[42] JOSEPH TUROW, THE VOICE CATCHERS: HOW MARKETERS LISTEN IN TO EXPLOIT YOUR FEELINGS, YOUR PRIVACY, AND YOUR WALLET (2021); JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER (2017); JOSEPH TUROW, NICHE ENVY: MARKETING DISCRIMINATION IN THE DIGITAL AGE (2006).

[43] He also argues that the CLEAR service causes economic harm because it misappropriates data subjects' own opportunity to sell information about themselves. (Turow Report at 5-6; Turow Dep. 227 "someone would get a different valuation on their data than would otherwise be the case; or might sell it to another organization that would try to get a different price and couldn't because of Thomson Reuters."). This is not correct. There is very little economic incentive for individuals to gather and manage their own databases about themselves and to overcome the myriad transaction costs that would be required for companies to contract for access to that data with each and every data subject. These would be a classic example of insurmountable transaction costs. Ronald H. Coase, *The Problem of Social Costs,* 3 J. LAW & ECON. 1 (1960) (explaining the concept of transaction costs). In theory, a company could offer money to data subjects in order to collect and aggregate data for future sale and re-use, but this is essentially what Google, Facebook, and other companies already do, using free services rather than cash payments, and Turow has criticized this business model.

Response to Interrogatories Attachment A (hereinafter ("Attachment A") at *2).[44] None of the opinion surveys that Prof. Turow conducted or relied upon asked survey respondents to react to a service that was similar to CLEAR (Turow Dep. 71 ("Not – not similar to CLEAR, no")), and so an analysis must rely on other resources and general knowledge in order to determine whether the CLEAR product is consistent with a social contract that most Californians would want given full information about risks and benefits.

One of the permissible uses is with the explicit consent of the data subject. Another is the functional equivalent, when a fiduciary or representative of the data subject has authorized the search. (Attachment A at *3). Since the Turow Report suggests these would be a legitimate (indeed, the *only* legitimate) use of personal data since they are uses under the control of the data subject or their representative, I will not analyze these and will focus on the other seven.

Each of the permitted purposes, separately and together, serves a compelling market or public welfare need and can therefore justify the use of personal information without the explicit consent of the data subjects. Thus, CLEAR limits its service to the *per se non-privacy-violation* category of data practices. Some permitted uses involve practices that directly benefit the data subject in a context where it would be impractical or impossible to get the data subject's consent. Others involve practices that are designed to directly protect the interests of somebody other than the data subject (e.g. the CLEAR client or third parties), but even in these instances, the data subject often benefits indirectly.

a. For the Direct Benefit of the Data Subject

When a wallet is returned to its owner, for example, the typical owner will not resent the good Samaritan who looked inside the wallet for the purpose of finding the identity and address of the owner. Similarly, some uses of the CLEAR platform are performed for the direct assistance and benefit of the data subject.

i. Use by a Person Holding a Legal or Beneficial Interest Relating to the Consumer

The first category of permitted use involves instances where CLEAR is used to find data subjects for their benefit or the benefit of their family member(s).

Some of the uses that fall into this category are high stakes, as when law enforcement or social services use CLEAR to locate individuals suffering from mental illness or displaced children (TR-BROOKS00746, 01564). Social services have used CLEAR to identify and locate extended family members in order to keep children out of the foster care system. (Attachment A at *4; TR-BROOKS00766)

Others are purely financial, as when social services agencies use CLEAR to find parents or custodial caretakers who haven't kept up their address with child support offices so that money can be routed to them. (TR-BROOKS01996). CLEAR was also used to find correct addresses for 60 million Medicare and Medicaid recipients who needed new medical ID cards. (TR-BROOKS02053; TR-BROOKS14319). This is not a trivial matter as the Social Security Administration master file was known to have inaccuracies in 25-30% of the records. (TR-BROOKS14319). There is no single good source of address information. For example, one in eight voter registrations are inaccurate.[45]

[44] Moreover, some of the data will not be retrieved unless users attest that in addition to using the system for one of the permissible uses, they also satisfy additional prerequisites. For example, voter registration data will not be available unless the user verifies that they are using it for an election-related or non-commercial purpose. (Attachment A at *3; TR-BROOKS013538).

[45] PEW: ONE IN EIGHT VOTER REGISTRATIONS INACCURATE; 51 MILLION CITIZENS UNREGISTERED (2012).

The best way to ensure that an important notice and mailing gets to as many intended recipients as possible is to cross-reference several sources of information, which is of course what CLEAR does well. Indeed, the Center for Medicare, Medicaid Services (CMS) selected Thomson Reuters for the contract because in a pilot test, CLEAR was able to find and confirm the right address on a list of 5,000 names and SSNs better than other similar services. (TR-BROOKS148319).

To use a highly relevant hypothetical, how would counsel in a class action case ensure that they have taken reasonable steps to provide notice of a settlement or judgment to all members of the class? Finding up-to-date address information is difficult and costly, and a service like CLEAR is a practical necessity for the proper function of consumer protection and class action work. (Attachment A at *5).

This category alone illustrates why privacy is not exclusively concerned with the consent and control of the data subject; there are cases where the use of data is unambiguously in the best interest of the data subject, but receiving consent is impractical or impossible.

Prof. Turow deliberately disregards actual CLEAR use cases, treating them as nothing more than trivial exceptions to an otherwise "malefactory" business. (Turow Dep. 258). For example, Prof. Turow diminishes the benefits and importance of the Veterans Affairs Department using CLEAR to locate veterans to continue benefits after they move as a "rabbit hole" that has "nothing to do with" his "essential opinion." (Turow Dep. 255-56). About the example of CLEAR being used by the U.S. Department of Health and Human Services to find the correct addresses for replacement Medicare cards, Turow said "you know you're making up th[ese] stories of benefits for obvious reasons, but what I'm saying is the—the cost benefit analysis is in a vacuum here." (Turow Dep. at 267-68). When asked about specific, contextualized use cases like these, Prof. Turow thought they were a distraction from the abstract and unmoored issue of "whether or not CLEAR is . . . giving people control over their data." (Turow Dep. 256).

Because Prof. Turow has refused to consider the ways in which CLEAR is actually used, and the way that those uses may confer benefits to Californians, his opinion cannot inform any understanding of whether CLEAR in fact causes harm. He has not explained why the CLEAR product should be regarded as anything other than a collection of beneficial "rabbit holes."

ii. Administering a Transaction that a Consumer Requests or Authorizes

CLEAR data is allowed to be used when a client is verifying the identity and critical attributes of a customer who is engaging the CLEAR client's services. (TR-BROOKS00001168) For example, when a business wants to secure a loan, the business will want to get through the initial requirements of verifying the identities and good standing of its principals. (TR-BROOKS272513-20). When data is used to establish trust that a person seeking a service is who they say they are, the data subjects benefit by making the process faster and less cumbersome. *Id.* They also benefit indirectly for the same reasons that data subjects generally benefit from protecting against fraud, which I discuss in the next Subpart.

b. For the Protection of Others (and Often for the Indirect Benefit of the Data Subject)

The Turow Report suggests that CLEAR causes "concrete privacy harms" any time the information accessed through CLEAR may "create a data-picture of the individual that is not sanctioned by the person and might well be at odds with the picture the individual has been trying to create." (Turow Report at 18).[46] This ignores the fact that the "picture" the data subject has been "trying to create"

[46] In deposition testimony, he further offered that any time a person experiences a negative consequence as a result of information about them being shared with a decisionmaker without their consent, it is a privacy harm and a violation of

may be deceitful and harmful to others who have more compelling interests in discovering the misrepresentation than the data subject has in keeping it in place.[47] One of the greatest services that a platform like CLEAR performs is to protect data subjects indirectly by allowing businesses to confidently differentiate them from attempted fraudsters and criminals, as the remaining use cases demonstrate.

i. Complying with Legal Requirements and Legal Process

This subsection addresses two permissible purposes: "Complying with federal, state, or local laws, rules, and other applicable legal requirements", and "complying with a properly authorized civil, criminal, or regulatory investigation, subpoena or summons by Federal, State, or local authority." (Attachment A at *3).

Federal and state law often require firms or employers to perform due diligence to detect or avoid illegal activity.

One well-known example is the anti-money laundering and Know Your Customer requirements in the U.S. Bank Secrecy Act. Financial institutions are legally obligated to create and maintain effective due diligence and monitoring systems.[48] Other industries that are not covered by the Bank Secrecy Act (including the legal profession) are nevertheless under regulatory or tort-based legal obligations to use reasonable care to guard against the criminal conduct of agents or customers.[49] CLEAR can also be used to execute particular court orders or judgments. For example, CLEAR has been used to discover that parents who are delinquent in child support payments have new income streams. (TR-BROOKS001995).

CLEAR has also been used to perform due diligence on employees or contractors who are in positions where conflicts of interest or abuses of position present significant risks. For example, one CLEAR client discovered that a prospective vendor for a children's hospital had an undisclosed pedophile conviction. (TR-BROOKS0000876).

This category of permitted uses is not just allowed but required under the law, and so the fact that CLEAR helps clients meet legal obligations is presumptively highly beneficial.

Data subjects benefit from the higher data quality and more complete records available through CLEAR. Clients have reported that CLEAR helps reduce the rate of false positives in the course of money laundering monitoring. (TR-BROOKS0000776). This means fewer bank customers are suspected of engaging in money laundering and are left undisturbed from credit card freezes, bank holds, and other consequences of follow-up investigations.

---

the right to be let alone, even if they are engaged in a criminal act. Turow Dep. 214. For example, he explained that it might be "repugnant" for a non-profit to use CLEAR to investigate a donor if the non-profit did not provide notice to the donor. (Turow Dep. at 271-72). He did not address how this could be done without undermining the very purpose of the search—to detect money laundering, bribery, or other malfeasance.

[47] *See, e.g.,* NISSENBAUM, *supra* note 11 at 178 (describing the employment context. "It is clear why presentation of self would be important for applicants, but just as clear why companies might resist applicants' claims trumping their own.")

[48] *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, MONEY LAUNDERING, available at https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/money-laundering/index-money-laundering.html.

[49] ABA Task Force on Gatekeeper Regulation and the Profession discussed a new ABA Model Rule that would impose "client due diligence" on the legal profession to avoid indirectly enabling money laundering or illegal tax shelters. AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY, FORMAL OPINION 491: OBLIGATIONS UNDER RULE 1.2(D) TO AVOID COUNSELING OR ASSISTING IN A CRIME OR FRAUD IN NON-LITIGATION SETTINGS (2020).

ii. Protecting Against or Preventing Fraud

If privacy were understood to require absolute control by a data subject, it would be very difficult to uncover fraud and false impersonations.[50] If a company has poor quality information about business associates or clients such that it cannot screen out fraudsters, the company will have to assume a certain amount of loss due to fraud and charge a high enough interest rate to *all* customers in order to cover those costs. The inability to screen out the fraudster will cause pure waste—a money hemorrhage—which will affect the lender and other borrowers alike. In the worst-case scenario, lack of information about the quality of a borrower can lead to a pernicious cycle—a "market for lemons"—where those who are willing to pay the higher interest rates are disproportionately more likely to be fraudsters. This can cause various markets to fail entirely.[51]

Thus, in order for certain activities to take place at all or to flourish, companies need to develop a way to investigate and gauge the veracity of the information that a prospective client or business partner has supplied. In other words, they need to access personal information about the prospective client or partner from a source that is not under the client or partner's control.

CLEAR is used for this very purpose. CLEAR clients have used CLEAR to uncover fraud when trying to find a defaulted borrower (TR-BROOKS00001168) or when verifying bank account applicants. (TR-BROOKS00001688) They have used the service to investigate whether borrowers are using multiple identities. (TR-BROOKS00001992).

The CLEAR clients who improve their detection of fraud are serving their own interests, of course, but they also serve the interests of their non-fraudulent customers and data subjects who will receive better terms if fraudsters are found and weeded out. A banking system with well-functioning verification protocols ensures that customers are able to avoid both street crime (by keeping their assets in a bank instead of holding them in cash) as well as identity theft.[52] Data subjects also benefit from fraud prevention when identity thieves are thwarted from illegally securing loans or initiating contracts in the data subject's name.

