2022

The Limitations of Privacy Rights

Daniel J. Solove

The Limitations of Privacy Rights

by

Daniel J. Solove

February 2022

ABSTRACT

Individual privacy rights are often at the heart of information privacy and data protection laws. The most comprehensive set of rights, from the European Union's General Data Protection Regulation (GDPR), includes the right to access, right to rectification (correction), right to erasure, right to restriction, right to data portability, right to object, and right to not be subject to automated decisions. Privacy laws around the world include many of these rights in various forms.

In this article, I contend that although rights are an important component of privacy regulation, rights are often asked to do far more work than they are capable of doing. Rights can only give individuals a small amount of power. Ultimately, rights are at most capable of being a supporting actor, a small component of a much larger architecture. I advance three reasons why rights cannot serve as the bulwark of privacy protection. First, rights put too much onus on individuals when many privacy problems are systematic. Second, individuals lack the time and expertise to make difficult decisions about privacy, and rights cannot practically be exercised at scale with the number of organizations than process people's data. Third, privacy cannot be protected by focusing solely on the atomistic individual. The personal data of many people is interrelated, and people's decisions about their own data have implications for the privacy of other people.

The main goal of providing privacy rights aims to provide individuals with control over their personal data. However, effective privacy protection involves not just facilitating individual control, but also bringing the collection, processing, and transfer of personal data under control. Privacy rights are not designed to achieve the latter goal; and they fail at the former goal.

After discussing these overarching reasons why rights are insufficient for the oversized role they currently play in privacy regulation, I discuss the common privacy rights and why each falls short of providing significant privacy protection. For each right, I propose broader structural measures that can achieve its underlying goals in a more systematic, rigorous, and less haphazard way.

THE LIMITATIONS OF PRIVACY RIGHTS
by Daniel J. Solove[1]

[1] John Marshall Harlan Research Professor of Law, George Washington University Law School. I would like to thank my research assistants Kimia Favagehi, Shushan Gabrielyan, and Jean Hyun for excellent work. Thanks to Danielle Citron, Don Clarke, Woodrow Hartzog, Chris Hoofnagle, Paul Schwartz, and Ari Waldman for helpful feedback.

INTRODUCTION

Individual privacy rights are enshrined at the heart of most information privacy and data protection laws.[2] Countless privacy laws in the United States and worldwide provide individuals with rights in their personal data, such as a right to information about their data, rights to access and correct their data, a right to delete their data, and a right to opt out of certain uses of their data, among others.

Generally, there are two broad types of substantive elements in privacy laws: rights and duties. Rights are typically invoked by individuals to have knowledge and control regarding their personal data. Duties involve requirements for entities that collect, use, or transfer personal data.

Rights are the centerpiece of many privacy laws. Many duties of privacy laws are designed to help administer the rights that the law provides. For example, the European Union's the General Data Protection Regulation (GDPR) provides for seven individual rights. More than 140 countries now have comprehensive privacy laws,[3] most of which were designed based on the GDPR or its predecessor, the EU Data Protection Directive. Under the GDPR and many other laws, data subjects may make rights requests called "data subject access requests" (DSARs). Complying with DSARs requires being able to locate relevant personal data to provide to data subjects, verify the identities of data subjects, process requests to delete or to stop processing data, and so on. Many elements of privacy laws involve mechanisms to ensure that organizations effectively administer these rights.

Privacy laws have always relied heavily on rights, and the trend is increasing. Comprehensive privacy laws worldwide have typically included many privacy rights.[4] Many privacy laws in the United States rely heavily on privacy rights. For example, under the California Consumer Privacy Act's (CCPA), the central set of protections involve a robust right to information – providing individuals with extensive information about the collection and use of their personal data – as well as a strong right to opt out and a right to delete data.[5] A key goal of the law involves "putting consumers back in charge of their own data."[6]

A main impetus for rights involves a desire to address the problem that individuals lack much power in their relationships with the gigantic organizations that have massive digital dossiers of their personal data.[7] As stated by the famous 1973 government report on privacy that spawned the principles animating many privacy rights, computer databases are upending "the mutuality of record-generating relationships to assign the institution a unilateral role in making decisions about

[2] In this article, I use terms "information privacy" and "data protection" synonymously. The EU uses the term "data protection,' as do many laws based on EU law. In the US, the term "privacy" is predominantly used.

[3] Katitza Rodriguez and Veridiana Alimontis, *A Look-Back and Ahead on Data Protection in Latin America and Spain,* EFF (Sept. 21, 2020), https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain.

[4] *See* Jamaica, Data Protection Act. *See also* Graham Greenleaf, *Jamaica Adopts a Post-GDPR Data Privacy Law*, 167 Privacy Laws & Business International Report 1, 5-8 (Aug. 16, 2020), https://ssrn.com/abstract=3712745.

[5] CCPA 1798.105 (right to delete), 1798.106 (right to correct), 1798.110 & 1798.115 (right to know), 1798.120 (right to opt out of sale or sharing), 1798.121 (right to limit use or disclosure of sensitive info).

[6] Californians for Consumer Privacy, https://www.caprivacy.org/.

[7] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

the content and use of its records about individuals."[8] As the report aptly observed, individuals are increasingly powerless and vulnerable as their personal data is gathered, aggregated, transferred, analyzed, and used to make decisions affecting their lives. I will call this problem "data disempowerment." The response of privacy laws has been to attempt to put individuals back in control over their personal data by giving them rights.

In this article, I argue that although rights are an important component of privacy regulation, rights are often asked to do far more work than they are capable of doing. Privacy rights cannot solve the problem of data disempowerment. The ability of individuals to exercise control over their personal data is quite limited; there is a ceiling to individual control. Rights can give people a small amount of power in a few isolated instances, but this power is too fragmented and haphazard to have a meaningful impact on protecting privacy. Ultimately, rights are at most capable of being a supporting actor, a small component in a much larger architecture.

I advance three reasons why rights are quite limited as an effective way to protect privacy. First, many rights are not practical for individuals to exercise. Rights put too much of the onus on individuals to fight a war that they cannot win. Attempting to use privacy rights as a primary way to protect privacy is akin to arming an individual with a dagger to fight an entire army. People cannot exercise their rights in the kind of systematic way necessary to have a meaningful impact.

Second, privacy rights involve "privacy self-management," a term I have used to describe an approach to privacy that seeks to empower individuals to take control of their personal data.[9] Unfortunately, people lack the expertise to make meaningful choices about their data. These choices involve weighing the costs and benefits of allowing the collection, use, or transfer of their data. Although the benefits are immediate and concrete, the costs involve risks that are more abstract and speculative. Individuals lack the expertise to understand and assess the risks. Even experts lack the knowledge about how the data will be used in the future and how algorithms will reach decisions regarding the data.

Third, privacy cannot be protected at the level of the atomistic individual. Individuals make privacy choices that have effects not just for themselves but for many others. For example, sharing one's genetic data also shares the genetic data of one's family members. In today's world of machine learning, the personal data of everyone in a data set has an impact on the decisions that the system makes.

To address these limitations with privacy rights, I contend that rights should not be used as a primary means to regulate privacy. Privacy is about power.[10] Rights cannot empower individuals enough to equalize the power imbalance between individuals and the organizations that collect and use their data. Effective privacy protection involves not just facilitating individual control but also bringing the collection, processing, and transfer of personal data under control. These two

[8] SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 40 (1973).

[9] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013).

[10] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy,* 53 Stan. L. Rev. 1393, 1413-30 (2001) (describing different types of power involved with privacy).

forms of control – individuals *having control* and the data ecosystem *being under control* – are very different, but they are often conflated in privacy policymaking. Individual control is important, but it is only achievable in a limited way. The more practical and effective aim is to bring the data ecosystem under better control.

Thus, to be effective, privacy laws must augment rights with broader measures that are more societal and architectural in nature. For example, privacy rights grant individuals the right to correct errors in their records. A more structural measure involves ensuring that organizations carefully carry out their duty to maintain accurate records. In contrast to rights, structural measures do not rely upon on individuals as the engine of privacy protection.

This article proceeds in three parts. Part I traces the development of privacy rights. Part II discusses the reasons why privacy rights are limited in the role they can play in privacy protection. Part III analyzes each of the main types of privacy rights, discusses the benefits and shortcomings of each, and sets forth the structural measures that privacy laws should require.

I. THE RISE OF PRIVACY RIGHTS

Privacy rights have long been a central component of privacy regulation. In contrast to Constitutional rights, privacy rights in statutes can apply to private or public sector organizations depending upon the statutory scope. In many instances, privacy rights are inalienable – people cannot agree to relinquish them, but the rights must often be exercised or invoked.

Privacy rights in statutes began to emerge in the 1970s in legislation in the US and Europe. For example, in 1970, the Fair Credit Reporting Act (FCRA), was passed in the US.[11] The FCRA provided for several individual rights including right of access and correction, among others.[12]

In 1973, a report by the U.S. Department of Health, Education, and Welfare (HEW) noted concerns about the increasing proliferation of digital record systems and stressed the importance of ensuring that individuals have "a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it."[13] The HEW report articulated one of the earliest sets of Fair Information Practice Principles (FIPPs) which proposed individual rights to know about the data being collected and its intended use, to correct errors in records, and to prevent new secondary uses of personal data.[14]

During the 1970s and 1980s, countless privacy laws were passed in the US and EU, and nearly all of them contained rights, especially the rights to access and

[11] Fair Credit Reporting Act, 15 U.S.C. §1681b.
[12] *Id.*
[13] *Id.* at 40-41.
[14] SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 41–42 (1973). A year earlier, a similar report by the Younger Committee in Great Britain, articulated a set of 10 principles, many of which were similar to the HEW principles, although none of the Younger principles were cast in terms of providing rights to individuals. *See* Robert Gellman, *Fair Information Practices: A Basic History - Version 2.20,* at 5-6 (2021), https://ssrn.com/abstract=2415020. In 1980, the OECD Privacy Guidelines expanded the FIPPs into eight principles. Org. for Econ. Co-operation and Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

correction.[15]

In the 1980s, many Latin American countries embraced a core set of privacy rights in their constitutions known as the "writ of habeas data."[16] The writ's name means "you have the data."[17] Habeas data rights first appeared in 1988 in Brazil's constitution and soon spread to other countries, such as Colombia (1991), Paraguay (1992), Peru (1995), Argentina (1994), and Ecuador (1996).[18] Many Latin American countries enacted comprehensive privacy laws starting in the late 1990s and continuing on robustly through the early 21st century. Habeas data evolved into a core group of privacy rights referred to as the "ARCO" rights, named for the first letter of each.[19] These rights include:

- *Right to Access.* This right involves direct access to one's records. It is often combined with the right to information.

- *Right to Rectification.* This right, also called the right to "correction," involves one's ability to correct errors in one's records.

- *Right to Cancellation.* This right, also known as the right to "erasure" or "deletion," involves one's ability to have data deleted from one's records.

- *Right to Opposition.* This right, also knowns as the right to "restriction" or "object," involves one's ability to object to and stop the processing of personal data. In the EU, the right to object and the right to restriction are bifurcated into two separate rights.

In the US, most laws provided rights to information, access, and correction, but not many other rights. Instead, many US laws provided individuals with rights to opt out or opt in to the collection and use of their data.[20]

Back over in the EU, the Data Protection Directive of 1995 included the most robust set of rights thus far in privacy laws:

- Right to Information
- Right to Access
- Right to Rectification
- Right to Restriction
- Right to Erasure
- Right to Object
- Right to Not Be Subject to Automated Decisions[21]

---

[15] For a timeline of the history of privacy law, including when major laws were passed, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 8-13 (2019).

[16] Andrés Guadamuz, *Habeas Data vs the European Data Protection Directive*, 2001 J. Info. L. & Tech. Issue 3 (2001); Sarah L. Lode, *"You Have the Data"...The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?*, 94 Ind. L.J. Supplement 41 (2019).

[17] Josiah Wolfson, *The Expanding Scope of Human Rights in a Technological World - Using the Inter-American Court of Human Rights to Establish a Minimum Data Protection Standard Across Latin America*, 48 U. Miami Inter-American L. Rev. 206 (2017).

[18] Andrés Guadamuz, *Habeas Data vs the European Data Protection Directive*, 2001 J. Info. L. & Tech. Issue 3 (2001).

[19] Arturo J. Carrillo *Follow the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America*, Minn. J. Int'l L. (forthcoming 2021).

[20] *See infra* at _.

[21] European Union Data Protection Directive, Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

In 2014, the European Court of Justice (CJEU) issued a notable decision declaring that individuals had a right to demand that search engines not report certain data about them in searches.[22] The CJEU derived this right from the right to erasure, and this right has become known as the "right to be forgotten."

In 2016, the EU enacted the General Data Protection Regulation (GDPR), which supersedes the Data Protection Directive.[23] In Chapter 3, at Articles 12-22, the GDPR provided all of the Directive's rights and added a right to data portability.[24] The full set of GDPR rights includes:

- *Right to Information.* As set forth in Articles 13 and 14, this right involves a right to obtain information about the types of personal data that are collected about a person and how that data is processed.[25]

- *Right to Access.* At Article 15, the GDPR provides individuals with a right to have direct access to their records.[26]

- *Right to Rectification.* The GPPR Article 16 provides a right to correct one's records as well as add information to an incomplete record.[27]

- *Right to Erasure.* Article 17 of the GDPR provides a right to have data removed from records under certain circumstances. This right also encompasses the "right to be forgotten," which is actually a different right, as it does not involve the deletion of data but instead a right to obscurity.[28]

- *Right to Restriction.* Article 18 of the GDPR enables an individual to demand that organizations stop processing their data. This right often works in tandem with the right to object in Article 21.[29]

- *Right to Data Portability.* Article 20 provides for a right to data portability. This right is a spinoff of the right to access, as it requires access to one's records in a commonly-used format. [30]

- *Right to Object.* Under Article 21 of the GDPR, individuals have a right to object to the processing of their personal data. [31]

- *Right to Not Be Subject to Automated Decisions.* Article 22 of the GDPR provides for transparency regarding automated decisionmaking and a right to not be subject to a "decision based solely on automated processing, including

[22] Google Spain SL v. Agencia Española de Protección de Datos, in the European Court of Justice, Case C-131/12, 2014 E.C.R. 317.
[23] Regulation (EU) 2016/679 (General Data Protection Regulation).
[24] GDPR art. 12-22.
[25] GDPR art. 13-14.
[26] GDPR art. 15.
[27] GDPR art. 16.
[28] GDPR art. 17.
[29] GDPR art. 18.
[30] GDPR art. 20.
[31] GDPR art. 21.