CLEAR is also regularly used by government agencies to prevent fraud-on-the-public. For example, when the government engages with outside vendors to perform specific tasks, a significant portion is lost to fraud. During the pandemic, vendor fraud has been a particularly pronounced problem, costing taxpayers as much as $1 billion by some estimates.[53] CLEAR allows government clients to find evidence in the personal histories of vendor owners or key employees that the vendor may be engaged in fraud—for example, if they own multiple cars or properties in different states out of proportion to the income expected from their line of work, or if they have a history of unpaid debts or successive bankruptcies. (TR-BROOKS146614). CLEAR clients have also used CLEAR to screen out fraud and waste in their Medicare/Medicaid systems. (TR-BROOKS00002103).

When these searches are performed, the taxpayers are the beneficiaries because they avoid the waste that they'd have to eventually pay for when tax evasion or fraud is uncorrected. But it's important to

---

[50] Richard Posner, *The Right of Privacy,* 12 GEORGIA L. REV. 393, 401, 403 ("To the extent that people conceal personal information in order to mislead, the economic case for according legal protection to such information is no better than that for permitting fraud in the sale of goods." And "there is a prima facie case for assigning the property right [to personal data] *away* from the individual where secrecy would reduce the social product by misleading the people with whom he deals.").

[51] *See* George A. Akerlof, *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism,* 84 Q. J. ECON. 488 (1970).

[52] Nicholas Economides & Przemyslaw Jeziorski, 36 MARKETING SCIENCE 815 (2017) (studying mobile devices that can verify identity in Tanzania. Mobile payments networks allow for easy deposits and withdrawals and reduce the risk of robbery).

[53] J. DAVID MCSWANE, PANDEMIC, INC: CHASING THE CAPITALISTS AND THIEVES WHO GOT RICH WHILE WE GOT SICK (2022).

recognize that data subjects also benefit directly from fraud investigations performed with the help of CLEAR because those investigations can clear up suspicion that would fester or result in more intrusive actions in the absence of CLEAR. For example, if a new bank account is flagged for possible identity theft, CLEAR data can be and has been used to resolve the ambiguity in favor of the account-holder and ensure that their account isn't frozen or reported to law enforcement. (TR-BROOKS00001689) When CLEAR has been used to investigate tax fraud, it has occasionally led to information that shows the target of the investigation had unclaimed tax benefits that they didn't realize they were entitled to, thereby reducing the number of revenue service letters, investigations, and collection attempts. (TR-BROOKS00001872) It has also allowed CLEAR clients to provide information to potential vendors to let them know that they need licenses or other requirements so that they can avoid unintentional non-compliance. (TR-BROOKS00001872). And all of this makes tax and government benefits compliance work more efficiently, which in turn benefits the public (taxpayers).

Thus, the prevention of fraud is another context where unconsented access to the sort of personal data contained in CLEAR is well-justified. Fraud prevention is often thought to be at the core of the interests that must override interests in control over personal data.[54]

iii. Use by a Law Enforcement Agency on a Matter Related to Public Safety

Crime takes a large toll on U.S. residents, imposing as much as $1 trillion in losses per year.[55] Crime flourishes in low information environments where the perpetrator's identity or activity cannot be observed.[56] A good deal of crime control is preventative, using whatever resources are available to reduce the opportunity for a criminal to commit an unlawful act without detection and identification. One such resource is, of course, police patrol.[57] Others are technological—artificial lighting[58], alarm systems[59], surveillance cameras[60], and mobile phones.[61] All of these cause dramatic reductions in crime, and this reinforces the important role of discovery of a criminal's preparatory activities and attempts.

Recently, private firms and police have begun to use more data-intensive means of illuminating (and therefore deterring) criminal activity. Digital identification using DNA databases and crime detection

---

[54] For example, the GDPR permits the processing of personal data without consent if it is necessary for the purposes of preventing fraud. EU GDPR Recital 47. The FTC also recognized that transparency can get in the way of the accuracy of an independent risk mitigation data system. FTC Data Brokers Report, *supra* note 25 at vii-ix.

[55] Aaron Chalfin, *The Economic Costs of Crime,* in THE ENCYCLOPEDIA OF CRIME & PUNISHMENT (2015).

[56] They are, in other words, crimes of opportunity that exploit low information. Philip J. Cook & John MacDonald, *Public Safety Through Private Action: An Economic Assessment of BIDS,* 121 ECON. J. 445 (2011); Eric Piza et al., *CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis,* 18 CRIM. & PUB. POLICY 134 (2019).

[57] Sherman and Weisburd 1995; Evans and Owens 2006; Mohler et al., *Randomized Controlled Field Trials of Predictive Policing,* 110 J. AM. STAT. ASSOC. (2015).

[58] Aaron Chalfin et al., *Reducing Crime Through Environmental Design: Evidence from a Randomized Experiment of Street Lighting in New York City,* NBER WORKING PAPER NO.25798 (2019)

[59] Philip J. Cook & John MacDonald, *The Role of Private Action in Controlling Crime,* in CONTROLLING CRIME: STRATEGIES AND TRADEOFFS (Philip J. Cook et al., eds.) (2011).

[60] Mikael Priks, *The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway*, 125 Econ. J. F289 (2015); Jillian B. Carr & Jennifer L. Doleac, *Keep the Kids Inside? Juvenile Curfews and Urban Gun Violence*, 100 Rev. Econ. & Stat. 609 (2018).

[61] Jonathan Klick et al., *Mobile Phones and Crime Deterrence: An Underappreciated Link,* in RESEARCH HANDBOOK ON THE ECONOMICS OF CRIMINAL LAW (Alon Harel & Keith N. Hylton, eds. 2012).

using Big Data predictive policing have been shown to reduce crime.[62] Thus, personal data that can reveal suspicious activity or identify criminals are likely to improve public safety.

CLEAR has been used to solve cold murder cases (Attachment A at *4), to locate missing or kidnapped persons (*Id.*), and to respond to active shooter situations (Attachment A at *5). For example, officers used CLEAR to locate the San Bernardino shooters, who had provided an incorrect address to the rental car company, which was the main lead that the police had following the active shooter alert. (TR-BROOKS00001856). Law enforcement has used CLEAR to find additional addresses to locate a wanted suspect, and have reported back to CLEAR that their service provides not only more information, but higher quality information. (TR-BROOKS000806, TR-BROOKS000842, TR-BROOKS001564; TR-BROOKS000860). Importantly, in many of these cases, law enforcement agents believe that the results would not have occurred without the use of CLEAR. For example, one law enforcement agency was having difficulty responding to a spate of auto thefts, and within a week of securing access to CLEAR, they were able to recover 25 out of 29 stolen cars and identify the airport parking attendant who was taking bribes in exchange for turning a blind eye to the thefts. (TR-BROOKS049485).

CLEAR has also been valuable for improving the efficacy of the National Crime Information Center (NCIC) database by allowing law enforcement to figure out accurate names and other identifiers to search for outstanding warrants. (TR-BROOKS00000761).

As with the example of using CLEAR for fraud detection, law enforcement use of CLEAR is also beneficial for data subjects, not only indirectly (through its impact on public safety) but directly as well. CLEAR has been used by public defenders for exoneration purposes (Attachment A at *4), and it has been used to eliminate innocent individuals from suspicion, as was the case when the son of a criminal child pornography producer was able to be disambiguated from his father. (TR-BROOKS00002004).[63] CLEAR can also help law enforcement quickly discern whether a suspect is a threat or is in a state of mental or financial distress. (TR-BROOKS00001990, 00002001). Indeed, as I describe in more detail below, named Plaintiff Cat Brooks may have benefited in exactly this way given that the [redacted]

Law enforcement and public safety have long been recognized as critical public functions that must, in some circumstances, override interests in privacy as long as there is sufficient process in advance (e.g. securing a warrant or subpoena) or as long as the privacy intrusions are not significant. Where the Fourth Amendment allows police to perform a search, privacy statutes and norms have traditionally allowed or sometimes even required firms to cooperate with police investigations.[64] Thus, this permissible use is narrowly circumscribed around a traditional and highly valuable context where the benefits of data access exceed the detriment to data subjects.

iv. Resolving a Consumer Dispute or Managing Institutional Risk

Finally, Thomson Reuters allows CLEAR to be used by firms that are resolving disputes with a customer or managing institutional risk. These uses include investigating a claim or preparing for a

[62] Jennifer L. Doleac, *The Effects of DNA Databases on Crime,* 9 AM. ECON. J.: APPLIED ECON. 165 (2017) (DNA); Giovanni Mastrobuoni, *Crime is Terribly Revealing: Information Technology and Police Productivity* 87 REV. ECON. STUD. 2727 (2016) (predictive policing).

[63] These uses are consistent with what Joshua Fairfield and Erik Luna have called "digital innocence." Joshua A. T. Fairfield & Erik Luna, *Digital Innocence,* 99 CORNELL L. REV. 981 (2014).

[64] Communications Assistance for Law Enforcement Act, 47 U.S.C. 1001-1010 (requiring telecommunications providers to design equipment to facilitate targeted surveillance for law enforcement); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions,* 111 MICH. L. REV. 485 (2013).

litigation defense. It also includes executing contractual rights, for example, to recover or repossess collateral and other items if a customer has breached an agreement that establishes the firm's right to recovery. CLEAR clients have also used CLEAR to protect their customers and employees during the COVID-19 pandemic by finding the best contact information for the purpose of contact tracing.

These cases have a lot of conceptual overlap to uses related to fraud (e.g. where a customer has promised to return collateral in the event of a breach but then skips town) and to uses related to the direct benefit of the data subject (e.g. where a customer is notified that they may have been exposed to a virus or other public health risk so that they can take appropriate precautions.) Thus, the reasoning laid out in the subsections above apply to this category as well.

In summary, the set of limited uses for which the CLEAR platform is made available to clients is narrowly tailored to the practical interests of society. Prof. Turow believes that these beneficial examples are exceptions—the rare beneficial use for an otherwise corrupt and exploitative company. He compared Thomson Reuters to mobsters and Tammany Hall gangsters who should be regarded as bad even though they built the Brooklyn Bridge. (Turow Dep. 273-74). His Report and deposition testimony repeatedly suggest that the CLEAR platform collects excessive amounts of data and makes them available for marketing and nearly any other commercial purpose that CLEAR clients wish. (Turow Dep. 51 (claiming CLEAR is selling "audiences" to its clients); Turow Dep. 257 (referring to Thomson Reuters as a "malefactor"); Turow Report at 13 (claiming that CLEAR is accessible for a "variety of uses")). Given this mistaken belief, Prof. Turow concludes that the beneficial use cases still cannot justify the platform as a whole. (Turow Dep. 274). But his understanding of exceptional beneficial use cases against a backdrop of routine privacy-invading uses is badly mistaken. Based on the evidence referenced above, the beneficial use cases *are* the routine use cases. Indeed, they are the *only* permitted uses.

c. The Individual and Collective Benefits for Californians Are Highly Dependent on the Particulars of the Data Subject, the Purpose of the Search, and the Quality of the Data Relative to Other Available Options

Prof. Turow claims that "while the specific content of individual reports may vary, every Californian whose information is accessible through CLEAR has suffered the same fundamental privacy harm of a lack of control and a violation of their right to be let alone." (Turow Report at 13). Prof. Turow also believes that CLEAR customers would have an option to get the information they need to complete a socially beneficial project without resorting to the use of a data search product like CLEAR. (Turow Dep. 262 ("Why couldn't they go to another place to find those data that is more legitimate?"); Turow Dep. 267 ("maybe they could find out a better way to get those addresses"). The implication is that Prof. Turow believes there either is or could be a way to access the right data, at the right time, with the consent and control of the data subject, in order to accomplish the socially valuable goals described above.