> profiling." The right includes the ability to "obtain human intervention" and to "contest the decision."[32]

The slate of rights in the GDPR is the most comprehensive set of rights among privacy laws worldwide. Only a few laws have all the rights in the GDPR. But many laws passed after the GDPR are including more of the GDPR rights, and existing laws are being amended to add additional GDPR rights.

In the US, the latest chapter in privacy regulation has been a burgeoning series of broad privacy laws enacted by the states. The trend began in 2018 with the California Consumer Privacy Act (CCPA). The CCPA contained rights to information, deletion (erasure) and data portability. In 2020, the California Privacy Right Act (CCPA), which amended the CCPA to add a right to correction and a right to limit the use and disclosure of sensitive personal information (akin to a right to restriction).

Other states have followed in California's footsteps. Enacted in 2021, Virginia's Consumer Data Protection Act (VCDPA) provides rights to information, access, correction, deletion, data portability, and opt out.[33] Also enacted in 2021, Colorado's Privacy Rights Act provides a similar set of rights.[34] These laws are primarily rights-based approaches, as they rely heavily on individuals exercising rights to learn about how their data is being collected and used and exercise rights to opt out or delete their data. The laws have several other non-rights-based provisions, many of which involve requirements to facilitate administering rights. The clear center of gravity in these laws is providing rights for consumers to exercise.

Early enforcement of the CCPA demonstrates that rights are the main focus. In a press release describing enforcement efforts for the first year of CCPA enforcement, the California Attorney General emphasized its focus on the "groundbreaking rights" of the CCPA and "urged more Californians to take advantage of their new rights."[35] The case examples provided in the press release all focused on rights violations, such as failing to notify consumers of certain uses of their data, failing to provide a notice when requiring consumers provide data to participate in a loyalty program, failing to respond to individual requests in a timely manner, and failing to have an opt out link on the company's homepage.[36] On a page listing examples of its enforcement actions, the California Attorney General's examples mostly include non-compliant privacy notices, failure to have opt out links, and failure to respond to consumer rights requests.[37] Except for a few cases involving non-compliant service provider contracts, the vast bulk of the enforcement involves making sure companies minister to individual rights.

Enforcement's focus on rights is not surprising. Many violations come to the attention of regulations by way of individual complaints, and rights violations are

---

[32] GDPR art. 22.
[33] Virginia Consumer Data Protection Act, S.B. 1392 (2021).
[34] Colorado Privacy Rights Act, Bill 6-1-1304.
[35] Press Release, *Attorney General Bonta Announces First-Year Enforcement Update on the California Consumer Privacy Act, Launches New Online Tool for Consumers to Notify Businesses of Potential Violations* (July 19, 2021), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-first-year-enforcement-update-california.
[36] *Id.*
[37] Office of the California Attorney General, *CCPA Enforcement Case Examples*, https://oag.ca.gov/privacy/ccpa/enforcement.

the type of overt violation that is likely to be readily caught. Many of the other privacy violations not involving the administration of rights occur in the shadows; they are much harder to discover.

II. PROBLEMS AND SHORTCOMINGS

Privacy rights are a fundamental part of most privacy laws. Rights are laudable because they can give people the ability to have a small amount of knowledge and power. But rights cannot provide a more systematic protection of privacy for individuals, let alone for society.

In this Part, I advance three arguments to support this contention. First, rights present individuals with an endless burden of chores. People are provided with something to do, so they feel as though they are in control. Unfortunately, this control is often illusory. Rights are often difficult and time-consuming to invoke, so they might be effective for occasional use, but not for contending with for the hordes of companies that are processing people's data.[38] Privacy rights do not scale.

Second, people are ill-equipped to engage in privacy self-management. Even if people were able to free up hundreds of hours each year to use their rights with all the organizations processing their data, people lack sufficient understanding about the complexities of privacy to make meaningful decisions about the exercise of their rights.[39]

Third, rights have too individualistic a focus to address the societal dimensions of privacy. Individual privacy decisions affect not just themselves. Much personal data is shared between people, not "owned" by just one individual. Personal data is also interrelated; each person's data affects inferences and decisions not just about that person but about many other people.

A. AN ENDLESS BURDEN OF CHORES

On the surface, privacy laws that give people rights appear to empower people, but in reality, these rights are just shiny tools that most people lack the time to use frequently and the knowledge to use effectively.

Even worse than creating a mirage of control and empowerment, rights can lead to the unfair blaming of individuals when they fail to exercise their rights. The onus is placed on individuals to take action, and when individuals end up not doing so, some commentators declare that this is evidence that people do not care about privacy.[40] Policymakers can pat themselves on the back and claim that they did something to protect privacy, but they have merely armed people with a tiny dagger to slay a vast army – a quest that is doomed to failure.

In many cases, an individual must exercise not just one right but several rights. These multiple rights must be exercised with hundreds if not thousands of organizations. Even when a person exercises rights with each organization, the

[38] Solove, *Privacy Self-Management, supra* note _, at X.
[39] Daniel J. Solove, *The Myth of the Privacy Paradox,* 89 Geo. Wash. L. Rev. 1 (2021); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013).
[40] Solove, *Privacy Paradox*, *supra* note _, at X.

data that these organizations gather and the uses of the data change over time. For example, new information is constantly being added to a person's credit report. Thus, individuals must not just exercise rights once for each consumer reporting agency, but also must do so on a routine basis, perhaps even daily. This would be a challenging task if consumer reporting agencies were the only organizations that gathered and used people's data. But there are hundreds, perhaps thousands, of such organizations. Policing one's records across all these organizations on a frequent basis would be a tough job for a large team of full-time workers; there is no plausible way for a lone individual to exercise all of the rights provided by various privacy laws in a meaningful systematic way.

In the end, rights often fail to empower individuals. Instead, rights end up as mere chores that are unpaid, tedious, and time-consuming. Rights are impossible to exercise in the kind of systematic way that will actually control the way that people's data is collected, processed, and transferred.

B. PROBLEMS WITH PRIVACY SELF-MANAGEMENT

The overarching goals of rights are to empower individuals to control their data. To be truly empowered, people should be able to make appropriate cost-benefit risk decisions about the collection, use, or transfer of their data. On the surface, privacy rights appear to be empowering. Rights are thus a go-to for many privacy laws. But rights fail because people just do not know enough and cannot know enough to make good cost-benefit decisions about their data.[41]

With many privacy decisions, the benefits are immediate and concrete. People can receive access to entertainment, news, and information. They can obtain great services and products. They can use convenient and useful technologies. On the privacy side is a risk that is often vague, abstract, and speculative.

Even without the scaling problems, rights are doomed to fail. People cannot use rights in a meaningful way even if they had adequate time and attention to devote to exercising their rights. Rights often give people only perfunctory control, not meaningful control. People receive information, notices, and a few limited choices such as to opt out or object. But they often are rather powerless to do much about the judgments being made about them based on their data.[42]

Compounding these difficulties is the fact that the implications of allowing the collection, use, or dissemination of various pieces of data constantly changes and evolves. With each additional piece of data, the privacy risks change. More data revealed can lead to more data combined, which can give rise to inferences that generate secondary data about people.[43] New uses change the risk.

Even the same piece of data evolves in its risks. For example, today's photo is more revealing than yesterday's photo. A photo in the past would just reveal what was

[41] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV 1879 (2013).

[42] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2007). This problem is exacerbated by the use of artificial intelligence, which often results in decisions made without due process or being heard. Evelyn Douek, *Facebook's "Oversight Board:" Move Fast with Stable Infrastructure and Humility*, 21 N.C. J.L. & Tech. 1, 13 (2019).

[43] Alicia Solow-Niederman, *Information Privacy and the Inference Economy* (Aug. 5, 2021) (draft on file with author).

captured in the photo. Today, a photo includes extensive metadata about geolocation, time, and other things. The ability to identify people, items, and places in the photo is vastly enhanced. The privacy risks of sharing a photo are entirely different from the quaint old days when a photo was just a photo, not a treasure trove of data. People are often unaware of how much data they are sharing when they share a photo. More broadly, people do not realize the full story of what is going on with their data, and without this understanding, people cannot effectively use their rights to gain control of their data.

Photos are just the tip of the iceberg. Data begets data; it multiples like mice. The documentary *Don't F**k with Cats* illustrates how much more one can learn from data today than before.[44] A disgruntled man posted online videos of his killing of kittens. A group of outraged people who saw the video attempted to identify the killer. The amateur sleuths were able to analyze various items and other things in the video to figure out more information about the killer. As they narrowed in on the killer, they were able to find photographs of him, from which they were eventually able to identify where he lived from the background of the photos and using Google Maps. They were able to coordinate and share information via the Internet. Digital technologies enabled them to figure out a lot more than they would have been able to figure out circa 1980 or 1990 or even 2000. The documentary shows how small pieces of data can be combined and analyzed to reveal a lot more information. Technology is amplifying this process.

People are not data scientists. They have trouble understanding the implications of their personal data at face value, let alone the downstream uses and secondary data that can be generated. Rights can help put people in a cockpit with a lot of buttons, levers, settings, toggles, and choices, but if people do not know how to fly the plane, these controls are meaningless.

C. THE SOCIETAL DIMENSIONS OF PRIVACY

Another limitation of privacy rights is that they depend upon the actions of atomistic individuals. Protecting privacy cannot be accomplished solely on an individualized level, as there are societal implications for many decisions that people make regarding personal data.

There are several distinct yet related points involved with the societal dimension of privacy: (1) individual privacy has a social value because protecting it contributes to societal goals; (2) personal data is often shared between people rather than owned exclusively by one individual; and (3) with artificial intelligence, machine learning, and algorithmic decisionmaking, personal data is interrelated, making an individual's privacy decisions affect other people beyond the individual alone. All of these points lead to the conclusion that privacy cannot be regulated primarily by giving individuals greater control.

1. The Social Value of Privacy

Scholars have long pointed out that protecting individual privacy is not just for the sake of the individual but because of the larger social value of protecting individual privacy. Indeed, this claim can be made more generally about all individual rights. As John Dewey argued, rights are not only justified by their importance to

[44] Don't F**k with Cats (2019), https://www.netflix.com/title/81031373.

individuals but by "the contribution they make to the welfare of the community."[45] Robert Post persuasively contends that privacy "safeguards the rule of civility that in some significant measure constitute both individuals and community,"[46] Spiros Simitis argues that "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."[47]

Scholars, including myself, have pointed out that privacy is a social value.[48] Paul Schwartz contends that privacy is essential for democracy.[49] As Ruth Gavison writes, "Privacy is also essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy."[50] Julie Cohen also views privacy as a "constitutive element of a civil society."[51] Neil Richards elaborates that privacy protects intellectual activities that undergird the freedom of thinking, exploration of ideas, and speech, which are essential components of a free society.[52]

Protecting individual rights has typically been the main way of protecting individual freedom, so it is not surprising that privacy law seeks to protect privacy with privacy rights. Rights are often understood as rights against the government, such as Constitutional rights in the US, but there is also a broader tradition of positive rights that understands rights as involving government obligations to protect against incursions by private parties. For example, in the EU, there is a duty of member nations to protect privacy rights against infringements not just by the government but by others.[53] In the US, the common law tradition has long viewed tort protections against others as "rights," and it is no accident that the famous 1890 article by Samuel Warren and Louis Brandeis was called *The Right to Privacy*.[54]

Protecting individual privacy has a value for society, and society need not protect individual privacy solely by giving individuals rights that they can choose to invoke. Certainly, providing people with rights can help in promoting privacy's social value if people's exercise of their rights leads them to have the kind of robust privacy necessary for the larger ends of society. However, people struggle to exercise their rights. People often are coerced or manipulated into consenting to various uses of their data.[55]

---

[45] JOHN DEWEY, *Liberalism and Civil Liberties* (1936), *in* 11 LATER WORKS 374 (Jo Ann Boydston ed. 1991).
[46] Robert C. Post, The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 Calif. L. Rev. 957, 959 (1989).
[47] Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707, 709 (1987). In analyzing the problems of federal legislative policymaking on privacy, Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits. See Priscilla M. Regan, Legislating Privacy (1995).
[48] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).
[49] Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 Vand. L Rev. 1609, 1613 (1999).
[50] Ruth Gavison, *Privacy and the Limits of Law*, 89 Yale L.J. 421, 455 (1980).
[51] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1428 (2000).
[52] NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING INDIVIDUAL LIBERTIES IN THE DIGITAL AGE (2015); NEIL M. RICHARDS, WHY PRIVACY MATTERS (2021).
[53] Vladislava Stoyanova, *The Disjunctive Structure of Positive Rights Under the European Convention on Human Rights*, 87 Nordic J. of Int'l L. 344 (2018) ("There is little doubt that the European Convention on Human Rights (ECHR) imposes positive obligations upon states to ensure the rights enshrined therein.").
[54] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).
[55] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995, 999 (2014) (noting how companies exploit "irrationality or vulnerability in consumers"); Ido Kilovaty, *Legally Cognizable Manipulation*, 34 Berkeley Tech. L.J. 449, 469 (2019); Tal Zarsky, *Privacy and Manipulation in the*

Additionally, privacy issues extend beyond threats to individual privacy. There are larger societal problems caused or worsened by certain uses of personal data, such as discrimination as well as subordination of minority groups and the poor.[56] As Ari Waldman notes, "*Individual* rights will not solve *collective* privacy problems."[57]

Privacy rights work differently than many constitutional or statutory rights. For example, when a person challenges a law based on the right to free speech under the First Amendment to the U.S. Constitution, the judicial decision has effects that go far beyond the person's case. The law might be partially or fully invalidated. The person's challenge thus leads to a result that has broader societal effects. In contrast, exercising a privacy right often merely affects that individual. For example, if an individual gains access to her records or deletes data from her records, this has no larger societal impact. More generally, privacy rights contribute only in a minor way to the larger societal interests involved with privacy. Their effects are far more individualistic than Constitutional rights.

2. Shared Personal Data

Personal data is often shared between people. This fact is often underappreciated. The language of property is often invoked regarding personal data. People are said to "own" their data.[58] For many reasons, property is a poor fit for conceptualizing privacy.

Many types of personal data do not merely involve the isolated individual. For example, a photo of a person at a party with others does not just involve the personal data of that person but also of all the other people in the photo. Genetic information is shared among family members. Uploading one's contacts to a social media site implicates the privacy of each of the contacts.

Even a transaction, such as buying a book, involves shared data. Suppose I sell copies of one of my books on eBay. A celebrity buys my book. When I see the name and address of the celebrity, I become giddy with excitement. I post about it on social media. Meanwhile, the celebrity is irked because I am posting about a book the celebrity bought. Whom does this fact belong to? For me, it is an important moment in my life. I want to share my life story with the world, and the celebrity's identity is part of that story. But the data is also about the celebrity's life too. It is shared data. We both have a claim to it.

Companies that sell products and services to people can make the same claim. Information about a transaction is also information about their own activities for

Digital Age, 20 Theoretical Inquiries in Law 157, 174 (2019) ("[m]anipulative practices impair the process of choosing, subjecting it to the preferences and influences of a third party, as opposed to those of the individuals themselves.").

[56] Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 Cal. L. Rev. _, 36 (2021); Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671 (2016); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018).

[57] Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 Cal. L. Rev. _, manuscript p. 35 (2021).

[58] *See, e.g.,* Lawrence Lessig, Code and Other Laws of Cyberspace (1999); *but see* Pamela Samuelson, *Privacy as Intellectual Property?,* 52 Stan. L. Rev. 1125, 1137-47 (2000) (critiquing arguments for treating personal data as property); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy,* 53 Stan. L. Rev. 1393 (2001).

their own records.

As Simeon de Brouwer observes, there are "privacy externalities" because people's decisions to allow the collection and use of their personal data can also reveal data about other people.[59] For example, a person's autobiography will invariably involve personal information about other people: parents, siblings, children, spouses, partners, colleagues, friends, enemies, neighbors, and others. It is often impossible to tell one's story without referring to the personal data of other people. Much of our personal data is shared because much of life involves relationships and transactions between people.

Privacy rights are exercised by separate individuals to tend to their data. Such rights of lone individuals cannot extend to shared data without violating the privacy of others. This leaves shared data in a no man's land

3. Interrelated Personal Data

Rights also are limited when people's privacy decisions involve interrelated data. Interrelated data is somewhat different than shared data. Shared data involves facts that are directly connected between two or more people – such as genetic data. Interrelated data involves data that is not necessarily shared but that affects inferences made about others.

In today's "inference economy," machine learning and other forms of algorithmic decisionmaking work by making inferences based on data sets.[60] Everyone's data in the data set is used to make inferences, which are often then used to make decisions affecting people. As Salomé Viljoen notes, "Data flows are designed to represent the ways that people are like one another and reveal meaningful things about one another; how we are alike biologically, interpersonally, politically, and economically."[61] Viljoen observes that "data's relationality is central to the business of data production and constitutes much of what makes data production economically valuable to begin with."[62]

Many algorithms involve finding patterns in aggregations of data about millions of people. Rights are limited to the individual, so access, knowledge, algorithmic transparency, and other rights lack much meaning with just one particular individual's data isolated. The lone individual merely seeking information about decisions affecting her and how her particular data is being used will never learn the whole story. To truly understand how these algorithms reach decisions, one must examine the data of everyone fed into the algorithm.

The game Clue demonstrates the interrelatedness of personal data and how inferences about a person can be made based on other people's data. This murder mystery game involves the random selection of a murderer, a murder weapon, and a room where the crime occurred. The characters are Mr. Green, Mrs. White, Miss Scarlet, Colonel Mustard, Professor Plum, and Mrs. Peacock. The murder weapons

[59] Simeon de Brouwer, *Privacy Self-Management and the Issue of Privacy Externalities: Of Thwarted Expectations, and Harmful Exploitation*, Internet Policy Review, Vo. 9, No. 4 (Dec. 21, 2020).
[60] Alicia Solow-Niederman, *Information Privacy and the Inference Economy* (Aug. 5, 2021) (draft on file with author).
[61] Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance*, 131 Yale L.J. _ (2021), manuscript at 28.
[62] *Id.* at 30.

include a rope, candlestick, knife, gun, wrench, and lead pipe. Thera are various rooms in the house.

Cards for each are stuffed into an envelope that is set aside. Players are dealt cards for the other people, weapons, and rooms. Players know that the characters, rooms, and weapons in their hand are innocent, but they do not know what is in the other players' hands. As the game progresses, players learn about various cards in each other's hands, and are thus able to use the process of elimination to figure out who did it, with what weapon, and in which room.

Suppose the killer is Colonel Mustard in the library with the knife. With each piece of data revealed, such as the fact that Mr. Green or Professor Plum are not the culprit, one learns more about Colonel Mustard. Eventually, through process of elimination, a player can know for certain that the killer is Colonel Mustard.

Clue is an apt demonstration that much personal data is not only *relational* because it involves multiple people in some sort of relationship, but also because information about people can be used to make inferences about other people. Information about Professor Plum can affect inferences made about Colonel Mustard even if neither Plum nor Mustard share the same pieces of data.

Shifting from the game to real life, the exercise of individual rights has effects in the data ecosystem, as it can affect inferences. Each person might have a miniscule effect, but collectively these effects could be notable. Individuals exercising rights or failing to do so does not just affect themselves.

Returning to the Clue example, suppose that Company Z maintains records about all of the Clue characters. Company Z learns that Colonel Mustard is guilty, so it changes the designation in his record from "suspect" to "guilty." With Colonel Mustard's data indicating that he is the culprit, Company Z can infer that the other characters are innocent. Company Z therefore changes the records of the other characters from indicating that they are suspects to indicating that they are innocent. Colonel Mustard is outraged that he is identified as the culprit and demands that this data be deleted. But if the records of the other characters state that they are innocent, we will still know by inference that Colonel Mustard is the culprit even though he deleted this data.

Adding another twist, if Colonel Mustard exercises a right to delete his data, then a dilemma arises about how to handle the records of the other characters. As the records of the other characters indicate that they are innocent, their collected data will still result in the inference that Colonel Mustard is the culprit. To truly protect Colonel Mustard, the inferences made based on the deleted data must also be removed from the other characters' records. If the information about innocence is also deleted from the records of the other characters, then this turns each of them back into a suspect. As a result, these characters would likely be quite unhappy when Colonel Mustard's data is deleted. They would claim that their records went from accurately stating that they were innocent to now incorrectly stating that they are still suspected of the murder. They might claim that their rights are violated by the change.

In sum, because a person's data might be the piece in a puzzle that also enables inferences to be made about others, that person's exercise of rights can affect other people – and vice versa.

4. The Inadequacy of Individual Control

Exercising rights is akin to trying to empty the ocean with one cup at a time. The gigantic machinery of what Shoshana Zuboff calls "surveillance capitalism" is barely affected by the miniscule number of people who occasionally exercise one of their privacy rights.[63]

Of course, rights are an important component of privacy regulation. Rights can be useful to individuals for occasional situations, and they should certainly be part of privacy laws. Rights can force companies to spend more time and resources dealing with privacy. Administering rights, such as responding to data subject access requests, requires an understanding of the personal data being collected and processed. In this way, rights can improve organizational privacy practices. But most privacy laws rely far too heavily on rights. The result is that so many laws create the illusion that they are protecting privacy through rights when they are not.

Individuals are often powerless and vulnerable in a world where their vast quantities of their personal data is collected and used in ways that affect their lives. It thus seems intuitive to try to give individuals more control over their personal data with privacy rights. Ultimately, however, individuals can never be fully in control. To be effective, control cannot just be placed in the hands of individuals; control must come from society.

III. PRIVACY RIGHTS AND SOCIETAL MEASURES

In this Part, I analyze specific common privacy rights, and I discuss their strengths and shortcomings. As the GDPR rights are the most comprehensive and standard set of rights, I use these rights as the basic framework. However, there are other rights that are not quite identical to the GDPR rights but that are related. I discuss each in connection with its closest relative.

I discuss the failure of each right both facially and in practice. A right fails facially if it does not address key problems, is not suited to achieving relevant goals, or is structurally doomed and inherently unworkable. The goals behind many rights are often lost, and it is not clear that policymakers really understand and consider the goals when including rights in laws. In practice, many rights are implemented in a hollow and meaningless way. People rarely exercise rights and are often stymied when they do.

In evaluating each right, it is important to focus on their goals. I discuss various goals that the rights explicitly aim to achieve as well as normatively what the goals should be. After discussing the shortcomings of each right, I then recommend the types of societal measures that would achieve these goals in a more structural and effective way.

[63] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019).

A. RIGHT TO INFORMATION OR NOTICE

The right to information is a right of data subjects to know about the existence of record systems involving their personal data and to know about the types of data an organization gathers about data subjects and about how it is processed. Called the "right to information" under the GDPR and many other privacy laws around the world, this right is also referred to as a "right to notice" or "right to know" in the US.[64]

The right to information is an important part of privacy protection. Most privacy laws provide for this right. Indeed, it is hard to imagine a privacy law lacking in at least some dimensions of this right. The right often requires disclosing information about the data gathered about people; how the data is used, transferred, and protected; and data subject rights. Information is provided on one or both of the following ways – through a general notice posted to a website or sent to data subjects or in response to a request by a data subject.

Some laws require that the notice be provided directly to people, such as the US Gramm-Leach-Bliley Act, which requires financial institutions to deliver a printed privacy notice annually (unless people opt to receive it electronically).[65] In most laws, notice can be via a statement posted on a website. For example, the GDPR provides data subjects with a right to be informed about their personal data that entities hold, how it will be used, and to whom it will be transferred.[66] The notice also must inform data subjects about their rights regarding their data. According to Recital 58, this information can be posted on a public website in the form of a privacy notice.[67]

The amount of information in the notice varies from law to law. Some laws provide specific elements that must be included in a notice. For example, the California Online Privacy Protection Act (CalOPPA) requires a list of categories of personal data collected, categories of third parties with whom personal data is shared, and other information.[68] The GDPR requires that the privacy notice identify the controller, the data protection officer, the purposes for collecting the data, the categories of recipients, the period of storage of the data, whether there will be automated processing, and information about a data subject's rights.[69]

The privacy practices for data gathered through a website are frequently different from the privacy practices for data gathered within a relationship with a data subject or for data gathered from other sources. Some organizations might have different notices for their website data versus their account or relationship data. This bifurcation will might confuse people, but it is ironically a more accurate description of how the data will be processed.

Another dimension of notice provisions in privacy laws is regulation about how conspicuous the notice must be. Under the GLBA, notice must be "clear and

[64] California Consumer Privacy Act (CCPA) (right to know); Gramm-Leach-Bliley Act (privacy notices); HIPAA (notice of privacy practices).
[65] FDIC, Privacy of Consumer Financial Information §332.9.
[66] GDPR art 13-14.
[67] GDPR Recital 58.
[68] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).
[69] GDPR art. 13-14.

conspicuous."[70] The CalOPPA requires that a privacy notice be posted conspicuously on an organization's website.[71] The CCPA goes a step further by mandating a conspicuous button for people to opt out of selling or sharing personal data.[72]

The CCPA's right to "know" provides individuals with a right to request the specific pieces of personal data that organizations have collected about them.[73] This part of the CCPA's right to know is similar to a right to access and will be discussed later on.

On the surface, the right to information aims to provide information about privacy practices to individuals. It is uncontroversial to contend that individuals should have a right to know. The right to information should exist no matter what reasons people want to know, even if out of mere curiosity. But as a component of a regime of privacy protection, the right to information should achieve to something more. Framed in a broader more structural way, there are at least two important goals that could be achieved in connection with providing individuals with information: (1) informing individuals so they can make wise decisions; and (2) promoting accountability internally in organizations and externally to experts and regulators.

1. Informed Decisions

Merely providing information to people is a formalistic exercise that achieves very little. A more meaningful goal for effective privacy protection should be to *inform* people. There is an enormous difference between providing people with information and actually informing people so that they can make informed decisions. Indeed, it is hard to view privacy law as successful if it merely provides information to people but fails to result in any improvements in their decisions.

Several problems, however, make the right to information fail to inform people. The right looks far more meaningful and protective than it is in practice. One set of problems involves difficulties in people's ability to make full use of the right. In most laws, the right to information requires data subjects to make a specific request for information or to locate and read a privacy notice. But people lack knowledge of the legions of companies that gather enormous quantities of personal data about them from a panoply of sources. Having a privacy notice posted on a website is not enough to alert people to the fact. To have an accurate picture of the entities that have a data subject's personal data, the data subject must be directly informed about these entities. People cannot exercise the right to information in a meaningful way if they lack knowledge that particular organizations have their data.

In practice, rights to information are used only by a small number of people. Even when people seek the information, doing so once is insufficient. Many organizations are constantly gathering more and more information and are repeatedly changing their privacy notices. Thus, for each organization, people must repeatedly exercise their right to information.

[70] 17 CFR § 248.4.
[71] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).
[72] CCPA, 1798.185.
[73] CCPA, 1798.100(a).

Reading privacy notices is a task that does not scale.[74] There are simply too many privacy notices to read – people get notice fatigue. According to a study by Aleecia McDonald and Lorrie Cranor, if people were to read all relevant privacy notices, it would take more than 200 hours a year.[75] It is simply not practical – or fully rational – to read each privacy notice carefully.

Privacy notices are notoriously complex. They are often written in turgid lifeless prose that is at a very high reading level.[76] Moreover, most privacy notices are finely pureed by lawyers and then whipped into a batter with no discernible flavor. They have as much substance as a Twinkie has nutrition.

Even if all people were to suddenly start reading privacy notices, people often lack the ability to understand the information they receive about their data and are not in a good position to make thoughtful cost-benefit decisions.[77]

Several privacy laws valiantly try to address some of these problems. Some laws require that privacy notices be written in ways that people can understand. For example, Virginia's CDPA requires that privacy notices be "reasonably accessible, clear, and meaningful."[78] The GDPR requires that privacy notices be "concise, easily accessible and easy to understand" and written in "clear and plain language."[79]

Despite these ideals, many privacy notices are more complicated than James Joyce's *Finnegan's Wake*. In defense of privacy notice authors, privacy is quite complex, so describing it plainly and concisely yet accurately is not an easy task. In fact, it can be an almost impossible task because privacy is too complicated to be dumbed down to something pithy and clear.