This is not correct. Some permissible uses of CLEAR performed for the direct benefit of the data subject *have to be* done without advanced authorization, such as locating the data subject to deliver a payment that is owed to them. (*See* discussion *infra*, Part V(c)(i)). The premise of the search is that the data subject cannot be found. For other permissible purposes, data subject control would undermine the goal of detecting fraud, crime, or other wrongdoing. There is no "better way." Other options are either equally lacking in consent, more noisy and error-prone, or both (e.g. interviewing neighbors or finding other data aggregators like the Google search bar).

The effects on individual data subjects will be mixed: not every data subject will be made better off, at least not directly. But as long as the purpose of running a search is legitimate (e.g. to prevent crime or fraud), and as long as on balance the information made available through a platform like CLEAR is more complete or more accurate than the information sources that would be used in its absence, there will be more "winners" than "losers", and society will be well-served.

To understand why this is so, consider the role of information when consumers make decisions about which restaurants to patronize. When consumers have greater access to information about businesses, they are more likely to have a good experience and, thus, will eat out more often. But not every restaurant will see its patronage increase: information from Yelp reviews and other independent review systems tends to help smaller or less well-known market participants more, and chain restaurants therefore lose their relative share of the restaurant market.[65]

The same mixed effects occur when businesses judge their potential clients and contractors, too.[66] Imagine how a person who is tasked with vetting new consultants to make sure they are not fraudsters or embezzlers would approach their job. The vettor would inevitably have *some* information—the results of a Google search, or a public records search, for example. This is the baseline we must judge CLEAR against. We must consider the impact of CLEAR on data subjects as well as society as compared to a decision that is made with lower-quality information.[67] That is, what we must *not* do is fall subject to the Nirvana fallacy where the use of CLEAR is compared to a situation where the company does not access any information without the data subject's consent and still, miraculously, winds up correctly identifying which prospective consultants are going to engage in criminal activity. Prof. Turow engages in this fallacy when he said "CLEAR is not the be all and end all of – of the ways to find out [information for socially beneficial purposes]. It just happens to be used because it exists." (Turow Dep. 275).

When comparing the effect of the use of CLEAR on a lower-quality source of information, the marginal effect of CLEAR will cause the vettor's opinion of the data subject to either improve, diminish, or stay about the same. Let's consider how this can affect data subjects and the decision-makers as a whole by plotting the effects of using CLEAR against a lower-quality alternative source. It is possible that some data subjects can wrongly be perceived as more risky after a CLEAR search than they would have been perceived after a search of a different kind, but as long as the overall accuracy and completeness of the data is better in the CLEAR platform, these instances will be greatly outnumbered by the instances where a decision-maker makes *better* judgments. That is, in most cases, CLEAR will help decision-makers have confidence about innocent clients who would otherwise look more suspicious with lower quality data. And CLEAR would also help decision-makers have greater suspicion about the data subjects who are *not* innocent—who are likely to engage in fraud or crime.

A visual representation of CLEAR's impact in a fraud detection system might look like this:

---

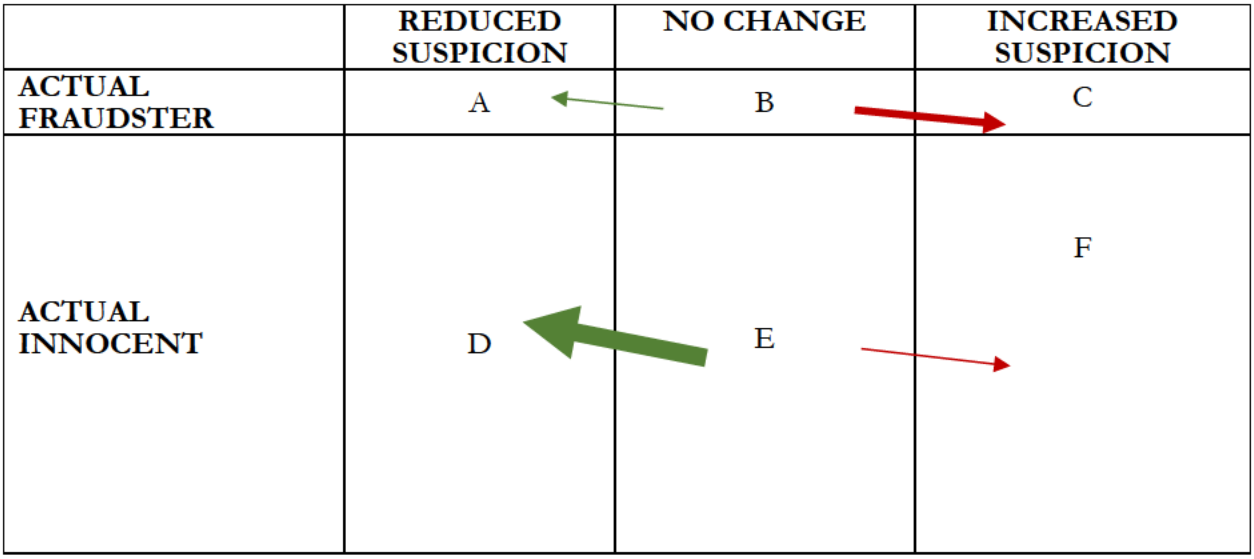
[65] Luca (2011). The same is true for hotels. Hollenbeck (2018)

[66] A range of social institutions have allowed market transactions to take place even when individuals do not know each other well enough to have longstanding relationships of trust. Word of mouth, gossip, and status signals help create enough of an incentive for trade partners to cooperate, and enough of a disincentive against deception. Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance,* 89 J. POL. ECON. (1981); Hongbin Cai et al., *Seller Reputation: From Word-of-Mouth to Centralized Feedback,* 34 INT'L J. IND. ORG. 51 (2014); Carl Shapiro, *Premiums for High Quality Products as Returns to Reputations,* 98 Q. J. ECON. 659 (1983).

[67] The Turow Report questions the quality of the data that the CLEAR service makes available. Turow Report at 14 n.40. However, Prof. Turow does not claim that the quality of CLEAR data is inferior to the quality of the data that would be used by CLEAR clients in the absence of the CLEAR service. My analysis in this Part assumes that data available on CLEAR is more complete and leads to more accurate assessments of the data subjects. This is a justified assumption based on the empirical literature, cited earlier in this report, that finds access to more and more varied data leads to better "matching," to use the economics term. CLEAR's business model depends on adding value by improving accuracy—both by raising red flags that would go unnoticed and by removing unwarranted suspicion—and has selected its vendors and designed its user interface to do precisely that. I directly address CLEAR's protocols for maintaining data quality in Part VI.

A Decision-Maker's Impression of Data Subjects After CLEAR Search As Compared to the Impression After a Lower-Information Search†

†The size of the arrows represent the relative proportion of data subjects who are moved to greater or lesser suspicion when a CLEAR search is used instead of a lower-quality information search. Thicker arrows mean relatively more data subjects are moved in the direction of the arrow. The thickness of the rows indicates the relative proportion of data subjects that are actual fraudsters is small (thin) compared to innocent actors (thick). This chart is for illustration purposes only; the relative thickness of each arrow will depend on many factors including the quality of the alternative information source, the type and frequency of fraud(s) that are being investigated, and the ability of the decision-maker to infer risk from historical information.



The chart helps us make sense of the impact that CLEAR can have on data subjects and others. As compared to alternative sources of information, we can expect that the information made available through a platform like CLEAR will allow clients to better match their *perceptions* of risk to the *actual* risk. This is generally true of data repositories that use more, varied, and credible sources of information, and nothing in Prof. the Turow Report suggests it would be otherwise.[68]

For data subjects where there is no difference between the perception of risk under low-quality information and CLEAR—that is, the middle column including groups B and E—the impact of CLEAR will be negligible. Data subjects in groups A and D (the first column) will be in a *better* position as a result of CLEAR. When it comes to group A, this is not actually a good outcome because, while the fraudster might be happy, the costs of their crimes will be borne by others. But for group D, this is an unqualified good outcome. The data subject is better off because the possibility of misperceived risk is cleared away, and the vettor is also better off because they can proceed with a relationship rather than changing course, declining to work with the data subject, or engaging in more research.

Finally, we must consider the two groups that might have a claim that CLEAR has made them materially worse off than they would have been in the absence of the CLEAR product: groups C and F (the last column). Group C can be ignored, as fraudsters who have correctly been judged as risky do not have a cognizable claim to harm. Group F represents the portion of data subjects

[68] *See* sources *supra* note 36.

whose more complete record of personal details suggest that they pose a greater risk than the vettor would have assumed with lower quality information, but who in fact do not pose any such risk. This is genuine system error (assuming the set in group F is not empty). But the losses to this group are counterbalanced by the gains among data subjects in group D who are correctly perceived to be less risky when a more complete and accurate set of information is used. So, although some individuals will be misclassified, fewer will be than would occur under conditions of lower quality data.[69] Thus, even if Group F is not empty, as long as harm to Group C is substantially smaller than the benefits to Group F, the social contract approach to privacy would suggest that most people would agree in advance that use of better, more complete information should be used in these circumstances. And of course all data subjects and the general public stand to benefit from the increased detection of fraudsters (group C).

Those who are not well-steeped in the empirical information economics literature might doubt the size of these arrows. They might believe that more complete information leads to more distrust overall, and a net loss of matching and opportunities. This isn't so. The experience with credit reports shows that lending becomes more common, and at cheaper interest rates, when there is more information, even though the increase in information includes more data related to late payments, defaulting, and other seemingly negative attributes.[70] Nor do the type of risk scoring systems that can be displayed in CLEAR with the user's input and direction (TR-BROOKS 001314-21; 272516) lead decision-makers to have heightened suspicion; a 2018 study of the impact of public safety risk assessment scores in the pre-trial detention decisions in the state of Kentucky found that after a new law went into effect that required judges to look at an automated risk score, the percentage of arrestees who were released without bail increased across the board, including for individuals with relatively high risk scores.[71]

The end result is that, system-wide, the impact of CLEAR is positive because it increases accuracy and efficiency. These cost-savings are ultimately shared by consumers (who don't have to pay extra to cover the costs of system-wide fraud) and the public at large (who are better protected from fraud, money-laundering, theft, and other crimes). For individual data subjects, the benefits or costs will depend on the particulars of each search context (what the nature of the assessment or vetting is, what data sources are available, what the next best alternative to CLEAR would be if the client had to use something else). But even though the impact on individual data subjects varies by person and search, the effect is positive on net.[72] For at least some purposes, people will generally accept and even expect that information will be used to capture these social benefits.

---

[69] Avi Goldfarb & Catherine Tucker, *Digital Economics,* NBER WORKING PAPER NO. 23684 at 11-13 (2017).

[70] Prior to the advent of the credit report, some individuals could gain the trust of others by having a family member, neighbor, or organization vouch for them, or by having a good reputation. These social vouching systems leave much to be desired-- they used noisy signals of trustworthiness such as whether a creditor's daughter was chaste. DAVID GRAEBER, DEBT: THE FIRST 5,000 YEARS 328 (2011). Perhaps because these mechanisms were so noisy and nepotistic, credit markets for large sums, suitable for investments, were very tight and reserved almost exclusively for business rather than personal use. Lewis Tappan created the first large scale systematic collection of records for the purposes of assessing credit-worthiness in 1841 after losing much of his wealth a few years earlier in an economic depression caused by the over-extension of credit. (Tappan's large collection of gossip and reputation ledgers were the first information assets of what would eventually become Dun & Bradstreet). These efforts, which eventually led to the credit reporting industry, allowed individuals without letters of introduction and other trappings of the upper class to access large loans and build up personal wealth. *Id.*

[71] Megan Stevenson, *Assessing Risk Assessment in Action,* 103 MINN. L. REV. 303, 351, 354. Note that the study found that detainees with high risk scores were, at the same time, somewhat less likely to be released within three days of booking, suggesting that scores led to individuals in this group being treated with more leniency in some cases, and less in others. Detainees with low and moderate risk scores were 9% and 7% (respectively) more likely to be released within three days of booking. *Id.* at 354.