Most organizations post a link to their privacy notices on the footer of their main page – and often on the site's general footer for all pages. The problem, though, is that most people do not read privacy notices.[80] Privacy laws often do little to address this problem except to require that a privacy notice be conspicuous. The failure of many people to read privacy notices, however, is likely not due to a lack of conspicuousness. No matter how conspicuous a privacy notice is, most people probably will not read it.

Even in the rare cases where people want to read privacy notices, they are time-consuming to review, difficult to understand, and not presented to people at relevant times or at the moment when they are interested in engaging.

Some commentators propose making privacy notices like nutrition labels or

---

[74] Solove, Privacy *Self-Management*, *supra* note X, at _.
[75] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S, A Journal of Law and Policy for the Information Society 540, 565 (2008).
[76] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev 1879 (2013).
[77] *Id.* at _.
[78] Virginia Consumer Data Protection Act, S.B. 1392 § 59.1-574(C).
[79] GDPR Recital 58.
[80] See Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure, 159 U. PA. L. REV. 647, 665–78 (2011); Florencia Marotta-Wurgler, Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts,"* 78 U. CHI. L. REV. 165, 178 (2011) (noting that people read contract boilerplate terms less than 1% of the time).

making notices more visceral.[81] Attempts to make notice simpler create the risk of oversimplifying. Privacy is quite complex and often cannot be understood as simply as the amount of fat and sodium on a nutrition label.

Another improvement might be to provide direct notice to data subjects – without their even having to ask for it. Direct notice would be impractical in many circumstances. Data controllers may have a lot of data about a person but not any contact information about the person. Another difficulty is that with so many entities having personal data about people, direct notice would unleash a tsunami of individual notices. Flooding people with these notices might become a nuisance, and it is unlikely that people would read the notices.

There are ways to improve the way that individuals are informed, though there are no silver bullets. To address the problem of too many notices to read, the law should set forth standard privacy terms that people could rely upon as the default. Deviations from these standard default terms would be prominently displayed to consumers. It is far easier to review important divergences from the norm than to read through thousands of privacy notices. The move to standard terms and calling out deviations would ease the burden on individuals significantly.

To address the problems of inattentiveness and notice fatigue, privacy laws could impose heightened notice requirements when there are greater risks of harm to data subjects.[82] Heightened notice would be more prominent than ordinary notice, and its timing would be more relevant to when data subjects would make key decisions or when risks would likely materialize.[83]

Heightened notice will certainly help address notice fatigue by bringing to people's attention the outlier activities and ones that are potentially harmful so people can focus their attention on the important things.

But even heightened notice is not enough. It can alert people to higher risks, but people still lack the tools they need to make the appropriate cost-benefit analysis for their decisions regarding their data. In the U.S. especially, privacy law relies far too heavily on the notice-and-choice approach, which involves providing people with notice and then relying on them to make decisions about their privacy based on the notice. Often, laws deem people's inaction (such as not opting out) as a form of consent or acquiescence in the practices stated in the notice, even when most people do not read the notice.

With the notice-and-choice approach, the right to information is twisted into serving a pernicious purpose – to legitimize nearly any form of data collection and use through an implausible fiction of consent. If improved notice merely serves as additional shine to the veneer of the notice-and-choice approach, then improved notice ultimately might amount to better signage along the road to hell.

Of course, there is nothing inherently wrong with the right to information. The

[81] Ryan Calo, *Against Notice Skepticism In Privacy (And Elsewhere)*, 87 Notre Dame L. Rev. 1027 (2012); Melanie Weir, *What are Apple's Privacy Nutrition Labels?*, Business Insider (Jan 20, 2021).
[82] In the American Law Institute's (ALI) Principles of the Law, Data Privacy, Paul Scwartz and I as reporters on the project proposed "heightened notice" that would be required for "any data activity that is significantly unexpected or that poses a significant risk of causing material harm to a data subject." ALI, Principles of the Law, Data Privacy § 4(e)(1).
[83] See ALI, Principles of the Law, Data Privacy § 4(e)(6) ("Heightened notice shall be made more prominently than ordinary notice and closer in time to the particular data activity.").

right is unobjectionable and is an essential component of most privacy laws. However, to be meaningful, the right to information must be part of a larger effort to ensure that people make informed decisions about their privacy. And, where this effort is not achievable, there must be other ways to protect privacy that do not turn on individual decisions.

No matter how much the right to information is improved, another fundamental problem is not endemic to the right itself. A major problem is the way that many privacy laws rely too much on the right to information. The problem is that the right is asked to do far too much work. Privacy laws try to leverage the right to information as a large part of the solution to privacy problems. The right to information is a useful go-to for policymakers because more transparency is often uncontroversial. The idea is that as long as organizations are transparent about what they are doing, as long as individuals have the ability to know, then it is okay for organizations to have the ability to do nearly anything they want.

Transparency is seen as the cure-all. Organizations can essentially build their own sandbox with boundaries as far out as they desire, marking out a vast desert within which to play. They can write the rules within the sandbox, so nearly anything can be permitted. Transparency is not enough. If the sandbox is too large and too tolerant of harmful activities, merely telling people it is dangerous is not enough given people's limitations in making good cost-benefit decisions regarding their privacy.

The law should establish boundaries for data collection and use. These boundaries need not be overly narrow; the sandbox for permissible collection and use can be large. The law should set norms so that people have a basic set of expectations about the use of their data without having to read through thousands of privacy notices.

2. Accountability

Informing people should not be the only goal related to the right to information. Notice also serves as an accountability mechanism internally as well as for experts and regulators to understand the data processing activities of organizations.

Internally, privacy policies help companies think about their privacy practices. Peter Swire points to a practical benefit of notices as leading to organizations to "inspect their own practices."[84] When organizations administer the right to information, they must be more aware of the data they collect, store, and use. Organizations must articulate their policies, which can make them use personal data in less of an ad hoc manner. Of course, not all organizations use this opportunity to get their house in order, but many do, Thus, internally, the right to information pushes organizations toward better data hygiene.

Beyond internal accountability, privacy notices create external accountability. Organizations must publicly state their privacy practices, which can be evaluated by experts, advocates, and regulators. If organizations fail to adhere to their stated practices, regulators can hold them accountable. In the US, for example, the FTC considers breaking promises in privacy notices as a "deceptive" trade practice

[84] Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 Minn. L. Rev. 1263, 1316 (2002). *But see* WALDMAN, INDUSTRY UNBOUND, *supra* note ___ at ___ (critiquing internal compliance and accountability programs as ineffective).

under Section 5 of the FTC Act.[85]

For the goal of accountability, more detail and complexity in a privacy notice is required than the vague vapid claims in many privacy notices. There is thus a dilemma at the heart of notice: The simpler and shorter privacy notices are written, the less meaningful detail they will often contain. Short and simple privacy notices do not provide enough information to help people have a good understanding of how their data will be processed. Making choices about privacy is quite complicated, so people must be provided with a lot of information to assess the risks and consequences of sharing their data or consenting to uses.

To address problems of conflicting goals of privacy notices, one solution might be to cleave the notice into two separate documents – a transparency statement with details and a more simple notice for data subjects.[86] The simple summary could help consumers get a very abbreviated sense of what a company is doing with privacy, and the detail could be referred to if people are interested in a deeper dive. The detailed document would be for the company's own internal accountability as well as for regulators to ensure that the company is following its practices. Of course, to be effective, regulators would have to enforce vigorously against companies that violated their promises. And, as discussed above, there must be substantive restrictions on inadequate or otherwise problematic privacy practices.

B. RIGHT TO ACCESS

The right to access provides individuals with a way to access their personal data that entities maintain. The right exists in most privacy laws.[87] For example, under the GDPR, data subjects have the right to access their personal data.[88] The U.S. Fair Credit Reporting Act (FCRA) provides individuals with the right to access their files.[89] HIPAA's right of access allows patients to obtain a copy of their medical records in the format they request.[90] Countless other privacy laws provide individuals with a right to access their data. For example, access is a core component of many Latin American privacy laws, as it is a key part of the foundational right to habeas data.[91]

To some extent, the right to access can overlap the right to information, though

[85] Solove & Hartzog, *FTC Common Law, supra* note _, at CITE.
[86] ALI, Principles of the Law, Data Privacy §§3- 4.
[87] Laws diverge on the time that organizations have to provide access. Many laws provide 30 days. One of the shortest time periods is Uruguay's right to access, which requires a response in just five days. Uruguay Law No. 18.331 on the Protection of Personal Data and Habeas Data Action. *See* Data Guidance, *Uruguay – Data Protection Overview* (Mar. 2021), https://www.dataguidance.com/notes/uruguay-data-protection-overview/.
[88] GDPR art. 15.
[89] Fair Credit Reporting Act, 15 U.S.C. § 1681(g)(a)(1) ("Every consumer reporting agency shall, upon request, and subject to section 1681h(a)(1) of this title, clearly and accurately disclose to the consumer: (1) All information in the consumer's file at the time of the request . . . .").
[90] 45 C.F.R. § 164.524(a)(1) (2019) ("[A]n individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set."); id.§ 164.524(c)(2)(i) ("The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.")., for as long as the protected health information is maintained in the designated record set, except for: (i) Psychotherapy notes; and (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.").
[91] Guadamuz, *Habeas Data vs the European Data Protection Directive*, *supra* note X, at __.

these rights are distinct. The right to access involves direct access to one's personal data, which some versions of the right to information also provide. For example, under the CCPA, the right to information encompasses the specific pieces of personal information that businesses maintain.[92] The right to information diverges when it requires information about purposes of use or data subject rights. In other laws, the right to information diverges when it does not involve access to actual personal data but instead provides information about categories of personal data collected or maintained. The distinction between the rights is that the right to access involves specific data and the right to information involves information about data collection and processing activities as well as rights.

Evaluating access rights depends upon the goals of providing access. There are several different goals, which depend upon the type of records involved: (1) learning about the specific personal data that organizations collect and process; (2) reviewing the data to make sure that it is accurate and complete; or (3) using the data for one's own aims and purposes.

1. Learning About Personal Data

The first goal involves learning about the specific personal data that organizations collect and process. This broad goal is the closest to the right to information. People might be curious about the specific pieces of personal data an organization maintains.

Access rights for learning goals, however, are often not very meaningful. For example, the CCPA gives individuals the right to see the specific data that organizations have collected.[93] This data often comes in the form of a data dump of all the personal data an organization has about a person.[94] Although people might learn that a lot more data is gathered about them than they had realized, they will often not learn much else. What matters more for understanding the privacy implications is how that data will be used. What types of analysis will be performed on the data? What conclusions will be drawn from the data? What decisions will be made based on those conclusions? These are key questions people must know to assess the consequences of consenting to an organization's processing of their data.

Additionally, there is also a scaling problem. Making access requests for the hundreds (and often thousands) of organizations that have data about a person will be a tremendous chore. Receiving data dumps from all of these organizations will be quite unwieldy. To achieve this goal, people must really be educated about how to make cost-benefit decisions about their data. As I have argued at length elsewhere, this is tremendously difficult for people to do.[95] The right to access cannot achieve this broader goal. Although ultimately, people will never be sufficiently educated and will never be able to make wise cost-benefit decisions about their data, the effort to try to educate them and help them is a worthy one and worth pursuing even in the face of failure. Moving the needle a little bit is still worthwhile.

---

[92] CCPA, 1798.100(a).
[93] CCPA, 1798.100(a).
[94] Kashmir Hill, "I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too," N.Y. Times (Nov. 4, 2019) ("[M]ost of these companies are just showing you the data they used to make decisions about you, not how they analyzed that data or what their decision was.").
[95] Solove, *Self-Management, supra* note X, at _.

However, teaching people to a limited degree and improving their decisions in a small way are far from adequate to addressing the problem that personal data is being used to affect people's lives in ways that are not always in their best interest. To address this problem, the law must do more to regulate data uses, algorithms, and inferences.

2. Reviewing Personal Data

Another goal of access is reviewing the personal data to make sure that it is accurate and complete. This goal matters most when there are potential negative consequences if the data has errors. For example, reviewing credit reports helps individuals protect themselves against errors or incomplete data, which could lead to negative consequences such as denial of loans, loss of job opportunities, or higher interest rates. This goal works in tandem with the right to rectification (or correction), where individuals have a right to correct errors or add data to their records to make them complete.

Access rights, however, fall short of achieving this goal in several ways. Access does not scale well, and it will be too great a burden for individuals to access and review all important records. The onus should not be on individuals to continually act as unpaid proofreaders of their records.

Additionally, people lack knowledge of the existence of many entities that maintain records about them. Many people even do not know that consumer reporting agencies have their data and cannot name any of the big three agencies. There are countless other entities that maintain records that have substantial effects on people's lives. For example, the Medical Information Bureau (MIB) maintains records used by health and life insurance companies to "assess an individual's risk and eligibility during the underwriting of life, health, disability income, critical illness, and long-term care insurance policies."[96] People can make a request to see their MIB file. But many people have no idea that the MIB exists, let alone that they can access their file or how to access their file. This problem exists with many entities. People cannot use access rights if they do not know the entities from which to seek access.

The goal of reviewing personal data should be achieved through stronger duties on organizations to ensure that data is accurate and complete. Despite many statutory principles and duties to maintain accurate records, these provisions in laws are mainly enforced by the right to rectification or correction. There must be enforcement mechanisms to ensure accuracy that does not place the burden on individuals. For example, external accuracy audits could be required for certain industries such as credit reporting or healthcare. I will discuss such audits later on with the discussion of the right to rectification.

3. Using Personal Data

A third goal for the right to access involves situations where people use their records for their own purposes. One of the most common types of records in this category is a medical record. In many cases, people access their medical records

[96] Medical Information Bureau, *The Facts About MIB's Underwriting Services*, https://www.mib.com/facts_about_mib.html.

to provide them to other healthcare providers or to understand their diagnosis and treatment.

In the United States, HIPAA provides a robust right to access medical records, but thus far, compliance has been poor. According to one study, more than 50% of medical providers did not meet the basic requirements in HIPAA for providing medical records.[97] A further 20% of the providers would not provide records until requests were escalated to supervisors.[98] Additionally, HIPAA requires health information to be disclosed to patients via email if they prefer, but many healthcare providers refuse to do so.[99] HIPAA states that covered entities "must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format."[100] However, many covered entities do not send records by email and getting electronic copies can be quite difficult. One study found that providers insisted on sending paper records, faxes, and CDs even when patients asked for records to be sent electronically.[101] Another study showed that only 33% of hospitals studied included email as an option on their record release forms.[102] These longstanding problems with access prompted the U.S. Department of Health and Human Services to begin a targeted enforcement campaign to improve compliance with HIPAA's access right.[103]

One reason for the poor compliance is that many providers have been slow to adopt modern digital technologies for recordkeeping and communication with patients. Organizations must make a decision about how much time and resources to allocate to access requests. Organizations may decide to devote little attention to access because enforcement is unlikely and the sanctions are not high enough or are not frequently imposed.

The story with HIPAA access demonstrates an important point: A right is not self-executing. Without the appropriate tools and procedures, organizations cannot administer the right properly and effectively.

A broader and more structural approach in the law would aim to make records serve individuals rather than merely serve the organizations that keep the records. For example, the law should consider medical records as an essential tool for the patient, not as just records for the benefit of the healthcare provider. Rather than

---

[97] Deven McGraw, Nasha Fitter, and Lisa Belliveau Taylor, *Health Care Provider Compliance with the HIPAA Right of Individual Access: A Scorecard and Survey* (Aug.13, 2019).
[98] *Id.*
[99] HIPAA, 45 CFR § 164.524 ("The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format."); Daniel J. Solove, *Yes, HIPAA Requires Medical Records to Be Emailed to Patients if Requested*, Privacy+Security Blog, Nov. 29, 2018, https://teachprivacy.com/hipaa-requires-medical-records-to-be-emailed-to-patients-if-requested/.
[100] 45 CFR § 164.524.
[101] Deven McGraw, Nasha Fitter, and Lisa Belliveau Taylor, *Health Care Provider Compliance with the HIPAA Right of Individual Access*: *A Scorecard and Survey*, https://www.medrxiv.org/content/medrxiv/early/2019/08/13/19004291.full.pdf.
[102] Carolyn T. Lye, Howard P. Forman, Ruiyi Gao, *Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records,* JAMA Network Open (Oct. 5, 2018), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2705850.
[103] *OCR Resolves Twentieth Investigation in HIPAA Right of Access Initiative with $80,000 Settlement*, Health and Human Services (Sept. 10, 2021), https://www.hhs.gov/about/news/2021/09/10/ocr-resolves-twentieth-investigation-in-hipaa-right-of-access-initiative-with-settlement.html ("OCR created this initiative to support individuals' right to timely access their health records at a reasonable cost under the HIPAA Privacy Rule.").

merely mandate access, the law could facilitate greater engagement with records. The law could subsidize better record systems that enable easier and wider patient access. Instead of waving a stick when providers fail to provide adequate access, the law could do a lot more to help improve access with carrots.

One way to improve access to medical records might be to require that records be automatically made available to patients without the need to make a request.[104] In one study, when patients received their records automatically, almost all of the patients were "enthusiastic" about the program. Doctors viewed the program positively as well: "Approximately three-quarters of all the doctors said that such transparency had none of the dreaded impacts on their practice. Many felt there was more trust, better communication, more shared decision-making and increased patient satisfaction."[105] None of the doctors chose to stop sharing the notes with their patients after the study had concluded. The patients benefited greatly from the increased access: "[A]lmost 80 percent of the patients said that reading their doctors' notes helped them to take their medications more regularly and better follow their doctors' treatment recommendations."[106]

C. RIGHT TO DATA PORTABILITY

Several privacy laws provide people with a right to data portability. This right requires that organizations provide people with a copy of their data in a form that they can readily take and use with another organization. The GDPR provides that data subjects have the right to receive their personal data in a "structured, commonly used and machine-readable format" and to transmit the data to another controller "without hindrance."[107] The right to data portability is a cousin to the right to access; data portability is akin to an access right on steroids giving people rights to all of their data in a usable format.

As one of the newest EU rights, first emerging under the GDPR, the right to data portability lags other rights in worldwide recognition. Nonetheless, more recent privacy laws are recognizing the right to data portability, such as Brazil, Barbados, Panama, Thailand, and Kenya.[108]

---

[104] Automatic access is not necessary or desirable for all types of records, just records where access would most benefit people.

[105] Pauline Chen, *Letting Patients Read the Doctor's Notes,* N.Y. Times Blog, Oct. 4, 2012. http://well.blogs.nytimes.com/2012/10/04/letting-patients-read-the-doctors-notes/.

[106] *Id.*

[107] GDPR art. 20(1) ("The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. . . .").

[108] See Brazil Lei Geral Da Proteção De Dados Pessoais (LGPD), Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial Da Uniao [D.O.U.] de 15.08.2018 (Braz.), English translation at https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/) (requiring "portability of the data to another service provider or product provider, by the means of an express request, pursuant with the regulations of the national authority, and subject to commercial and industrial secrets."); Thailand Personal Data Protection Act, B.E. 2562 (2019) (Thai.), https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf ("The Data Controller shall arrange such Personal Data to be in the format which is readable or commonly used by ways of automatic tools or equipment, and can be used or disclosed by automated means."); The Data Protection Act, No. 181 (2019) Kenya Gazette Supplement No. 24 §§ 38(1) ("A data subject has the right to receive personal data concerning them in a structured, commonly used and machine-readable format.").

In the US, privacy laws generally lack a right to data portability, but newer state laws are starting to include this right. For example, the CCPA requires businesses provide personal information in a portable and "readily usable format" to allow consumers to transfer the information to another entity "without hindrance."[109] The VCDPA establishes a similar right to data portability.[110]

1. Enhanced Access and Data Ownership

In many ways, data portability is an extension of the right to access. It is a right to access with a specification about the format of the data. In this way, the right is a success; it improves the right to access. However, data portability alone is not the answer to the shortcomings of the right to access in achieving many of the goals.

At the outset, the data portability right under the GDPR does not involve all personal data maintained by controllers but only the data that was provided by the data subject.[111] "Provided" means data provided directly or indirectly through user activity (such as tracking user interaction with an entity's website).[112] Many organizations maintain data gathered about data subjects in other ways, and this data is not covered by the GDPR's right to data portability.

Data portability has less value when data is interconnected with data of others, such as on social media. Only porting a person's data without information supplied by others is incomplete. Porting other people's information would violate the privacy of these people. For example, a person's ability to port a list of email addresses for their entire set of LinkedIn contacts affects the privacy of those contacts. Overall, is such portability privacy protective or a privacy risk? The answer is quite unclear. Moreover, as Peter Swire and Yianni Lagos note, data portability can increase risks to data security.[113]

Thus, on many sites where data portability would be most desired by users, there will be significant limitations on how much data can be ported and how useful porting the data will be. Moreover, data portability is difficult for regulators to enforce. Regulators would have to analyze the technology involved and how readily the data could be ported. Thus far, data portability operates more as a suggestion than a rigorous requirement.

2. Competition

The right to data portability also aims to serve the goal of promoting competition. Data portability aims to empower individuals to switch to competitors and not be

[109] Cal. Civ. Code § 1798.100(d) (West 2020) ("[T]he information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.").
[110] See Consumer Privacy Rights Act, ch. 36, 2021 Va. Legis. Serv. 1, 4 (West) (to be codified at Va. Code Ann. 59.1-573(A)(4)) ("To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means").
[111] Sasha Hondagneu-Messner, *Data Portability: A Guide and a Roadmap*, 47 Rutgers Computer & Tech. L.J. 240, 254 (2021).
[112] Id. at 254-55. For more background on the scope of the GDPR's right to data portability, see Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (Apr. 5, 2017).
[113] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,* 72 Md. L. Rev. 335, 374 (2013).

locked in because their data is locked up.[114] According to guidance by the Article 29 Working Party (now called the European Data Protection Board), data portability "can foster a more competitive market environment by allowing consumers more easily to switch providers."[115]

However, although it is sometimes assumed that privacy and antitrust are complementary, Erika Douglas aptly contends that there are significant tensions between these two domains.[116] For example, smaller companies have argued that they must be able to access and scrape data from large competitors in order to be competitive. In *HiQ Labs v. LinkedIn*, LinkedIn blocked HiQ from scraping personal data from its users' profiles. HiQ argued that this blocking was anti-competitive. HiQ won the case, but the U.S. Supreme Court granted certiorari and will be looking at the issue. [117]

Data portability often does not work effectively to increase competition. Removing one's data from a social media site such as Facebook and placing it elsewhere will not readily re-create the experience of Facebook. All one's friends and interwoven data would not be ported. There is a collective action problem, and it is not readily solvable by data portability.

As a feature of *privacy* laws, data portability should aim to enhance competition for *privacy*, not just competition in general. There are many other ways to address general competition, which is what anti-competition law seeks to do. Data portability thus should have the narrower goal to promote competition about privacy.

But this goal is doomed without addressing the market failure that prevents meaningful competition about privacy. People certainly care about privacy, yet their behavior does not appear to match their stated attitudes.[118] Elsewhere, I have argued that this gap between attitudes and behavior is not a "paradox," as it has oft been called, but reflects the fact that attitudes and behaviors regarding privacy involve different things. Abstractly, many people deeply care about privacy. Behavior involves concrete and contextual situations involving risk calculations. In these situations, people are presented with immediate benefits that they can readily understand. As discussed earlier, people cannot make good cost-benefit decisions regarding privacy because the implications of the future use of their data are too complex to figure out. Privacy often does not fare well when balanced against immediate benefits and technology's dazzle.

Often, competition about privacy involves a lot of rhetoric about how much a company cares about privacy, but nothing makes this rhetoric match reality. Just because a company shouts "privacy" more loudly does not mean it protects privacy more than other companies.

---

[114] Whitney Nixdorf, *Planting in A Walled Garden: Data Portability Policies to Inform Consumers How Much (If Any) of the Harvest Is Their Share*, 29 Transnat'l L. & Contemp. Probs. 135, 148 (2019).
[115] Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability* (Apr. 5, 2017).
[116] Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, Yale L.J. Forum 647, 661-80 (Jan. 18, 2021).
[117] HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). For background about the clash between privacy and anti-competition law, see Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, Yale L.J. Forum (Jan. 18, 2021).
[118] Daniel J. Solove, *The Myth of the Privacy Paradox,* 89 Geo. Wash. L. Rev. 1 (2021).

Moreover, privacy is just one dimension among many that companies might compete upon. Other dimensions, such as price and quality, are easier for consumers to understand, assess, and compare. Thus far, these other dimensions appear to far outmatch privacy in the market.

Data portability, in and of itself, is far from sufficient to create such competition in privacy. The data portability right seems to rest on the assumption that there is a healthy market for privacy; the hope is that portability will grease the wheels, and they will turn. But this hope is unrealistic.

There is a more practical way that the law can help consumers when making choices between companies – to stop the bad apples with deficient privacy practices. Strong privacy comes at a cost, as it involves personnel and time to address privacy adequately. Privacy also might involve forbearance on collecting or using personal data that has a high opportunity cost. Companies that incur these costs should not have to compete against companies that shortchange privacy with underfunded programs without adequate resources or companies that ignore privacy for greater profit. If companies can get away with being cheap and opportunistic about privacy, then those companies that do so have an advantage. For example, they might be able to offer lower prices than other companies that take privacy seriously.

The law can help prevent this unfair advantage by ensuring that companies cannot get away with poor privacy practices and cutting corners. Operating in this more structural way, the law could ensure that companies that try to protect privacy well are not at a competitive disadvantage.

D. RIGHT TO RECTIFICATION OR CORRECTION

One of the most common rights in privacy laws is the right to rectification or correction. The right provides individuals with the ability to request that errors in their records be corrected as well that data be added so that the records reflect the complete story. For example, under the right to rectification in Article 16 of the GDPR, data subjects have the right to have errors in their personal data corrected.[119] In addition, data subjects have the right to have "incomplete personal data completed."[120]

1. Accurate Records

A primary goal of the right to rectification is to promote accurate records. This goal is important because records of personal data are often riddled with errors. According to a FTC report in 2013, about 5% of consumers "had an error on one of their credit reports serious enough to result in higher borrowing fees."[121] A health IT expert estimates that about 70% of medical records have errors.[122] These facts are not surprising because personal data is gathered, processed, and transferred

[119] GDPR art. 16.
[120] GDPR art. 16.
[121] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 150 (2016).
[122] Christina Farr, *This Patient's Medical Record Said She'd Given Birth Twice - In Fact, She'd Never Been Pregnant* CNBC (2018), https://www.cnbc.com/2018/12/09/medical-record-errors-common-hard-to-fix.html (last visited Feb 13, 2020).

on a gigantic scale and with enormous frequency. Errors in data can readily spread as information flows from one record system to another.

As with other rights, the right to correction places on the onus on individuals to act as proofreaders of their records. Engaging in free proofreading for organizations is not a task that many individuals have the time or wherewithal to do. The task does not scale given the vast number of organizations that collect and process personal data. Not only is reviewing records time-consuming, but making a correction request is even more of drain on time. Compounding this problem is the fact that an individual's dossier with a particular organization is not static. Data is constantly being added and changed in the dossier, sometimes even on a daily or weekly basis. Thus, it is unlikely individuals will be able to continually review their records at one organization, let alone the hundreds (or perhaps thousands) of organizations that possess their data.

The problem of record accuracy is exacerbated by the fact that the optimal degree of accuracy diverges for organizations and individuals. For individuals, an inaccuracy in records could lead to being charged a higher interest rate, being denied a loan, being rejected for a job, being barred from flying, or even being improperly arrested. For organizations, the stakes for errors are much lower. If a consumer reporting agency has incorrect data, it might miscalculate a credit score. The harm to the consumer reporting agency is minimal; creditors likely will not even know about the error and will just move on to offer a loan to someone else. Of course, very high error rates might not be optimal, but many organizations can tolerate a moderate error rate.