[72] The private sector has spawned and sustained an industry of information intermediaries precisely because the data collection and organizing services that they offer allow clients to more accurately (and, thus, more fairly and with less

d. Analysis of Benefits and Harms to the Named Plaintiffs

The economic and practical impact to any given data subject will depend on their characteristics and the context of the transaction, but as the last subpart explained, we should expect the typical data subject to benefit from the CLEAR product given its limitations of use to socially beneficial purposes. This appears to be true for named plaintiffs Cat Brooks and Rasheed Shabazz as well.

Nothing in the records I reviewed suggest to me that named plaintiffs Cat Brooks or Rasheed Shabazz have been concretely harmed by CLEAR. In fact, there may be reason to think that CLEAR has helped and will help each of them avoid others' negative misperceptions of them. In terms of the diagram presented above in Part V-c, Cat Brooks and Rasheed Shabazz are likely to be in group "D." That is, if CLEAR is used with respect to Ms. Brooks and Mr. Shabazz, the use will most likely result in confirming that they are both upstanding individuals who pose low risk to themselves and others.

For example, in Cat Brooks' case, Brooks was not able to identify any adverse impact on her from any search conducted using CLEAR.[73] [redacted]

In the future, CLEAR could help protect Cat Brooks from other adverse actions by aggregating enough records for users to quickly see which ones have errors. For example, [redacted] If either document—[redacted]—were the only source used by a decision-maker, suspicion of Cat Brooks could rise, and the decision-maker would have to take more precautions to verify Cat Brooks' identity. A CLEAR client, however, would see [redacted] (TR-BROOKS008262-63). With the whole set of records on CLEAR, the decision-maker would ignore [redacted] and have more confidence that, e.g., Cat Brooks is not trying to impersonate a much older or differently named individual. [redacted] create a more accurate picture than either one in isolation, and therefore avoid risks of misplaced suspicion that Brooks might face if any one information source is used alone. Also, Cat Brooks' Wikipedia page stated that she had been arrested in 2015, which Ms. Brooks testified was inaccurate. (Brooks Dep. at 101). It is possible that a company considering a transaction of some sort with Brooks that did not have access to CLEAR would use a Google search and the information contained in her Wikipedia page in order to assess her, and these sources would be less accurate and potentially more harmful to her reputation.[74]

---

cost) identify clients or business partners who would otherwise be miscategorized. Goldfarb & Tucker, *supra* note 70 at 26 (discussing how the private sector has generated mechanisms to reduce error in reputation systems).

[73] Brooks' own investigator conducted searches on her name, but those searches were conducted with her consent. TR-BROOKS055887

[74] The plaintiffs claim that they are "saddled" with high risk inform scores. (Complaint at 10-11). In fact, Brooks' report only displays a high score when all possible flags were selected by her team (TR-BROOKS008256-59). Also, the Complaint alleges that plaintiff Brooks might be harmed by the Risk Inform score because it can incorporate and "penalize her" for having changed her name. Complaint at 9-10. The CLEAR reports clearly label the Risk Inform scores, when they are requested by users, so that it's immediately clear how much of the score is attributable to the name change, allowing the user to see that in context, there is no reason for concern. TR-BROOKS008256-59. Moreover, since alternative data resources like Google searches and browsing Wikipedia pages would lead to the same information, the fact that Ms. Brooks has changed her name is readily discoverable to any decision-maker who is likely to hold that

In Rasheed Shabazz's case, Plaintiffs' complaint alleges that CLEAR poses risk by retrieving court records related to a divorce and unpaid child support against a different person who shares Shabazz's birthname (Reginald James). (Complaint at 11). While it's true that CLEAR provides these court records upon a search of the plaintiff's birthname and date of birth, the CLEAR report provides an "Averse Records" risk indicator score of 0—a signal to users that they should not assume these records actually pertain to the James Reginald who was born in [redacted]. (Video, TR-BROOKS010275 at 13:00). In order to even see these records, the user has to click on "Averse Records" despite the fact that the platform indicates there is a "0.00" risk. (*Id.*). To know whether Rasheed Shabazz is likely to be made worse off as a result of the retrieval of these records, we need to consider what information would be consulted in the absence of CLEAR. Manual public records or court docket searches could very well result in the same retrieval of records, and without the "0" adverse records risk score signaling a mismatch. Things could be even worse if a decision-maker who isn't able to access CLEAR decides instead to run a Google search on "Rasheed Shabazz." They may discover a rape conviction of somebody named [redacted] and become concerned that they cannot rule out, without more information, that this might be the same "Rasheed Shabazz". Users of CLEAR, on the other hand, will not even encounter the records for [redacted] (TR-BROOKS008719-8740; Video, TR-BROOKS010275).

Cat Brooks' and Rasheed Shabazz's CLEAR reports provide information that is more positive and reassuring than a naïve Google search, public records search, or more limited search for information would suggest. CLEAR reports show factors like name changes in context, and they do not provide erroneous information about arrests (Brooks) or convictions (Shabazz) that did not take place but are publicly reported in Google searches. Although both named plaintiffs have multiple names associated with their social security numbers—something that tends to heighten concern and lead to more scrutiny when it comes up in verification and background checks— the fact that both have changed names is a fact that is likely to be uncovered by entities who are vetting and verifying each plaintiff whether they use CLEAR or not. By providing a more complete record, CLEAR will tend to reduce suspicion. Thus, as far as I can tell, neither named plaintiffs' data has been accessed through CLEAR in a manner that caused concrete harm to them, and there is reason to believe that CLEAR can help, and possibly already has helped, the named plaintiffs by steering users of the CLEAR platform toward an action that is less circumspect and more beneficial.

Thus, while the particular benefits and costs of the CLEAR platform depend on many factors that will vary search by search, economic theory and the extant empirical evidence suggest CLEAR can bestow benefits on data subjects and California residents more generally. And data subject control is neither necessary nor desirable to serve the interests of Californians.

The foregoing analyses show that CLEAR only permits access to personal data when the benefits of access are particularly strong. CLEAR facilitates some of the most important economic and public safety functions that people expect and rely on.

VI. CLEAR Has Strong Protections Against Risks of Misuse or Mistaken Associations

The Turow Report opined that there was a lack of protections in place to ensure the reliability of information made available through CLEAR and to ensure that clients were not using the data outside the range of permissible purposes. (Turow Report at 5 (referring to "protections in place (or lack thereof)" of each of these)). Prof. Turow's analysis of CLEAR's safeguards is based on his belief that CLEAR's protocols, even if highly effective at preventing and detecting access or use of data that violates the terms of service, would still not reduce the "essential misuse of CLEAR, which

fact against her. Mr. Shabazz has also publicly disclosed his birthname and his decision for changing his name. (TR-BROOKS008701).

is that CLEAR, itself, takes data . . . and doesn't give people control over those data." (Turow Dep. 305).

To the contrary, because CLEAR has reasonable protocols for credentialing, training, and monitoring clients that use the system, CLEAR does not create a significant risk of misuse by clients or unintended data disclosures. And since the permitted uses are highly beneficial, the CLEAR product as a whole avoids creating significant risks of privacy harm.

a. CLEAR Minimizes the Risk of Misuse Using Credentialing, Training, User Interface Design, Query Logs, and Audits

The Turow Report states "CLEAR customers must certify that they have a 'permissible use' for CLEAR when they log in. I have seen no evidence that Thomson Reuters investigates that a customer's use is, in fact, permissible." (Turow Report at 13-14). This may give the impression that it would be easy to use CLEAR for unpermitted purposes and that this may happen with some frequency. I do not agree; the record provides ample evidence that Thomson Reuters has good systems for preventing, preempting, and detecting misuse.[75]

First, CLEAR has many precautions in place at the front end, when a client begins the credentialing process. To become a subscriber, a client must first go through a credentialing process in which a compliance team at Thomson Reuters reviews the application and considers whether the client's typical use cases are permissible. (TR-BROOKS013638-40; TR-BROOKS013534-35). They also vet each client to ensure that newer businesses, or businesses with little public presence or reputation, do not present a high risk for engaging in abuse. (TR-BROOKS295350). I have also reviewed records demonstrating that Thomson Reuters salespersons escalate some new clients to the compliance team if, for example, the type of business of the prospective client is a new type of customer for CLEAR, if the business is relatively new, or if the business address is in a different state from where the principals live. (Id.)

This is not a formality. A 2020 compliance report shows that the compliance team did follow-up investigation requiring discussions with managers and owners of prospective clients and also conducted independent investigations. (*Id.*) Prospective clients have been denied because they intended to use CLEAR for wage garnishment (not a permitted use), because they intended to use the service to return found or unclaimed money (not a permitted use even though presumptively helpful to data subjects), because the intended uses were FCRA-related searches related to employment or lending, because the business was not properly licensed, and because Thomson Reuters could not validate the business as legitimate, among other reasons. (Id.) Thomson Reuters declined over [redacted] in potential contracts during the year on account of concerns that some of the prospective clients posed a risk of misuse. (*Id.*; TRBROOKS305116). This represents a significant portion of potential new business—over [redacted] of potential contracts—that were declined in order to maintain TR's standards for keeping risk to a minimum. (TRBROOKS305116).

Clients must be recredentialed, and employees with access to CLEAR must be re-trained, every two years at the latest (Attachment A at *5). In addition to agreeing to use CLEAR only for a permissible purpose, clients must also affirmatively certify that they will *not* use CLEAR for any FCRA purpose, or any purpose other than those explicitly permitted. (Attachment A at *5).

[75] Turow also claims that a customer may run a "person search" that allows the customer to view "information that pertains to other individuals unrelated to the target of their investigation (and, accordingly, unrelated to the customer's selected permissible use.)" (Turow Report at 14). I disagree that the limited details retrieved related to a data subject's neighbors, associates, and family are "unrelated to the target of their investigation" because many of the intended purposes for CLEAR involve situations were talking to family members, neighbors, or associates can resolve a problem. For example, if law enforcement are trying to find a missing or kidnapped person, contacting the person's neighbors and business associates will certainly be useful and relevant for the investigation.

CLEAR clients are contractually obligated to refrain from using, copying, or distributing data accessed through CLEAR in any way other than those described in the licensing agreement. (TR-BROOKS000482; TR-BROOKS001369) Sharing passwords is prohibited, and subscribers must ensure that they have taken reasonable precautions to avoid unauthorized access to the CLEAR system. (TR-BROOKS000482). Specifically, clients must use adequate malware protection software (TR-BROOKS000482). And they must immediately report to Thomson Reuters if they believe an employee has misused the platform in violation of the terms of use. (TR-BROOKS013538).

Once a subscriber has access to CLEAR, Thomson Reuters uses reasonable protocols to ensure that clients have the incentive to comply with their contractual terms and to detect and report instances of misuse. The format of the query system re-enforces the rules and obligations: except for limited exceptions where other security is in place, a client first has to get through a two-factor authentication process to access the query screen. (TR-BROOKS001374). Before entering search terms, the user must select a permissible purpose (*Id.*) Outside a limited batch retrieval process, users can run only one search at a time. Clients are forbidden from using scripts or other automated searches. (TR-BROOKS001369).

The data that is ultimately retrieved for a search will depend on the permissible purpose. For example, records covered by the Driver's Privacy Protection Act ("DPPA") can be used only for purposes of fraud prevention, debt recovery, in connection with a legal proceeding or insurance claim, or for use by a government agency and will not display unless the user selects one of these purposes. Voter registration records can only be used for election-related or non-commercial purposes. (Attachment A at *3)

Users understand that queries are logged so that the search and the login credentials of the person who ran the search can be reviewed retrospectively. (Fox Dep. at 155, 160; TR-BROOKS001378). The user manual makes this clear, and the settings menu on the CLEAR dashboard also makes this obvious by allowing users to see their own "History." (TR-BROOKS001378). Thus, all users have the information and the motivation to refrain from unpermitted searches.

Thomson Reuters has also created systems to make it likely to detect non-compliance. The licensing agreements with CLEAR's data vendors give vendors the right to audit CLEAR's systems, including the query logs. (Fox Dep. at 176). The [redacted] and some states' Departments of Motor Vehicles have conducted such audits. (*Id.*) The licensing agreement explains that Thomson Reuters has the right to use the logs to audit or monitor the use of their system in order to find violations of the agreement. (TRBROOKS000482).

Thomson Reuters also conducts its own audits. In 2020, Thomson Reuters initiated a public records audit program that selected thirty customers each month to respond to a survey designed to elicit whether CLEAR data were being used in compliance with the agreement terms. (TRBROOKS304709-20). The goal is "to ensure that our investigative products are used by LEGITIMATE ENTITIES with a PERMITTED USE CASE with a demonstrable PERMISSIBLE USE under the applicable regulations.") (TR-BROOKS 305116). The program ensured that half of the audit surveys were sent to CLEAR users who may be at higher risk of improper access—i.e. users who were in collections or repo industries or who worked in settings with less managerial oversight (e.g. realtors or clients who run a home business). (TR-BROOKS 304709-20). Clients are obligated under the terms of their licensing agreement to comply with the audit, and those who do not respond to the audit survey after a second reminder email are informed that their access to CLEAR will be suspended. (TR-BROOKS304719-20). Thomson Reuters also actively monitors its query logs for some of the most common misuses of databases: snooping for the details of celebrities, politicians and other highly visible individuals. (Fox Dep. at 162-63). Thomson Reuters can and does terminate access upon discovery of a suspected breach of security or breach of the agreement terms. (TR-BROOKS 00483).

Finally, clients are required to immediately report to Thomson Reuters if they discover that any employee has misused CLEAR data. (Attachment A at *1) Administrators of the clients have access to all queries run by their employees through a service called "QuickView." (Fox Dep. 163-64; TR-BROOKS001372). And clients must assist Thomson Reuters in investigations of privacy breaches. (TR-BROOKS 000483).

The United States District Court for the Southern District of New York and the Second Circuit Court of Appeals was similarly convinced that Thomson Reuters has adequate protections in place to prevent misuse, finding that the protections were well designed to prevent this misuse of CLEAR for (unpermitted) purposes related to credit reporting. *Kidd v. Thomson Reuters Corp.*, 299 F.Supp.3d 400, 407 (S.D. NY. 2017); *Kidd v. Thomson Reuters Corp.*, 925 F.3d 99, 101-02, 107-08 (2021). In addition to noting the vetting processes I've described here, the District Court also explained that Thomson Reuters opens investigations when it learns of alleged misuse. Between 2012 and 2017, Thomson Reuters opened forty-six investigations which resulted in ten terminations. *Id.* at 402.

Based on all of these measures and protections, Turow's opinion that the CLEAR product has a "lack" of "protections in place" is unfounded. (Turow Report at 5). To the contrary, CLEAR has multiple overlapping protections that help prevent or detect misuse.

b. CLEAR Minimizes the Risk of Overcollection and Mistaken Associations Using Data Quality Procedures, User Interface Design, and Training

TR also reduces risks of unintended harm by limiting data collection and by ensuring that users understand the limits of the CLEAR platform.

TR only collects data that is likely to be useful and reliable. First, it acquires new data only when there is a demonstrated need. The impetus for collecting new data from a new or existing vendor typically starts with client requests. Thomson Reuters staff then conduct an internal analysis to see if existing data access could meet the needs of their clients. If it does not, then Thomson Reuters would seek a new data source. (Fox Dep. at 25). The type of information contained in CLEAR reports are well-matched to their functional purpose and do not contain gratuitous detail. It does not provide content of communications or detailed geolocation data. The Complaint describes CLEAR as providing a "360 degree view" of the data subjects, but the specific list of information—"address, cell phone number, and information about relatives, neighbors and associates" (Complaint at 2)—actually offer a quite limited "view", and provide only the sort of data that might be essential for, e.g., locating the plaintiffs in an emergency. Plaintiffs insinuate that CLEAR provides information about abortion, desecrating a flag, and homosexual acts (Complaint at 8), but as far as I can tell these refer only to criminal records. They are items in a long list of specific criminal convictions that may appear in a data subject's criminal record. (Plaintiffs' video of CLEAR search-TR-BROOKS010275; TR-BROOKS001363 et seq. (user manual)). Even when CLEAR contracts with private sources of data such as banks that have access to sensitive data, these sources only provide basic account and header information. Much of the information comes from public records. As a whole, the sensitivity of the data is similar to, and arguably lower than, the sensitivity of information contained in credit reports.

Factors considered when acquiring data include not only the quantity or completeness of a data source (to ensure it will have efficacy to meet the needs of clients), but also the quality of the data. Accuracy is a significant factor for assessing quality. There are two levels of accuracy to assess: one is whether the vendors' records accurately reflect the information contained in their raw sources, and the other is whether those raw sources accurately reflect facts about the data subjects. (Fox Dep. 25). CLEAR uses the reputation of the vendor, TR's experience with the vendor, and the relevance of the type of data in the vendor's possession to assess whether to contract with the vendor for new data. (Fox Dep. at 29-31). One factor in this assessment is the relationship the vendor has to the

original source of records. (Fox Dep. 157). Thomson Reuters steers away from vendors that hoover as much data as possible without exercising quality control. (Fox Dep. 30). And conversely these higher-reputation vendors implicitly find that CLEAR is a responsible data shepherd as none have invoked privacy as a reason to refuse to license data to Thomson Reuters. (Fox Dep. 121).

Because Thomson Reuters keeps a minimum standard of reliability for both of these layers, it creates a natural limit to the amount of data that will be collected even when Thomson Reuters is aware that clients have noticed a gap in records. By maintaining data quality standards as well as standards for data vendors, Thomson Reuters would not and could not hoover all available data regardless of accuracy. In fact, CLEAR sometimes improved the accuracy of public records vendors by triangulating between records and correcting typos and other errors. (Fox Dep. 28). Thus, CLEAR data is likely to be *more* accurate than raw public records, which would often become the source of information for CLEAR's clients in the absence of services like CLEAR. Thomson Reuters also uses dynamic procedures to maintain data quality. When CLEAR has discovered an error in an arrest or criminal record, this prompts Thomson Reuters to "take a close look at our data and see if we can make any improvements. . . If we see [] a number of them coming out of a particular court, that's when we will probably have a conversation with a vendor." (Fox Dep. at 158). Thomson Reuters has a procedure that enables clients or data subjects to report discovered errors, and following investigation, Thomson Reuters will either delete an inaccurate record or sever the connection between the record and the data subject. (Response to Interrogatories Attachment A at *7). Thus, there are stop gaps in place if the prospective efforts to avoid errors fail.

These data quality procedures ensure that CLEAR does not over-collect data by including information that is either flawed, irrelevant, or gratuitous given the limited purposes that the CLEAR platform allows.[76]

CLEAR's value proposition is not just that it offers *more* or *different* data than, say, a public records or Google search, but that it includes a higher quality set of data that is organized in a manner that helps users make sense of it. Thus, Thomson Reuters has an obvious business incentive to reduce error and clutter as much as it can. Thomson Reuters has lost customers on the basis of mis-pinned information—that is, information that matches part of a search query but actually pertains to another person. (Fox Dep. 94 (describing what "mis-pinning" is)). In one case, Thomson Reuters and its former client did not agree on the right way to balance the risk of over-producing records that are not related to the search target versus the risk of not producing records that actually do relate to the target.[77] These are difficult business decisions upon which reasonable minds will differ, and the tension between overinclusion and underinclusion errors is usually best addressed by collecting *more* data, not less.

To reduce the risk of harm from error, Thomson Reuters has many protocols to help prevent clients from misinterpreting CLEAR reports. During the training process, clients are taught that they must treat CLEAR reports as a retrieval service and come to their own conclusions about the assessment or meaning. (Fox Dep. 131). Thomson Reuters' training explains that the data is unverified and that there will be times when common names or other search parameters are shared by two or more individuals. Clients are instructed to view the data "critically" and to consider whether the underlying records are describing the target of their search. (Fox Dep. 171).

---

[76] Thus, based on the evidence I have seen, I disagree with Prof. Turow's conclusion that Thomson Reuters is "stockpiling unnecessary information." Turow Report at 15.

[77] As one CLEAR employee put it, "This is one of those items that is a balancing act of being loose enough to bring back non exact matches but not too loose to where we bring in irrelevant records. We are always evaluating those processes" TR-BROOKS057007. It should be noted that this former client went to a different service, presumably a competitor. It did not stop running due diligence searches. Id.

A user will have to understand that a full name and a state of residence is more likely to pull up records on one unique person if the name is uncommon, and is at greater risk of pulling multiple individuals' data if the name is popular. (Fox Dep. 131-135). The subscriber license uses bold and capital letters to highlight the portion of the agreement that reminds clients that information provided may not be suitably accurate or up-to-date for their purposes (TR-BROOKS00483).

The user interface design also guards against overconfidence. CLEAR has a screen in the application that indicates how current the records that the client is viewing are, and how frequently they are updated. (Fox Dep. 59). The search results page has a filter button that allows users to filter the results in various ways (TR-BROOKS001368), and this serves as a visual reminder that the results can be overinclusive.

As with the assessment of benefits, risks of misuse and misinterpretation should be assessed in comparison to the sources of information that clients will use in the absence of CLEAR. Prof. Turow offers no reason to believe that the misinterpretation or mis-association would be worse with CLEAR than without it. In CLEAR's absence, clients may instead turn directly to CLEAR's data sources or to competitors. Public records are erroneous, and states explicitly deny that they make any warranties about the accuracy or completeness of the records. (TR-BROOKS000620-21).

For the foregoing reasons, Thomson Reuters adequately manages the risk of misuse, error, and misinterpretation of the data that the CLEAR platform makes available. Given that it permits the service to be used only for per-se non-violative purposes, it is unlikely that CLEAR has caused harm to *any* Californian. It's effect on Californians as a class is positive.

VII. Conclusion

To summarize my analyses above:

• Prof. Turow's theory of privacy harm is that one will occur each and every time a company collects, shares, or uses information about a person without their consent and control. **In fact, while data subject control is an important factor, privacy is nearly universally understood as a right and interest that must be analyzed in context.**

• Prof. Turow believes his evaluation of privacy does not need to consider the specific purposes for which CLEAR data is collected or used, nor the specific benefits and harms that may result from those uses, because all Californians suffer from a loss of control over their data. **In fact, there are several socially valuable and individually beneficial uses of personal data that are routinely recognized as legitimate and privacy-respecting even though they occur without consent.** These include using information to find the data subject in order to help them, preventing and detecting fraud, and carrying out active law enforcement and community caretaking activities.

• Prof. Turow believes any beneficial impact certain uses of CLEAR might provide are outweighed and outnumbered by "malefactory" conduct. **In fact, the *only* purposes for which the CLEAR platform may be used are those that directly or indirectly benefit data subjects.**

• Prof. Turow doubts that the CLEAR platform has adequate security to ensure that the product isn't accessed or used outside the limited set of purposes that Thomson Reuters allows. **In fact, Thomson Reuters uses layers of security and care including a credentialing process, two-factor authentication, contractual obligations of care and reporting, routine auditing, and redress and removal of clients who breach their agreements.**

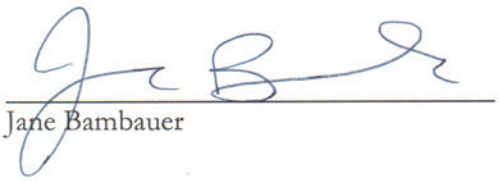
• Prof. Turow believes each and every Californian has been harmed by the CLEAR platform. **In fact, even the named Plaintiffs have benefited from their data's inclusion in the CLEAR**

product. The benefits and harms caused by the CLEAR platform will depend on the particulars of each person and use, and on average, Californians benefit from CLEAR.

• Prof. Turow believes that public agencies and companies can accomplish their goals without relying on data products like CLEAR. **In fact, in the absence of CLEAR, public agencies and companies would have to resort to using lower quality information and having worse results,** to the detriment of Californians who would more often become lost to the public benefits system or become victimized by fraud and crime and its costs.