Thinking about the right to correction in a more structural way, the goal is not merely to allow individuals to correct errors in particular records but also to ensure that record systems with personal data are maintained at an appropriate level of accuracy. This broader goal is one that many privacy laws purport to achieve by including a principle of "data quality," typically requiring that personal data be accurate, complete, and up-to-date. Data quality need not be perfect but should be reasonable and appropriate for the uses and potential risks. The principle of data quality is an essential one, as it requires accuracy without placing the onus on individuals to proofread and correct their records.

Although privacy laws frequently proclaim the data quality principle, it often amounts to hollow rhetoric. Rarely do the laws have mechanisms to ensure for data quality beyond merely stating the principle. A more rigorous requirement of data quality would require concrete ways to monitor organizations to ensure that they are adhering to the principle. The right to correction should serve as a secondary level of protection – as a backstop for individuals to correct occasional errors. In practice, however, enforcement of data quality falls back to individuals, who must raise right-to-correction complaints or seek to enforce data quality through a private right of action in laws that have them.

When plaintiffs have sought to use a private right of action for violations of data quality, courts have undermined their cases with narrow conceptions of harm. In the United States, the Supreme Court has recently undermined the enforcement of accuracy. In *TransUnion v. Ramirez,* TransUnion, a consumer reporting agency, falsely indicated that more than 8,000 people were terrorists on their credit

reports.[123] The errors emerged when TransUnion created a service called "Name Screen" where it would place alerts on credit reports when people were a "potential match" on the U.S. Treasury Department's Office of Foreign Assets Control's (OFAC) list of terrorists, drug traffickers, and other criminals. The process by which TransUnion added the alerts was quite shoddy. TransUnion would merely compare people's names to the OFAC list.

> If the consumer's first and last name matched the first and last name of an individual on OFAC's list, then TransUnion would place an alert on the credit report indicating that the consumer's name was a "potential match" to a name on the OFAC list. TransUnion did not compare any data other than first and last names. Unsurprisingly, TransUnion's Name Screen product generated many false positives. Thousands of law-abiding Americans happen to share a first and last name with one of the terrorists, drug traffickers, or serious criminals on OFAC's list of specially designated nationals.[124]

The plaintiffs argued that TransUnion failed to follow reasonable procedures to ensure accuracy, as required by the FCRA.[125]

The Court ultimately concluded that that only the plaintiffs whose reports were disclosed to others had standing to sue under the FCRA. Plaintiffs who had the error in their reports that had not yet been disclosed did not suffer a "concrete injury" and lacked standing to sue despite FCRA's granting individuals a statutory right to sue.[126]

With this disembowelment by the Court, FCRA's accuracy requirement is without meaningful heft or rigor. Instead of placing the onus on people like Ramirez to police their records, the law should mandate better processes for keeping records accurate. FCRA purportedly does this with its requirement to use "reasonable procedures to ensure maximum possible accuracy" but the lesson from *TransUnion v. Ramirez* is that consumer reporting agencies can avoid being liable for failing to adhere to this duty.

In many cases, there is the potential for errors in records not to be detected by individuals or to be discovered too late after damage already has been done. Returning to *TransUnion v. Ramirez,* the lead plaintiff only learned about the error of being mislabelled a terrorist when he tried to buy a car. He was stunned to be told by the car salesperson that he could not buy the car because he was on a terrorist list. Had he not tried to buy the car, he might never have known. Without knowledge, he would not have exercised his right to correct. Many other individuals had no idea that their records contained this egregious and damaging error.

Although FCRA's accuracy requirement might sound strong, especially with the use of the words "maximum possible accuracy," in practice, it falls far short. For example, in *Sarver v. Experian,* the court held that credit reporting agencies did not have a duty to analyse reports for "anomalous information." Doing so would

[123] TransUnion LLC v. Ramirez, 141 S.Ct. 2190 (2021).
[124] *Id.*
[125] See § 1681e(b).
[126] *TransUnion, supra* note _, at X.

be too big a burden on the company which processed a ton of data each day.[127] The irony is that the concept behind the obligation of maintaining accuracy was to ensure that companies did not consume more information than they could chew. Also, consumer reporting agencies offer credit report monitoring services where they tout their ability to look for anomalous information, which undercuts the claim that doing so to meet its statutory obligation is too difficult.

Privacy laws should require more steps to maintain accuracy whenever there is a risk of harm or negative consequence to people. Relying on rights to correct is too fragmented and minimal to incentivize organizations to improve the accuracy of their records. Placing the onus on individuals to bring private rights of action to enforce data quality requirements puts a big burden on individuals, who must engage in protracted litigation only to be rebuffed by courts that are reluctant to find harm. Thus, privacy laws end up with having empty shibboleths about strong data quality and high accuracy. Instead, concrete procedures should be mandated, such as reviewing records for anomalies, conducting audits of records for accuracy, and accountability to regulators for accuracy.

The law also must take more proactive steps to ensure that records are accurate. For example, HIPAA is commonly believed to have a right to correction, but it actually merely has a right to "amendment."[128] HIPAA allows patients to request that notations about errors be added to their file but not that the errors be removed or changed.[129] Thus, if incorrect data infects a record, there is no way to cleanse it out. Errors become akin to a chronic disease that must be forever managed; they do not go away. Erroneous data can readily take on a life of its own, and correction notations often go unread or unnoticed. Of course, there are certain reasons why erroneous information should not be entirely deleted, as the data could explain a diagnosis or need to be preserved in case of future litigation. But the erroneous data could be archived and removed from the main part of the record.

The right to rectification is an important one for occasional situations where people become aware of errors in their records that they want to take the time to fix. But the right is not well-designed to achieve the larger structural goal of accurate records.

2. Accurate Decisions and Predictive Judgments

Accurate records are important, but their value is not primarily based on accuracy for its own sake. Instead, accurate records are part of a larger more important goal – accurate *decisions*. Inaccurate records have the potential to lead to decisions that can cause harm to people and that are unfair.

Privacy laws mainly focus on accurate *records* rather than accurate *decisions*. For example, FCRA seeks to ensure accurate records, but says little about the quality of credit scoring. A credit score can be inaccurate not only if it is based on wrong data, but also if based on a faulty formula. The same is true for many decisions based on algorithms; the decisions could be flawed because the data is bad or because the algorithm is bad. Therefore, accurate records are far from sufficient to

[127] Sarver v. Experian Information Solutions, 390 F.3d 969 (7th Cir. 2004).
[128] HIPAA, 45 C.F.R. § 164.526.
[129] HIPAA, 45 C.F.R. § 164.526(c)(1) (providing that the covered entity must make the amendment by "identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment").

ensure accurate decisions. Accurate records are certainly a necessary condition to accurate decisions, but much more than accuracy of records must be regulated to ensure for accurate decisions.

The law focuses on *data* rather than *decisions* likely because of a fear of becoming too paternalistic. Although lawmakers should not be writing algorithms, there is a wide range of ways that the law can regulate algorithms without mandating specifics. The law could establish certain factors as off-limits. The law could set certain ideals for decisions and create accountability mechanisms to check if decisions are meeting these ideals.

Beyond *accurate* decisions, there is an even broader goal that the law should strive to achieve – *appropriate* decisions. Increasingly, predictive decisions are being made about people based upon the data in their records.[130] The data in a record could be entirely correct but predictions based upon it could be wrong. In this scenario, a right to correct the data will not be useful unless the prediction is part of the record and can be proven wrong. A predictive decision is often impossible to prove as incorrect because it is a prediction of a future occurrence that has not yet happened.

Only in a few contexts does the law protect against predictive judgments. For example, the Genetic Information Nondiscrimination Act (GINA) prohibits discrimination in employment and insurance based on genetic information.[131] However, laws generally do not restrict decisions based upon predictions or allow people to contest the assumptions and judgments behind the prediction.

Ultimately, the most important goal for privacy law is to protect people from faulty decisions. Decisions can be faulty because they are inaccurate, but predictive decisions often cannot be assessed as accurate or inaccurate. Nevertheless, predictive decisions must be fair, transparent, and not contrary to societal values.

Not only is the right to correct errors in records woefully insufficient as a means to make records more accurate systematically, but the right fails because it is focused on data and on accuracy. The law must not just focus on accurate *data* but also on accurate *decisions*. And, when regulating decisions, the law must regulate not just *accuracy* but also *adequacy*. The right to rectification is unable to achieve these goals. The law must regulate to ensure a minimum level of quality in decisions. Accurate data is a means to a larger end. It does not make sense to wash and wax a car and then drive it off a cliff. Pristine data is meaningless if decisions made based on it remain shoddy.

E. RIGHT TO ERASURE OR DELETION

Under the GDPR and many other privacy laws, data subjects have a right to "erasure" of their personal information.[132] This right is also called a right to

[130] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 133 (2016).
[131] Genetic Information Nondiscrimination Act, Pub.L. 110–233, 122 Stat. 881 (2008).
[132] GDPR art. 17; Argentina's Personal Data Protection Law; Peru's Personal Data Protection Law; Uruguay's Law on the Protection of Personal Data and Habeas Data Action; Brazil's LGPD; Kosovo's Law on the Protection of Personal Data; Montenegro's Personal Data Protection Law; Russia's Federal Law on Personal Data; Turkey's LPPD; Ghana's Data Protection Act; Israel's Privacy Protection Law; Hong Kong's Personal Data (Privacy) Ordinance; South Korea's Personal Information Protection Act. Privacy laws typically provide for some exceptions to the right of

"deletion" or "elimination" or "cancellation."

There has been significant confusion about the meaning of the right to erasure. The right is often conflated with the right to be forgotten, which is actually quite distinct. The GDPR exacerbates the confusion by putting the right to be forgotten in parentheses after the title of the right to erasure.[133]

There are several different circumstances under which laws recognize a right to erasure, such as illegally-processed data, withdrawn consent, or data that is no longer necessary. The GDPR recognizes all of these circumstances as ones justifying erasure.[134] The erasure rights of many other laws do not allow for erasure in some of these circumstances.

Deletion rights often allow for data subjects to demand the deletion of data that was properly processed with their consent. Under the GDPR's right to erasure, individuals can have data deleted if they withdraw consent to processing and if there is not another lawful basis to process.[135] Data subjects also can have data erased if they exercise their right to object to the processing and "there are no overriding legitimate grounds for the processing."[136]

In the US, only a few federal laws provide for a right to delete. COPPA through its regulations requires a right of parents to delete data gathered from their children as well as data that is no longer necessary for the purposes of collection.[137]

Recent US state privacy laws provide for rights to delete. Under Virginia's CDPA, people "have the right to delete personal data provided by or obtained about the consumer."[138] Likewise, under the CCPA, provides people with a broad right to delete personal data.[139] Additionally, when a business receives a consumer deletion request, it must explicitly notify and instruct any third parties that have received the consumer's personal information to delete it.

The VCDPA and CCPA are somewhat broader than the GDPR for erasure because the GDPR permits erasure when a person withdraws previously-supplied consent to process whereas the VCDPA and CCPA allow individuals to delete data even beyond the basis of withdrawal of consent. The VDCPA has the broadest deletion right, applying to information "provided by or obtained about the consumer."[140] The CCPA only applies to personal data "which the business has collected from the consumer."[141]

---

deletion, such as ensuring security, protecting against illegal activities, complying with a legal obligation, or ensuring the exercise of free speech.

[133] GDPR art. 17 ("Right to erasure ('right to be forgotten')").

[134] GDPR art 17.

[135] GDPR art 17(b).

[136] GDPR art 17(c).

[137] COPPA Rule, 16 C.F.R. § 312.4(d)(3) (a "parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so"); COPPA Rule, 16 C.F.R. § 312.10 ("An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.").

[138] VCDPA, § 59.1-573(A)(3).

[139] CCPA, 1798.105.

[140] VCDPA, § 59.1-573(A)(3).

[141] CCPA, 1798.105.

The most common circumstance that laws recognize as justifying erasure involves data that was improperly gathered. The GDPR's right to erasure extends to data that was "unlawfully processed."[142] Deleting such data follows basic legal principles of disgorging ill-gotten gains. Under many privacy laws, the data protection authority can order the destruction of improperly-gathered data.

1. Preventing Ill-Gotten Gains

A key goal of the right to erasure is to prevent organizations from keeping improperly-collected personal data.[143] The onus should not be on individuals to pursue actions to disgorge ill-gotten gains. The law ought to ensure that entities do not maintain data that they gathered or processed in violation of the law. In many cases, the law does so without placing the burden on individuals to enforce it.

For example, in several cases in the United States, the FTC has ordered the destruction of such data.[144] In one case, for instance, the FTC ordered Everalbum to delete photos and videos that it collected from consumers and use for its facial recognition technology without their consent.[145]

As with other rights and other goals, the right to erasure is useful in a secondary role to achieve the aim of disgorgement, but it is not sufficient to be the primary mechanism. Not enough individuals will exercise their rights to ensure that all the wrongly-acquired data is deleted. When privacy laws move beyond relying on individuals to exercise their right to erasure to police ill-gotten gains, they are dramatically more effective.

As Lauren Scholz argues, restitution should play a much larger role as a remedy for privacy violations.[146] The law should aim to address "the wrongful profit and the incentives that it creates for businesses."[147] No company should come out ahead for violating the law. Economic incentives must favor compliance.

---

[142] GDPR art 17(d).

[143] Restitution involves restoring victims to where they would have been absent the wrongful conduct. Lauren Henry Scholz, *Privacy Remedies,* 94 Ind. L.J. 653 (2019). Disgorgement involves returning the unlawful gains that a wrongdoer obtained through unjust enrichment. With restitution, the focus is on restoring what the victims lost. With disgorgement, the focus is on surrendering the profits that the wrongdoer gained. Restitution does not depend upon deliberate wrongdoing; even an innocent mistake that unjustly enriches a defendant can be subject to restitution. For example, restitution can involve a third party that was unwittingly given an undeserved benefit. Restitution can be used against third parties that benefit from another party's actions. For example, if a company wrongfully shares personal data with a third party, that third party could be ordered to purge the data.