Dated: September 7, 2022

Respectfully Submitted,



Jane Bambauer

Exhibit A:

Jane Bambauer

520.626.6004 | janebambauer@email.arizona.edu

ACADEMIC POSITIONS

University of Arizona James E. Rogers College of Law, Tucson, AZ.
The Dorothy H. and Lewis Rosenstiel Distinguished Professor of Law (2022 – present)
• Distinguished Legal Scholar (selected by peer committee) (2021-present)
• Deputy Director for Societal Impact, NSF Center for Quantum Networks (2020-present)
• Faculty Director, QuantLaw (2013-present)
• Faculty Co-Director, TechLaw (2019-present)
• Co-founder and Executive Editor, JOURNAL OF FREE SPEECH LAW (2021- present)

Professor of Law (2017-2022)
Associate Professor of Law (2012 - 2017)

Brooklyn Law School, Brooklyn, NY.
Visiting Assistant Professor of Law (2010 - 2012)

EDUCATION

Yale Law School, J.D., 2006.
- Journal of Law and Feminism, *Symposium Director and Editor*
- Legal Assistance Clinic, *Landlord/Tenant Intern at the New Haven Legal Assistance Association*
- Legislative Advocacy Clinic, *Tax Reform Advocate*

Yale University, B.S. in Mathematics, with Distinction, 2002.
- Deforster (2002), Stanley (2001), and Barge-Runck (2000) prizes for mathematics

ARTICLES

Reconsidering Tort Duty When AI Makes Everything Foreseeable (work-in-progress).

Filtered Dragnets and the Anti-Authoritarian Fourth Amendment (work-in-progress).

Reckless Associations, 36 HARVARD JOURNAL OF LAW & TECHNOLOGY __ (forthcoming 2023) (with Saura Masconale and Simone Sepe).

When a Small Change Makes a Big Difference, 55 U.C. DAVIS LAW REVIEW 2337 (2022) (with Tal Zarsky & Jonathan Mayer).

From Damage Caps to Decarceration: Extending Tort Law Safeguards to Criminal Sentencing, 102 BOSTON UNIVERSITY LAW REVIEW 1667 (2021) (with Andrea Roth).

The Quiet Resignation: Why Do So Many Female Lawyers Abandon Their Careers?, 10 U.C. IRVINE LAW REVIEW 799 (2020) (with Tauhidur Rahman).

The Algorithm Game, 94 NOTRE DAME L. REV. 1 (2018) (with Tal Zarsky).

Snake Oil Speech, 93 WASHINGTON LAW REVIEW 73 (2018).

Information Libertarianism, 105 CALIFORNIA LAW REVIEW 335 (2017) (with Derek Bambauer).

Other People's Papers, 94 TEXAS LAW REVIEW 205 (2015).

Outrageous and Irrational, 100 MINNESOTA LAW REVIEW 281 (2015) (with Toni Massaro).

Hassle, 113 MICHIGAN LAW REVIEW 461 (2015).

Is Data Speech?, 66 STANFORD LAW REVIEW 57 (2014).

The New Intrusion, 88 NOTRE DAME LAW REVIEW 205 (2012).

The Secret of My Success: How Status, Prestige, and School Performance Shape Legal Careers, 9 JOURNAL OF EMPIRICAL LEGAL STUDIES 893 (2012) (peer-reviewed) (with Richard Sander).

Tragedy of the Data Commons, 25 HARVARD JOURNAL OF LAW & TECHNOLOGY 1 (2011) (published as Jane Yakowitz).

Marooned: An Empirical Investigation of Law School Graduates Who Fail the Bar Exam, 60 JOURNAL OF LEGAL EDUCATION 3 (2010) (peer-reviewed) (published as Jane Yakowitz).

BOOKS

BUBLICK, BAMBAUER & ARELLANO, DOBBS ADVANCED TORTS: ECONOMIC AND DIGNITARY TORTS (2d Ed.) (2022).

ESSAYS, CHAPTERS, TECHNICAL PAPERS, AND OTHER WORKS

Sober and Self-Guided Newsgathering, invited chapter in MEDIA AS A GOVERNANCE INSTITUTION (Gus Hurwitz et al., eds., Cambridge University Press, forthcoming 2023).

Conceptions of Fairness in Artificial Intelligence, invited chapter in THE PHILOSOPHICAL FOUNDATIONS OF IT LAW (David Mangan, ed., Oxford University Press, forthcoming 2022).

Reinventing Cambridge Analytica One Good Intention at a Time, LAWFARE (2022).

Platforms: The First Amendment Misfits, 97 INDIANA LAW JOURNAL 1047 (2022) (with J. Rollins & V. Yesue).

Reckless Associations: A New Tort for a New Information Ecosystem, LAWFARE (2022).

Facial Recognition as a Least Bad Option, HOOVER INSTITUTE REPORT (2021).

Choosing Freedom, INQUEST (August 19, 2021) (with S. Mayson, A. Roth, and M. Stevenson).

COVID Apps Are Terrible. They Didn't Have to Be. LAWFARE.COM REPORT (2020) (with Brian Ray).

Plausible Deniability, 2020 PRIVACY IN STATISTICAL DATABASES 91 (2020) (peer-reviewed) (co-authored with David Sidi).

Privacy Versus Research in Big Data, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Evan Selinger et al., eds., Cambridge University Press, 2018).

Sensorship, in RON COLLINS & DAVID SKOVER, ROBOTICA: SPEECH RIGHTS & THE NEW TECHNOLOGIES (Cambridge University Press, 2018).

The Empirical First Amendment, 78 OHIO ST. L. J. 947 (2018) (symposium issue).

Dr. Robot, 51 U.C. DAVIS L. REV. 383 (2017) (symposium issue).

Identifying and Countering Fake News, University of Arizona Privacy & Free Expression White Paper (2017) (with M. Verstraete & D. Bambauer) (to be published in ARIZ. J. EMERGING TECH.).

Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal, George Mason University School of Law Program on Economics & Privacy White Paper (2017).

A Bad Education, 2017 U. ILL. L. REV. 109 (2017) (with J. Loe & D. Winkelman).

Glass Half Empty, 64 UCLA L. REV. DISC. 434 (2016) (invited contribution).

Are Privacy Disclosures Informational or Ideological?, 65 DEPAUL L. REV. 503 (2017) (Clifford symposium issue).

The Relationships Between Speech and Conduct, 49 U.C. DAVIS L. REV. 1941 (2016) (invited response to *Information Fiduciaries and the First Amendment* by Jack Balkin).

Assessing Data Intrusion Threats, SCIENCE (letter) (with D. Barth-Jones et al.) (2015).

All Life Is an Experiment. (Sometimes It's a Controlled Experiment.), 47 LOY. CHI. L. REV. 487 (2015) (symposium issue).

Freedom From Thought, 65 EMORY L. J. 219 (2015) (symposium issue).

Cyber-Exploitation and Distributed Enforcement, B.U. L. REV. ANNEX (November 6, 2015) (with D. Bambauer) (invited response to HATE CRIMES IN CYBERSPACE by Danielle Citron).

Collection Anxiety, 99 CORNELL L. REV. ONLINE 195 (2014) (invited response to *Digital Innocence* by Joshua Fairfield and Erik Luna).

Fool's Gold: An Illustrated Critique of Differential Privacy, 16 VAND. J. ENT. & TECH. L. 701 (2014) (with K. Muralidhar and R. Sarathy).

Vanished: Analyzing Censorship with Google Transparency Data, 18 VA. J. L. & TECH. 137 (2013) (with D. Bambauer).

Defending the Dog, 91 OR. L. REV. 1203 (2013) (symposium issue).

How the War on Drugs Distorts Privacy Law, 64 STAN. L. REV. ONLINE 131 (2012).

SELECTED PRESENTATIONS, COMMITTEES, AND AWARDS

Board Member, TPRC Conference on Communications, Information, and Internet Policy, American University Washington College of Law, Washington, D.C., 2017-present.

Program Committee Member, UNESCO Privacy in Statistical Databases, 2016-present.

Debate: Dobbs and the Potential Implications for Data Privacy, The Federalist Society Regulatory Transparency Project (2022).

Regular guest, *The Cyberlaw Podcast*, Steptoe & Johnson, Washington, D.C. (2020-present).

Reporter, The Collection and Use of Personally Identifiable Data, Uniform Law Commission, 2020-2021.

Debate: Private Control Over Public Discussion, The Federalist Society National Lawyers Convention, Washington, D.C., 2021 (arguing against Eugene Volokh, Randy Barnett, and Adam Candeub in favor of Facebook's and Twitter's ability to restrict and remove content on their platforms).

Distinguished Legal Scholar, awarded to one University of Arizona law faculty member each year for exceptional achievement in research (three year term, 2021-2024).

WeHealth, *Trading Privacy for Effectiveness in Exposure Notifications: A Debate* (with Peter Singer et al.), 2021.

Debate: Today's Distrust in Big Tech Is Healthy, Silicon Flatirons Topics in Law & Technology Event (leading the "opposed" team, which won the Oxford-style debate), Boulder, CO., 2021.

Cats, Cars, and Nazis, Freedom of Expression Scholars Conference Works-in-Progress, Yale Law School, New Haven, CT., 2020.

Privacy & Pandemics: Responsible Uses of Technology & Health Data, Future of Privacy Forum, September 2020.

Privacy and the Pandemic (invited panelist), Electronic Privacy Information Center, June 2020.

How the Pandemic Will Affect Washington's Privacy Policy Debate (invited panelist), Technology Policy Institute, April 2020.

Symposium on Algorithmic Criminal Justice (invited panelist), UCLA College of Law, Los Angeles, CA, January 2020.

Director, Program on Economics & Privacy, George Mason University Antonin Scalia Law School, Arlington, VA, 2018-2019.

Panelist, *Commercial Speech and the First Amendment*, Yale Law School's Abrams Institute for Freedom of Speech, New York, NY, 2019.

Measuring Grossly Excessive Punishment, Criminal Law Works-in-Progress Roundtable, Yale Law School, New Haven, CT., 2019 (invited author).

A Differentially Private Census Bureau?, Population Association of America Annual Conference, Austin, TX, 2019 (invited panelist).

Testimony, *GDPR and CCPA: Opt-Ins, Consumer Control, and the Impact on Competition and Innovation*, Senate Judiciary Committee, Washington, D.C., 2019.

Testimony, *The Impact of Privacy Regulations on Competition and Innovation*, Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century, Washington, D.C., 2018.

Testimony, *Free Speech and Data Privacy*, Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century, Washington, D.C., 2018.

How Speech Libertarianism Serves Progressives, invited response to Michael Seidman, *Can Free Speech Be Progressive?*, 118 COL. L. REV. 2219 (2018), Virtual Roundtable hosted by FIRST AMENDMENT WATCH, 2018.

Machine Influencers and Decision Makers, University of Arizona College of Science Public Lecture Series, Tucson, AZ, 2018 (rebroadcast on AZPM).

Female Labor Participation and the Limits of Law, Governance and the Law, University of Arizona and World Bank Development Economics Workshop, Tucson, AZ, 2017.

Guest blogger, Volokh Conspiracy, THE WASHINGTON POST, August-September 2017.

The Algorithm Game, Privacy Law Scholars Conference, UC Berkeley Law School, Berkeley, CA, 2017.

The First Amendment's Application to Rapidly Developing Information Technologies, The William O. Douglas Annual Lecture, Gonzaga University School of Law, Spokane, WA, 2017.

Google Fellow, Privacy Law Salon, Miami, FL, 2017.

Who Owns Your Data?, Presentation to the Conference of Chief Justices, Scottsdale, AZ, 2017.

Information Libertarianism, Free Expression Scholars Conference, Yale Law School, New Haven, CT, 2016. (plenary session).

Other People's Papers, University of Haifa Law Department Cyberforum, Haifa, Israel, 2016.

Bad Education, University of Haifa Law Department, Haifa, Israel, 2016.

Privacy Versus Research in the Age of Big Data, University of Utah LABS colloquium, Salt Lake City, UT, 2016.

2015-16 Privacy Fellow, George Mason University Law & Economics Center Research Roundtable (supporting experimental research on privacy).

Criminal Justice Roundtable, invited commentary on *The New Surveillance Discretion: Automated Suspicion, Big Data and Policing* by Elizabeth Joh, Vanderbilt University School of Law, Nashville, TN, 2015.

Harry W. Stonecipher Award for top scholarship in communication and free speech law, Association for Education in Journalism and Mass Communication Law & Policy Division, 2015.

Program Chair, TPRC Conference on Communications, Information, and Internet Policy, George Mason University School of Law, Arlington, VA, 2015.

Truth in the Age of Uncertainty, University of Maryland Law School, Baltimore, MD, 2015.

Hassle, Author talk, University of Michigan Law School, Ann Arbor, MI, 2015.

Data, the Police, and the Whole Constitution, University of Texas Faculty Colloquium, Austin, TX, 2015.

Freedom From Knowledge, The 2015 Randolph W. Thrower Symposium, Emory University School of Law, Atlanta, GA, 2015.

The Era of Big Data: Balancing Privacy Rights, Law Enforcement Needs, and Corporate Interests, National Asian-Pacific American Bar Association Annual Conference, Scottsdale, AZ, 2014.

Public Health in the Shadow of the First Amendment, Yale Law School, New Haven, CT, 2014.

Program Vice Chair, TPRC Conference on Communication, Information and Internet Policy, George Mason University School of Law, Arlington, VA, 2014.

Surveillance in the Technological Age: The Case of the NSA, Keynote Address at the International Criminal Law Conference, Babes-Bolyai University, Cluf-Napoca, Romania, 2014.

Is Data Speech?, Yale Law School Information Society Project, New Haven, CT, 2014.

Google Fellow, Privacy Law Salon (invitational event for scholars and industry), Miami, FL, 2014.

When Worlds Collide: Technology, Privacy, and Security, Appellate Judges Education Institute, San Diego, CA, 2013.

The De-Identified Data Commons, United Nations Economic Commission for Europe (Eurostat Work Session), Ottawa, Canada, 2013.

Into the Breach: Introduction to the 2012-2013 National Health Law Moot Court Problem, 34 J. LEG. MED. 337 (2013).

Problem Author, National Health Law Moot Court, Southern Illinois University, Carbondale, IL, 2012 (fictitious civil rights case based on a data breach at a public health clinic).

Seeding the Data Commons: Legal Safe Harbors for Research Data, Think Tank on the Identifiability of Genomic Data and Biospecimens, National Institute of Health / National Cancer Institute, Rockville, MD, 2012.

Invited Debater, *Is Privacy Overhyped?*, The Open Society Institute, New York, NY, 2012.

Invited Panelist, *Balancing Privacy Interests and Innovation*, Law and Information Society Symposium, Fordham Law School, New York, NY, 2012.

Invited Panelist, *Bullying Bans and the First Amendment*, Seton Hall Law School, Newark, NJ, 2012.

Google Fellow, Privacy Law Salon (invitational event for scholars and industry), Miami, FL, 2012.

Invited Speaker, *The Benefits and Risks of De-Identification*, The Future of Privacy Forum, Washington, D.C., 2011.

Tragedy of the Data Commons, The Privacy Working Group Speaker Series, Information Technology and Innovation Foundation, Washington, DC, 2011.

The Illusory Privacy Problem in Sorrell v. IMS Health, Technology Policy Institute, 2011 (technical paper) (with Daniel Barth-Jones).

Invited Interviewee, *Tragedy of the Data Commons*, Surprisingly Free Podcast Series, Mercatus Center, George Mason University, 2011.

Tragedy of the Data Commons, Google Public Policy Speaker Series, Mountain View, CA, 2011.

Moderator and Poster Presentation, *The Secret of My Success: How Status, Prestige, and School Performance Shape Legal Careers*, Conference on Empirical Legal Studies, Yale Law School, New Haven, CT, 2010.

The Secret of My Success: How Status, Prestige, and School Performance Shape Legal Careers, Law & Society Association Annual Meeting, Chicago, IL, 2010.

What Are the Effects of Failing the Bar? An Empirical Study, Law & Society Association Annual Meeting, Denver, CO, 2009.

OP-EDS AND PRESS COVERAGE

Jane Bambauer, *Bills Meant to Check Big Tech's Power Could Lead to More Disinformation*, WASHINGTON POST (June 6, 2022) (with Anupam Chander).

Jane Bambauer, *Letting Police Access Google Location Data Can Help Solve Crimes*, WASHINGTON POST (March 28, 2022) (note: I did not choose the headline).

Timothy B. Lee, *Why the 2020 Census Has 9 Fake People in a Single House*, FULL STACK ECONOMICS (March 7, 2022).

Michael Finnegan, *FBI Says Fortune Seized in Beverly Hills Raid Was Criminals' Loot. Owners Say: Where's the Proof?*, L.A. TIMES (Sept. 19, 2021).

Chris Roberts, *Marijuana Legalization Is Retiring Police Dogs. Why That's Good—And Why All Drug K9 Unites Should Go*, FORBES (May 30, 2021).

George F. Will, *A Cheerleader's Salty Language Gives the Supreme Court a Chance to Bolster the First Amendment*, WASH. POST (April 26, 2021) (describing amicus brief in *Mahonoy Area School Dist. v. B.L.*).

Kashmir Hill, *Your Face Is Not Your Own*, N.Y. TIMES (March 18, 2021).

Alisa Alering, *Are You Ready for the Quantum Internet?*, SCIENCE NODE (September 21, 2020).

Alexei Barrionuevo, *Coronavirus Tracing Apps Are Being Tested Around the World, But Will Concerts Get on Board?*, BILLBOARD.COM (May 28, 2020).

George Will, *A Cheerleader's Salty Language Gives the Supreme Court a Chance to Bolster the First Amendment*, WASHINGTON POST (April 27, 2021).

Jenny McGrath, *Inside the Groundbreaking Plan to Truly Anonymize Your 2020 Census Data*, DIGITAL TRENDS (February 28, 2020).

Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N. Y. TIMES (2019).

Danielle Abril, *Facebook's $5 Billion Privacy Settlement Argued Consumers Weren't Harmed. Experts Think the Damage Was Incalculable*, FORTUNE (2019).

Timmy Broderick, *Privacy, Accuracy, and the Looming 2020 Census*, CHRISTIAN SCIENCE MONITOR (2019).

Campus Free Speech, ARIZONA 360 (April 19, 2019) (interview broadcast on Arizona Public Media).

James Langford, *#GoodLuck: Odds Stacked Against Devin Nunes in His Lawsuit Against Twitter*, WASHINGTON EXAMINER (March 20, 2019) (reproduced in *The Hill*).

Andrew Howard, *UA Professor Cautions Senators to Go Slow in Bid to Protect Personal Data*, CRONKITE NEWS ARIZONA PBS (March 12, 2019).

Justin Sherman, *How to Regulate the Internet Without Becoming a Dictator*, FOREIGN POLICY (quoting *Is Data Speech?*).

Ariel Shapiro, *Trump's SCOTUS Nominee Thinks That ISPs Have First Amendment Rights, Which Could Spell Bad News for Your Privacy*, CNBC.COM (2018).

Tim Steller, *Cochise Officials Pursue Blogger for Publishing Transcript*, ARIZONA DAILY STAR (2017).

Ronald K. Collins, *11 First Amendment Experts Comment on Legality of NYT Release of Trump's Tax Returns*, CONCURRING OPINIONS (2016).

Jacob Gershman, *Free Speech Case About Cash vs. Plastic Store Prices Gests a Supreme Court Review*, WALL ST. J. (2016) (quoting from amici brief for *Expressions Hair Design v. Schneiderman*).

Stephanie Fairyington, *Do You Have a Right to Privacy in Your Marriage?*, TIME (2016).

Christopher Slobogin, *The Definition of Suspicion in an Era of Modern Policing*, JOTWELL (2016) (reviewing my article, *Hassle*).

Fernanda Santos, *Border Patrol Accused of Profiling and Abuse*, N.Y. TIMES (2015).

Connor Harris, *Matters of Mismatch: The Debate over Affirmative Action's Effectiveness*, HARVARD POLITICAL REVIEW (2015) (describing findings from *The Secret of My Success*).

Kathleen Hale, *Glory Johnson Says She Was Victim in Her Altercation with Brittney Griner*, SPORTSILLUSTRATED.COM (2015).

Tim Cushing, *The Government's Antipathy Towards Transparency Has Made FOIA Lawsuits the Default Process*, TECHDIRT (2014).

Driver-Less Cars About a Decade Away, UA Engineer Says, ARIZONA ILLUSTRATED (2014) (television coverage).

Katherine Jacobsen, *Google Challenges Secret Court Over Gag Order*, THE CHRISTIAN SCIENCE MONITOR (2013).

The Bright Side of Telephone Metadata, THE HUFFINGTON POST (2013).

Jerry Brito, *What Europe's 'Right to Be Forgotten' Has in Common with SOPA*, TIME.COM (2012).

More Bad Ideas From the E.U., FORBES.COM (2012).

Leon Neyfakh, *Our Data, Ourselves*, THE BOSTON GLOBE (2011) (describing *Tragedy of the Data Commons* in depth).

L. Gordon Crovitz, *The 0.00002% Privacy Solution*, THE WALL STREET JOURNAL (2011) (quoting *Tragedy of the Data Commons*).

Ashby Jones, *New Study: Forget the Rankings, Just Bring Home Straight A's*, THE WALL STREET JOURNAL LAW BLOG (2010) (describing findings from *The Secret of My Success*).

Terry Baynes, *Don't Sweat Your School's Status*, THE AMERICAN LAWYER (2010) (describing findings from *The Secret of My Success*).

Karen Sloan, *Those Who Never Pass Bar Exam Initially Lag Far Behind Those Who Do*, THE NATIONAL LAW JOURNAL (2010) (describing findings from *Marooned*).

Karen Dybis, *What Happens When You Fail the Bar Exam?*, NATIONAL JURIST (2010) (describing findings from *Marooned*).

SELECTED AMICUS BRIEFS AND PRO BONO WORK

ACLU v. Clearview, No.2020-CH-04353 (IL), Brief of Eugene Volokh, Jane Bambauer, and First Amendment Clinic at Duke Law School in support of defendant Clearview's motion to dismiss arguing that the Illinois Biometric Privacy Act as applied to Clearview is an unconstitutional restriction of speech.

Alabama v. U.S. Department of Commerce, No. 3:21-cv-211-RAH (M.D. Alab.), Brief of Jane Bambauer as Amicus Curiae in support of Alabama (arguing that the use of Differential Privacy to protect privacy in Census Data will needlessly degrade the quality of data used for redistricting and for the enforcement of Voting Rights Act claims).

Hassell v. Bird, No. S235968 (CA), Brief of Amici Curiae First Amendment and Internet Law Scholars in support of appellant, Yelp, Inc. (arguing that the First Amendment and Section 230 of the Communications Decency Act prohibit a court from ordering a non-party Internet intermediary to remove content).

ACLU Foundation of Arizona v. Department of Homeland Security, No. 14-2052 (D. Ariz.), co-plaintiff with Derek Bambauer and ACLU of Arizona in Freedom of Information Act request for documents related to Border Patrol operations in Arizona north of the Mexican border.

Expressions Hair Design v. Schneiderman, No. 15-1391 (U.S. Supreme Court), Brief of Amici Curiae First Amendment Scholars in support of petitioner's writ of certiori (arguing that credit card surcharge bans, as applied, are unconstitutional restrictions on commercial speech).

Sorrell v. IMS Health Inc., 564 U.S. 552 (2011), Brief of Dr. Khaled El Emam and Jane Yakowitz as Amici Curiae in support of IMS Health (arguing that HIPAA-compliant pharmacy data pose little risk of re-identification to the patients).

EXPERT WITNESS TESTIMONY

Sander v. The Regents of the University of California, Case No. RG18-928614 (Sup. Ct. Cal. 2021) (deposition testimony).