[144] See, e.g., In the Matter of Midwest Recovery Systems (FTC. Nov. 30, 2020) (settlement requiring deletion of debt information); In the Matter of Flo Health, Inc. (FTC, June 22, 2021) (settlement requiring Flo Health to instruct third parties that it improperly shared personal data with to delete that data). In 2021, the U.S. Supreme Court took away the FTC's ability to pursue some of these remedies. In *AMG Capital Management v. Federal Trade Commission*, the Court held that the FTC lacked authority under the FTC Act "to seek, [or] a court to award, equitable monetary relief such as restitution or disgorgement." Acting FTC Commissioner Rebecca Kelly Slaughter responded to the Court's decision by saying that "the Court has deprived the FTC of the strongest tool we had to help consumers when they need it most" and that the Court "ruled in favor of scam artists and dishonest corporations, leaving average Americans to pay for illegal behavior." AMG Capital Management v. Federal Trade Commission, 141 S.Ct. 1341 (2021).

[145] In the Matter of Everalbum, Inc. (FTC, May 7, 2021).

[146] Lauren Henry Scholz, *Privacy Remedies,* 94 Ind. L.J. 653 (2019)

[147] *Id.* at 677-78.

2. Data Minimization

A goal of deletion rights is to further the principle of data minimization, which typically states that data shall not be retained for longer than necessary to achieve the purposes stated at collection. Many laws have this principle. In addition to the right to delete, this principle is sometimes backed up by data retention requirements that explicitly require the deletion or anonymization of data that is no longer needed.[148] As Meg Leta Jones notes, one goal of a right to erasure is to clean out stale personal data: "Information loses context over time. It becomes displaced from its original setting."[149]

Quite a number of privacy laws provide people with the right to demand deletion of personal data that is no longer necessary for the purposes for which it was collected.[150]

The right to delete unnecessary data is different from data retention limitations. The right to delete is a right invoked by a data subject. A data retention obligation requires that data be deleted regardless of whether a data subject had requested it. Although a right to delete unnecessary data can be valuable to data subjects under certain situations, data subjects will find it highly impractical to use this right more systematically. There are so many entities that gather and store personal data that it will be nearly impossible for people to identify them all, figure out which data is no longer necessary for the purposes originally collected, and then make the deletion request. In short, this right does not scale, and it is not a feasible way to ensure adherence to the principle of data minimization. A right to erasure is thus secondary to data retention limitations.[151]

Data minimization must have rigor. Otherwise, it becomes a hollow principle that sounds as though it is protecting privacy but is doing no actual work. Data minimization is difficult to police, as it involves relevance to purposes and involves judgment calls. But if it is not done rigorously, then data minimization is empty. Privacy laws often state data minimization principles without a practical way to enforce them, rendering them little more than hollow feel-good rhetoric.

F. RIGHT TO BE FORGOTTEN

The so-called "right to be forgotten" (sometimes referred to as the "right to oblivion") emerged from the right to erasure. The right to be forgotten requires the removal of personal data from search engine results if a valid request is made by an individual.

The right to be forgotten is often conflated with the right to erasure or deletion, but the two rights are distinct. The right to erasure requires destruction of data. The

[148] COPPA Rule, 16 C.F.R. § 312.10 ("An operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion."); **Cite other laws:** Costa Rica,

[149] MEG LETA JONES, CTRL+Z: THE RIGHT TO BE FORGOTTEN 123 (2016).

[150] GDPR art. 17, **cite other laws.**

[151] See Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 Wake Forest L. Rev. 433, 435 (2014) ("While businesses have legitimate reasons to use data in their day-to-day operations, a statutorily defined expiration period is necessary to preserve the data subjects' dignitary and autonomy rights.").

right to be forgotten, in contrast, does not involve deleting data. Instead, it is best characterized as a right to obscurity.[152] The data is not destroyed but is simply not publicly disseminated in search results.

The conflation of the right to erasure and the right to be forgotten is made in the GDPR, which puts the "right to be forgotten" in parentheses after the title to the section on the right to erasure.[153] But this section involves a right to erasure and does not address the right to be forgotten.

The right to be forgotten emerged from a judicial interpretation of the right to erasure under the EU Data Protection Directive, the predecessor to the GDPR. In *Google Spain v. AEPD* (2014), the EU Court of Justice (CJEU), a Google search of the name of a Spanish citizen returned a result with links to a Spanish newspaper with information about his debts. The person wanted Google to remove these items from search results under his name. The CJEU required that Google remove certain search results linked to a person's name.[154]

The right to be forgotten merely requires that search engines remove links to third party web pages when data is inadequate, irrelevant, or excessive. The underlying data does not have to be deleted. Thus, the newspaper websites with the data about the person's debts could continue to display the information. Nor did Google have to delete the information; it just was restricted from disclosing it in search results.

The GDPR, which was in the later stages of being forged when the right to be forgotten was born, attempts to codify the right to erasure by adding it in parentheses to the right to erasure. However, as Miquel Peguera observes, the GDPR's right to erasure "does not deal specifically with search engines. It also does not establish with particularity a data subject's right to request the delisting of links displayed in search engines' results for name-specific queries – in short, it does not codify *Google Spain*."[155]

Subsequent to *Google Spain*, judicial decisions have embraced a right to be forgotten in other countries, including Mexico, Japan, Russia, Colombia, and India.[156]

Certain laws in the US offer limited rights that resemble the right to be forgotten. For example, expungement allows juveniles to have conviction information sealed.[157] In 2013, California passed an "online eraser" law that provides children under 18 with a right to delete information they shared on social media.[158] These rights are much more limited than the broad right to be forgotten in the EU.

---

[152] Evan Selinger and Woodrow Hartzog, *Google Can't Forget You But It Should Make You Hard to Find*, Wired (May 20, 2014), http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/ ("[T]he talk about forgetting and disappearing is really concern about the concept of obscurity in the protection of our personal information.").
[153] GDPR art. 17.
[154] Google Spain SL v. Agencia Española de Protección de Datos, in the European Court of Justice, Case C-131/12, 2014 E.C.R. 317.
[155] Miquel Peguera, *The Shaky Ground of the Right to Be Delisted*, 18 Vand. J. Ent. & Tech. L. 507, 557 (2016).
[156] Dawn C. Nunziato, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to be Forgotten*, 39 U. Pa. J. Int'l L. 1011, 1059-64 (2018).
[157] *See infra*.
[158] Cal. Bus. & Prof. Code §§ 22580-81, S.B. 568, 2013 Leg. Rev. Sess. (Cal. 2013).

1. Obscurity

As mentioned above, the right to be forgotten is really a right to obscurity rather than a right to erasure. Privacy is not just about keeping secrets hidden away from everyone; it is also about modulating the accessibility of personal data and the boundaries of how it can flow.[159] As the U.S. Supreme Court stated in *DOJ v. Reporters Committee,* "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[160]

Obscurity of data has long been built into the social fabric. It has existed for centuries. As Woodrow Hartzog and Fred Stutzman contend, "people expect obscurity in everyday life."[161] Obscurity is a "middle ground protection" between the extremes of secrecy and being widely conspicuous.[162]

Before the Internet, much personal data was shielded through practical obscurity. Hunting for data from various sources was difficult and time-consuming. For example, obtaining information from public records would often involve traveling to many local government offices at great time and expense.

Digital technologies have greatly eviscerated practical obscurity.[163] Information is now vastly more accessible, which can thwart privacy expectations. What was once a needle in a haystack is now available at the click of a mouse.

To return to the example of public records, with the rise of the Internet, government entities have put their records online in electronic form, vastly increasing the accessibility of these records.[164] Large companies routinely vacuum up these records to compile massive databases of personal data about millions of people. This loss in obscurity results in uses of public records that are far beyond the original aims of freedom of information laws. These laws (also called sunshine laws) aim to make government activities more transparent. Today, public records are swept up *en masse* by Big Data corporations to construct gigantic databases about people. Instead of shedding light on the government, these databases are used to shed light on the lives of individuals.[165]

Enabling people to make right to be forgotten requests is woefully insufficient to address the problems caused by the loss of obscurity of personal data. As with other rights, the onus is placed on the individual to request that each search engine remove links to the data. It remains unclear whether the right would extend to many of the companies that are gobbling up all the data as their uses may fall under permissible grounds for data gathering without consent, such as legitimate purposes under the GDPR. And, in the US, no justification is needed.

---

[159] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).
[160] U.S. Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).
[161] Woodrow Hartzog & Fred Stutzman, The Case for Online Obscurity, 101 California Law Review 1, 8 (2013).
[162] *Id.* at _.
[163] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1176-78 (2002); Woodrow Hartzog & Frederic D. Stutzman, *The Case for Online Obscurity*, 101 Cal. L. Rev. 1 (2013).
[164] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137 (2002).
[165] *Id.*

Unfortunately, in *Google Spain,* the CJEU only vaguely conceptualized the right to be forgotten.[166] The CJEU did not specify the scope and applicability of the right, such as whether it extends beyond search engines. Although, the court noted that freedom of speech and the public interest in obtaining data are also to be considered in the balance, the court did not provide much guidance about how this balance should occur.[167] Instead, the court punted the balancing to organizations without sufficient oversight.[168]

In stats released by Google, there were about 800,000 requests in the year following the CJEU decision, with the number settling down to be consistently around 500,000 requests per year.[169] Roughly 50% of the delisting requests are granted and 50% are denied.[170] From the data supplied by Google, it is difficult to evaluate how well the delisting decisions are being made. The quantity of requests on its face might seem like a high number, but it is actually quite low when put in the context of the massive population of the EU plus the vast amount of visits to Google's site from the EU.

The right to be forgotten aims to achieve obscurity in a way that directly conflicts with free speech values. As Robert Post contends, the CJEU wrongly singled out search engines such as Google, characterizing them as mere profit-generating corporations. Instead, Post argues, "Internet search engines underwrite the virtual communicative space in which democratic public opinion is now partially formed."[171] The Internet would be "opaque" without the ability to locate information.[172]

In many of its applications, the right to be forgotten would run afoul of the First Amendment to the US Constitution, as it would bar the communication of potentially newsworthy information or information from court records or public records.[173] Thus, in the US, the First Amendment will significantly restrict the use of the right to be forgotten, leaving individuals without recourse.

Even without any First Amendment roadblocks, enabling people to make individual requests to be forgotten is not enough to protect them. Individuals who know how to make right to be forgotten requests and who are highly motivated might weary from the extensive labor of making requests. If Google were the sole repository of personal data in the world, the individual's burden might be eased, but Google is just one of many companies that maintain personal data that an

---

[166] Robert Post contends that the CJEU decision has inconsistencies and the CJEU wrongly theorized the right. Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right To Be Forgotten, and the Construction of the Public Sphere*, 67 Duke L.J. 981 (2018).

[167] The court stated: "Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."

[168] Patricia Sanchez Abril & Jacqueline D. Lipton, T*he Right to Be Forgotten: Who Decides What the World Forgets?*, 103 Ky. L.J. 363, 366 (2015).

[169] *Requests to delist content under European privacy law*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/eu-privacy/overview?hl=en_GB (last visited Oct. 17, 2021).

[170] *Id.*

[171] Post, *Google Spain, supra* note X, at 990.

[172] *Id.* at 1043.

[173] Dawn C. Nunziato, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to be Forgotten*, 39 U. Pa. J. Int'l L. 1011, 1042-46 (2018).

individual might want to be forgotten. Moreover, individuals might think that they are succeeding in zapping data from the Internet only to later discover that the same facts can be inferred from other data about them online.

As with other individual rights, the right to be forgotten fails to address the more systemic problem of the loss of obscurity. Large corporations can still vacuum up massive quantities of personal data. Obscurity is rapidly becoming extinct. A few individuals might fight back by requesting specific information be removed from specific sites, but these cases are far too isolated, fragmented, and specific to make a sufficient social impact.

As more thorough and effective way to build back obscurity in the digital age, the law should impose duties to preserve obscurity. For example, government entities should have a duty to protect privacy in their records. In many cases, records are just dumped online without considering the consequences. When the government makes records available, it should be required to conduct a privacy impact assessment and determine ways to protect the data from misuse. Some states have passed statues that limit the use of certain public records by making requesters agree to limitations in use in order to access the records.[174] All states should do so.

Duties can also be imposed on private sector entities that share data on individuals for various purposes. In US law, there actually is a limited requirement of forgetting under the Fair Credit Reporting Act (FCRA) – a provision that prevents consumer reporting agencies from reporting in certain instances bankruptcies that are more than 10 years old, as well as lawsuits, judgments, and criminal convictions that are more than 7 years old.[175] The law does not require that the information be deleted, just that it not be disclosed in credit reports. These restrictions do not depend upon individuals having to invoke them; they are automatic. More privacy laws should impose similar restrictions that do not put the onus on individuals.

Another US law, the Genetic Information Nondiscrimination Act (GINA), prohibits employers from obtaining employee or applicant genetic information except under certain limited circumstances.[176] This law does not focus on the erasure of genetic data; instead, it works by limiting dissemination, thus making the data more obscure. GINA is a direct restriction; it is not a right that individuals must invoke.

2. Second Chances

Another goal behind the right to be forgotten is to provide space for people to grow and to allow people to have second chances. As John Dewey aptly stated, a person is not "something complete, perfect, finished" but is "something moving, changing, discrete, and above all initiating instead of final."[177] People evolve and mature, a process impeded by shackling them to their past.[178]

---

[174] Law in LAPD case.
[175] FCRA, 15 U.S.C. 1681c(a)-(b).
[176] Genetic Information Nondiscrimination Act of 2008, Pub. L. 110–233, 122 Stat. 881.
[177] JOHN DEWEY, EXPERIENCE AND NATURE 167 (Jo Ann Boydston ed. 1987) (originally published in 1925).
[178] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 72-73 (2007).