Exhibit B:

Attachment B: Documents & Files Considered

Description / Beg Bates No.	End Bates No.
2020-12-03 (Dkt 1) Class Action Complaint	n/a
2021-09-10 (Dkt 60) Defendant's Answer and Affirmative Defenses to Plaintiffs' Class Action Complaint	n/a
2022-04-04 Thomson Reuters Responses to Plaintiffs' First Set of Interrogatories (with Attachment A)	n/a
2022-06-01 Expert Report of Professor Joseph Turow	n/a
2022-05-16 Steve Fox Deposition Transcript	n/a
2022-08-10 Cat Brooks Deposition Transcript	n/a
2022-08-18 Rasheed Shabazz Deposition Transcript	n/a
2022-08-26 Joseph Turow Deposition Transcript	n/a
PLAINTIFFS_005538	PLAINTIFFS_005547
PLAINTIFFS_005548	PLAINTIFFS_005580
PLAINTIFFS_005581	PLAINTIFFS_005607
PLAINTIFFS_005608	PLAINTIFFS_005617
PLAINTIFFS_005618	PLAINTIFFS_005652
PLAINTIFFS_005653	PLAINTIFFS_005661
PLAINTIFFS_005662	PLAINTIFFS_005703
PLAINTIFFS_010275	PLAINTIFFS_010275
PLAINTIFFS_011040	PLAINTIFFS_011125
PLAINTIFFS_011126	PLAINTIFFS_011253
PLAINTIFFS_011254	PLAINTIFFS_011274
PLAINTIFFS_011275	PLAINTIFFS_011312
PLAINTIFFS_011314	PLAINTIFFS_011314
TR-BROOKS000011	TR-BROOKS000028
TR-BROOKS000056	TR-BROOKS000059
TR-BROOKS000075	TR-BROOKS000076
TR-BROOKS000082	TR-BROOKS000086
TR-BROOKS000482	TR-BROOKS000484
TR-BROOKS000610	TR-BROOKS000624
TR-BROOKS000746	TR-BROOKS000749
TR-BROOKS000761	TR-BROOKS000765
TR-BROOKS000766	TR-BROOKS000770
TR-BROOKS000776	TR-BROOKS000780
TR-BROOKS000806	TR-BROOKS000812
TR-BROOKS000841	TR-BROOKS000844

Attachment B: Documents & Files Considered

Description / Beg Bates No.	End Bates No.
TR-BROOKS000860	TR-BROOKS000864
TR-BROOKS000876	TR-BROOKS000879
TR-BROOKS000896	TR-BROOKS000897
TR-BROOKS001097	TR-BROOKS001099
TR-BROOKS001168	TR-BROOKS001169
TR-BROOKS001261	TR-BROOKS001308
TR-BROOKS001312	TR-BROOKS001327
TR-BROOKS001363	TR-BROOKS001482
TR-BROOKS001564	TR-BROOKS001565
TR-BROOKS001688	TR-BROOKS001691
TR-BROOKS001692	TR-BROOKS001695
TR-BROOKS001816	TR-BROOKS001819
TR-BROOKS001855	TR-BROOKS001858
TR-BROOKS001872	TR-BROOKS001873
TR-BROOKS001985	TR-BROOKS001987
TR-BROOKS001988	TR-BROOKS001990
TR-BROOKS001991	TR-BROOKS001994
TR-BROOKS001995	TR-BROOKS001996
TR-BROOKS001999	TR-BROOKS002002
TR-BROOKS002003	TR-BROOKS002005
TR-BROOKS002051	TR-BROOKS002053
TR-BROOKS002086	TR-BROOKS002093
TR-BROOKS002101	TR-BROOKS002104
TR-BROOKS002239	TR-BROOKS002242
TR-BROOKS002251	TR-BROOKS002252
TR-BROOKS002253	TR-BROOKS002254
TR-BROOKS002292	TR-BROOKS002294
TR-BROOKS003259	TR-BROOKS003261
TR-BROOKS003512	TR-BROOKS003527
TR-BROOKS003528	TR-BROOKS003529
TR-BROOKS003530	TR-BROOKS003532
TR-BROOKS003533	TR-BROOKS003535
TR-BROOKS003536	TR-BROOKS003542
TR-BROOKS003543	TR-BROOKS003543
TR-BROOKS003544	TR-BROOKS003544
TR-BROOKS003545	TR-BROOKS005219
TR-BROOKS005220	TR-BROOKS008254

Attachment B: Documents & Files Considered

Description / Beg Bates No.	End Bates No.
TR-BROOKS008255	TR-BROOKS008276
TR-BROOKS008277	TR-BROOKS008277
TR-BROOKS008278	TR-BROOKS008278
TR-BROOKS008279	TR-BROOKS008279
TR-BROOKS008280	TR-BROOKS008308
TR-BROOKS008309	TR-BROOKS008318
TR-BROOKS008319	TR-BROOKS008319
TR-BROOKS008320	TR-BROOKS008320
TR-BROOKS008321	TR-BROOKS008321
TR-BROOKS008322	TR-BROOKS008323
TR-BROOKS008324	TR-BROOKS008324
TR-BROOKS008325	TR-BROOKS008325
TR-BROOKS008326	TR-BROOKS008341
TR-BROOKS008342	TR-BROOKS008343
TR-BROOKS008344	TR-BROOKS008350
TR-BROOKS008351	TR-BROOKS008352
TR-BROOKS008353	TR-BROOKS008718
TR-BROOKS008719	TR-BROOKS008740
TR-BROOKS008741	TR-BROOKS008741
TR-BROOKS008742	TR-BROOKS008742
TR-BROOKS008743	TR-BROOKS008743
TR-BROOKS008744	TR-BROOKS008744
TR-BROOKS008745	TR-BROOKS008745
TR-BROOKS008746	TR-BROOKS008746
TR-BROOKS008747	TR-BROOKS008758
TR-BROOKS008759	TR-BROOKS008759
TR-BROOKS008812	TR-BROOKS008812
TR-BROOKS008813	TR-BROOKS008813
TR-BROOKS008814	TR-BROOKS008814
TR-BROOKS008815	TR-BROOKS008815
TR-BROOKS008816	TR-BROOKS008826
TR-BROOKS008827	TR-BROOKS008829
TR-BROOKS008830	TR-BROOKS008830
TR-BROOKS010211	TR-BROOKS010218
TR-BROOKS010219	TR-BROOKS010221
TR-BROOKS010222	TR-BROOKS010222
TR-BROOKS010223	TR-BROOKS010223

Attachment B: Documents & Files Considered

Description / Beg Bates No.	End Bates No.
TR-BROOKS010224	TR-BROOKS010233
TR-BROOKS010234	TR-BROOKS010234
TR-BROOKS010235	TR-BROOKS010235
TR-BROOKS013534	TR-BROOKS013535
TR-BROOKS013536	TR-BROOKS013538
TR-BROOKS013638	TR-BROOKS013640
TR-BROOKS013720	TR-BROOKS013722
TR-BROOKS018313	TR-BROOKS018313
TR-BROOKS018645	TR-BROOKS018645
TR-BROOKS030530	TR-BROOKS030535
TR-BROOKS035826	TR-BROOKS035829
TR-BROOKS035870	TR-BROOKS035871
TR-BROOKS038817	TR-BROOKS038835
TR-BROOKS039301	TR-BROOKS039307
TR-BROOKS041418	TR-BROOKS041426
TR-BROOKS041734	TR-BROOKS041735
TR-BROOKS044782	TR-BROOKS044782
TR-BROOKS046629	TR-BROOKS046629
TR-BROOKS046643	TR-BROOKS046644
TR-BROOKS046645	TR-BROOKS046646
TR-BROOKS046655	TR-BROOKS046655
TR-BROOKS049485	TR-BROOKS049485
TR-BROOKS049907	TR-BROOKS049907
TR-BROOKS055702	TR-BROOKS055703
TR-BROOKS055720	TR-BROOKS055721
TR-BROOKS055730	TR-BROOKS055732
TR-BROOKS055733	TR-BROOKS055734
TR-BROOKS055737	TR-BROOKS055738
TR-BROOKS055754	TR-BROOKS055755
TR-BROOKS055786	TR-BROOKS055787
TR-BROOKS055803	TR-BROOKS055804
TR-BROOKS055844	TR-BROOKS055845
TR-BROOKS055887	TR-BROOKS055887
TR-BROOKS055888	TR-BROOKS055888
TR-BROOKS057002	TR-BROOKS057018
TR-BROOKS060012	TR-BROOKS060013
TR-BROOKS070585	TR-BROOKS070592

Attachment B: Documents & Files Considered

Description / Beg Bates No.	End Bates No.
TR-BROOKS127726	TR-BROOKS127847
TR-BROOKS146612	TR-BROOKS146615
TR-BROOKS148319	TR-BROOKS148322
TR-BROOKS165057	TR-BROOKS165058
TR-BROOKS272512	TR-BROOKS272512
TR-BROOKS272513	TR-BROOKS272520
TR-BROOKS295350	TR-BROOKS295350
TR-BROOKS304709	TR-BROOKS304720
TR-BROOKS305113	TR-BROOKS305117

In addition to the cited articles and materials, I considered:

1. https://www.google.com/search?q=cat+brooks&oq=cat+brooks&aqs=chrome..69i57j46i20i131i263i433i512j35i39j0i20i263i512j0i512l6.4135j0j7&sourceid=chrome&ie=UTF-8#ip=1

2. https://www.google.com/search?q=rasheed+shabazz&sxsrf=ALiCzsaJMNorTZlshznsr9YgR5aBS4eV4Q%3A1662586881434&ei=ARAZY66WGv-fkPIPqJyNuAk&ved=0ahUKEwjumufj0oP6AhX_D0QIHShOA5cQ4dUDCA8&uact=5&oq=rasheed+shabazz&gs_lcp=Cgdnd3Mtd2l6EAMyBAgjECcyBAgAEB4yBAgAEB4yBggAEB4QBTIFCAAQhgMyBQgAEIYDOgQIABBDOgQILhBDOhEILhCABBCxAxCDARDHARDRAzoFCC4QkQI6BQgAEJECOgcIABCxAxBDOggIABCABBCxAzoKCC4QxwEQrwEQQzoKCAAQsQMQgwEQQzoLCAAQgAQQsQMQiwM6BwgAEEMQiwM6CAgAEIAEEIsDOgoILhCxAxBDEIsDOg4IABCABBCxAxCDARCLAzoHCC4QsQMQQzoFCAAQgAQ6CAguEIAEELEDOgcIABCABBAKOhAILhCABBCHAhDHARCvARAUOgsILhCABBCxAxDUAjoFCC4QgAQ6BggAEB4QBzoHCC4QsQMQDToKCC4QsQMQ1AIQDToECC4QDToECAAQDToHCCMQsAIQJ0oECEEYAEoECEYYAFAAWOMxYK80aABwAHgAgAHKAYgBlBGSAQYyLjEzLjGYAQCgAQG4AQLAAQE&sclient=gws-wiz

3. https://oaklandvoices.us/author/rasheed/

4. https://caselaw.findlaw.com/ga-court-of-appeals/1174544.html

5. William L. Prosser, Privacy, 48 CAL. L. REV. 383, 396 (1960).

6. Joseph E. Stiglitz, The Contributions of the Economics of Information to Twentieth Century Economics, 115 Q. J. ECON. 1441 (2000).

7. Jin-Hyuk Kim & Liad Wagman, Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis, 46 RAND J. OF ECON. 1 (2015).

8. Wendy Edelberg, Risk-Based Pricing of Interest Rates for Consumer Loans, 53 J. MONETARY ECON. 2283 (2006).

9. Inmaculada Hernandez & Yuting Zhang, Using Predictive Analytics and Big Data to Optimize Pharmaceutical Outcomes, 74 AM. J. HEALTH-SYST PHARM. 1494 (2017).

10. Daniel J. Solove & Danielle Keats Citron, Privacy Harms, work in progress available at https://scholarship.law.gwu.edu/faculty_publications/1534/.

11. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK (2007).