As Viktor Mayer-Schonberger observes, the ubiquity of digital data creates a "synthetic past reconstructed from the limited information digital memory has stored about it, an utterly skewed patchwork devoid of time and open to manipulation."[179] He aptly contends that digital memory "denies development and refuses to acknowledge that all humans change all the time."[180]

Expungement is a longstanding variation of a right to be forgotten. In the law of the US and other countries, expungement involves destroying or sealing criminal justice records from court systems or police departments.[181] In the US, expungement has largely been an issue of state law.[182] Most states provide juveniles with a right to petition to expunge a conviction.[183]

In practice, expungement has several significant limitations. It only involves certain types of data (criminal justice data) from certain types of records (government records).[184] Expungement is also often a time-consuming process that involves considerable hassle.[185]

Expungement also fails to remove the data from other entities where it is available, such as newspapers or background check companies.[186] With modern technology allowing companies to vacuum up public record data and compile gigantic searchable databases of it and with the ready availability of archived news articles online, expungement has lost its efficacy in today's digital age.[187]

In the US, the First Amendment severely restricts the ability of privacy law to stop the media from continuing to make expunged data available.[188] Some media entities are attempting to revitalize expungement by removing information about people's identities from archived stories about criminal convictions.[189] These voluntary efforts are laudable, but they depend solely upon the discretion of the media organizations; the law cannot force them to do so. But the law could incentivize companies to provide for obscurity through carrots rather than sticks.

Ultimately, the responsibility to protect obscurity depends significantly on how the government manages its records. In many circumstances, the government does not adequately consider privacy when generating and disseminating records. For example, court records can contain data about bankruptcy, health, mental illness, sexual assault, and other sensitive matters. Protective orders could be used to shield some of the information, but ultimately, there might come a time when the information might be relevant to a judicial decision. Excluding the information might conflict with a fully transparent judicial decision, as the facts that a court is

---

[179] VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 123 (2009).
[180] *Id.* at 125.
[181] American Bar Ass'n, *What Is Expungement?* (Nov. 20, 2018), https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-_expungement-/.
[182] *Id.*
[183] Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 379 (2019).
[184] Brian M. Murray, *Newspaper Expungement,* 116 Nw. U. L. Rev. Online 68, 70 (2021).
[185] J.J. Prescott & Sonja B. Starr, *Expungement of Criminal Convictions: An Empirical Study*, 133 Harv. L. Rev. 2460, 2486 (2020).
[186] *Id.*
[187] JAMES JACOBS, THE ETERNAL CRIMINAL RECORD (2015).
[188] Cox Broadcasting v. Cohn, 420 U.S. 469 (1975); Smith v. Daily Mail Pub. Co., 443 U.S. 97 (1979); The Florida Star v. B.J.F., 491 U.S. 524 (1989).
[189] Murray, *Newspaper Expungement, supra* note X, at __.

relying upon are often essential to understanding and assessing the holding. A more viable option might be to allow a litigant to proceed under a pseudonym. Proceeding under a pseudonym might not be a perfect protection of privacy, but it might present enough obscurity to provide a meaningful degree of protection. Unfortunately, the decision about proceeding under a pseudonym is left to the discretion of judges, with courts rarely permitting plaintiffs to proceed under a pseudonym.[190] As one court held: "Lawsuits are public events. A plaintiff should be permitted to proceed anonymously only in those exceptional cases."[191]

However, even highly important cases have involved the use of pseudonyms without undercutting the integrity of the case. Many U.S. Supreme Court cases have involved pseudonymous litigants, such as Jane Roe in *Roe v. Wade*. Even on its own initiative, the Supreme Court changed a sexual assault victim's name to just initials in *Florida Star v. B.J.F.*[192]

A more systemic acceptance of using pseudonyms in civil litigation would help shield personal data from widespread exposure. The judiciary as well as government agencies are shirking their important responsibility to promote obscurity.

G. Rights to Objection and Restriction (or Opt Out)

The rights to objection and restriction are defined in separate articles of the GDPR, but they often work in tandem. At Article 21, the GDPR provides a right to object.[193] Data subjects can object at any time to the processing of personal data that is based on the lawful bases of public interest or legitimate interests. When a data subject objects, the burden is on the controller to "demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims."[194]

Under the GDPR Article 18, data subjects have a right to restriction – to request that a data controller stop processing their personal data under certain circumstances. These circumstances include when the data subject contests the accuracy of the personal data or when the data subject has objected to the processing.[195]

The right to object works in tandem with the right to restriction, but the rights are different. The right to restriction involves the temporary or permanent stoppage of processing. The right to object involves the grounds upon which data subjects may object to the processing of their data. One of the main grounds for restriction is a valid objection.

1. Objectionable Processing

Most privacy laws around the world give data subjects the ability to withdraw

[190] See Doe v. Blue Cross & Blue Shield United of Wisconsin, 112 F.3d 869 (7th Cir. 1997) ("The use of fictitious names is disfavored, and the judge has an independent duty to determine whether exceptional circumstances justify such a departure from the normal method of proceeding in federal courts.").
[191] Doe v. Frank, 951 F.2d 320, 323 (11th Cir. 1992).
[192] Florida Star v. B.J.F., 491 U.S. 524 (1989).
[193] GDPR art. 21.
[194] GDPR art. 21.1
[195] GDPR art 18.

consent from processing. When this right is invoked, further processing of the data must stop, unless there is another lawful basis to process it without consent.[196]

The rights to object and restrict place the onus on individuals to learn about the purposes of processing and raise objections. Only in rare circumstances will individuals do so.

The rights to object and restrict are limited. The GDPR does not provide people with a right to stop the processing of their data whenever they desire. Instead, data processing is only stopped when data processing is in violation of the law or no longer with a legal basis.

Although similar to the right to object, the right to withdraw consent and stop processing is both broader and narrower. It is broader because consent can be withdrawn for any reason whereas the right to object must involve unjustifiable processing. The right to withdraw consent is also narrower because it only involves situations where data is being processed with consent. If the data is processed under other lawful bases that do not involve consent, then this right does not apply. In many cases, personal data is processed without consent. The right to object can only be invoked when data is processed pursuant to the public interest or to legitimate interests.

2. Opt Out or Opt In

In the US, only a few laws provide a similar right to restrict processing, though many laws provide related rights of opt out or opt in. Opting out involves taking action to choose not to have personal data collected, used, or disclosed.[197] In contrast, opting in means that people have to take an affirmative action to indicate consent, such as to check a box.[198]

Opt out rights are a close cousin of restriction or objection rights. All of these rights involve individuals taking an affirmative step to stop certain types of processing of their data.

The GDPR clearly rejects consent based on inaction, so opt out is out. In the US, privacy law is divided between opt-in laws and opt-out laws. Examples of opt-in laws include HIPAA for all uses and disclosures beyond those for treatment, payment, or healthcare operations, and the Children's Online Privacy Protection Act (COPPA).[199]

Many laws use a mix of opt-ins and opt-outs. For example, the federal Video Privacy Protection Act (VPPA) has an opt in for most types of sharing of personal data but an opt out for sharing names, addresses, and the subject matter of videos for marketing.[200] The Cable Communications Policy Act has an opt in for personal data about cable subscribers but an opt out for just the subscribers' names and addresses.[201]

A large number of US privacy laws provide opt out rights. As discussed above, opt

[196] GDPR art. 7.3
[197] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (7th ed. 2021).
[198] *Id.*
[199] HIPAA, 45 C.F.R. §164.508(a); Children's Online Privacy Protection Act, 15 U.S.C. §6502(b).
[200] VPPA, 18 U.S.C. §2710(2)(B) (opt in); 18 U.S.C. §2710(2)(d) (opt out).
[201] Cable Communications Policy Act, 47 U.S.C. §551(c)(1) (opt in); 47 U.S.C. §551(c)(2) (opt out).

out is part of the notice-and-choice approach, where consent is presumed from inaction (the failure to out out). The GLBA, CAN-SPAM Act, TCPA, and other laws rely heavily on opt out rights.

The emerging breed of state laws regulating privacy also relies heavily on opt out rights. Although the CCPA defines consent as "any freely given, specific, informed and unambiguous," it mostly provides opt out rights.[202] The CCPA is obsessed with data transfer; other uses of personal data are mostly not covered. Thus, the CCPA allows individuals to opt out of the sale or sharing of their personal data, but not most uses that data controllers will undertake.[203] Similar opt out rights are provided by VDCPA and the Colorado Privacy Act.[204]

Some privacy laws attempt to strengthen opt out rights by making the mechanisms to opt out more conspicuous and easy. For example, under the CCPA, businesses must provide a clear and conspicuous link on their internet home page titled "Do Not Sell or Share My Personal Information" that allows a consumer to opt out of the sale or sharing of their personal information.[205]

However, providing buttons still does not address the problematic fictions of consent that pervade the notice-and-choice approach. Even when opt out is conspicuous, people often do not want to undertake the chore of opting out.

3. Control Over Personal Data

Another goal of the rights of objection, restriction, opt in, and opt out is to give people control over their personal data. These rights, however, often just provide the illusion of control. Moreover, as Ari Waldman aptly observes, "Rights of control still require individuals to overcome every trick designed into platforms that encourage inertia or inaction or disclosure."[206]

The EU approach in the GDPR is to require a valid justification for data processing. This restrictive approach is generally avoided in the US, which has a general philosophy that if there is no harm, then companies should be able to use data in whatever ways they desire.

Even with the EU approach, the right to object can readily become an exercise in documentation. If a data controller has documented the legitimate interest and how the processing will not override data subject rights and interests, the controller can overcome an individual's objection. The onus remains on the individual to object, and most people will not have the time or wherewithal to object systematically to make a palpable difference for their privacy.

In the US, opting out puts the onus on the individual. Opting in is better, as it does not rely on the fiction that inaction means consent, but once a person has opted in, the onus is on the individual to monitor the use to ensure that the data is being used properly.

---

[202] CCPA, 1798.140(h).
[203] CCPA 1798.140(20).
[204] VDCPA, § 59.1-573(A)(5); cite to Colorado law.
[205] CCPA, 1798.185.
[206] ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 107 (2021).

It can be easy to entice people to opt in with discounts or with other means. For example, after the GDPR became effective in 2018, many websites added cookie notices to obtain affirmative consent for the use of cookies. On the surface, the cookie notices appear as though privacy law has achieved a great success, as the cookie notices generate many people clicking on a button to accept them. Ironically, though, the cookie notices are actually creating a fictitious consent. Many cookie notices pop up as a person immediately as that person visits a website, and they present the choice to accept cookies or click a button for other options. People do not want to take the time to explore the other options; they want to go to the site. Many are likely to click to accept the cookies rather than go through the detour. This is one way that organizations can get people to opt in even when they really are not really consenting.

Another way that this method of obtaining opt in consent is used is by presenting people with a lengthy terms of service or other long and cumbersome documents that nobody will read. People must click that they accept these terms or agree to these documents. This is meaningless opt in consent. In is a formalistic exercise that makes people appear to opt in, but it fails to reflect actual informed consent.

As discussed earlier, the law too often will be satisfied with formalities rather than real meaningful requirements. Formalities end up creating fictions that look good on the surface but are hollow underneath. Stating the use in a privacy notice that nobody reads fails to factor meaningfully in people's forming their expectations. This approach would move away from the maligned and discredited notice-and-choice approach. Sites can also get nearly everyone to click an accept button with hardly anyone understanding what they have accepted or even wanting to accept.

The law can protect privacy in far more effective ways than putting the onus on people to figure out the complex and intricate dimensions of privacy and the possible risks and consequences of allowing the collection, use, or disclosure of their personal data. The law should define at least the basic boundaries of data use.

Data should be processed in ways consistent with people's expectations. Existing privacy law allows for processing that might be unexpected for many people as long as the processing is mentioned in a privacy notice. As discussed above, most people do not read privacy notices, so this approach does not work. Instead, the law should focus on expectations. The burden should be on organizations to prove that they took reasonable measures to ensure that a data use was not unexpected.

I. RIGHT TO NOT BE SUBJECT TO AUTOMATED DECISIONS

The GDPR provides individuals with a "right not to be subject to a decision based solely on automated processing, including profiling."[207] Individuals have the "at least the right to obtain human intervention . . . to express his or her point of view and to contest the decision."[208]

The privacy laws of a few countries provide for a similar right, though most countries still do not recognize this right.[209] Brazil's LGPD provides data subjects

[207] GDPR, *supra* note X, art. 22(1) ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").
[208] Id. at art 22(3).
[209] Lei Geral Da Proteção De Dados Pessoais (LGPD), Lei No. 13.709, de 14 de Agosto de 2018, DIÁRIO

with a right to request a review of decisions made solely based on automated processing.[210] Controllers must disclose the criteria and procedures used for an automated decision, but the disclosure can be restricted to protect commercial secrecy.[211] Some laws only apply when the process produces negative or harmful effects to data subjects (Panama); other laws apply regardless of the harmfulness of the effects (GDPR).[212] Similar to the GDPR, the CCPA provides consumers with rights to opt out of automated decision-making, to learn about the algorithmic logic involved, and to know about the likely outcome.[213]

The GDPR provides for exceptions to this right, such as if the decision is necessary for a contract between the data subject and the controller, if it is authorized by the law of a union or member state of which the controller is subject, or if individuals provide explicit consent.[214]

1. Algorithmic Transparency

Several articles of the GDPR provide supporting rights to the automated processing right by requiring a limited degree of algorithmic transparency: Controllers must inform data subjects about the existence of automated decision-making, meaningful information about the logic involved, and the contemplated consequences.[215]

Algorithmic transparency is not a panacea because the logic of many algorithms evolves and is dependent not just on an individual's data but on the collective personal data of everyone. Algorithms find patterns in the aggregated data. To understand why a particular algorithm made a particular decision about a person, not only would one need to know the individual's data and the logic of the algorithm but also the data of other people used by the algorithm. But this data cannot be provided without compromising the privacy of other individuals.

For meaningful transparency, automated decisions should be understandable. With machine learning, however, automated decisions can become quite complicated. Even with transparency, the decisions can be problematic and unfair. Transparency is thus important, but it is far from enough to protect people from

---

OFICIAL DA UNIAO [D.O.U.] de 15.08.2018 (Braz.), translated in Brazilian General Data Protection Law (LGPD, English Translation), International Association of Privacy Professionals, (https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/) ("The data subject has the right to request for the review of decisions made solely based on automated processing of personal data affecting her/his interests, including decisions intended to define her/his personal, professional, consumer and credit profile, or aspects of her/his personality.").

[210] LGPD, *supra* note X, at _ ("The data subject has the right to request for the review of decisions made solely based on automated processing of personal data affecting her/his interests, including decisions intended to define her/his personal, professional, consumer and credit profile, or aspects of her/his personality.").

[211] Id. § 20(1) ("Whenever requested to do so, the controller shall provide clear and adequate information regarding the criteria and procedures used for an automated decision, subject to commercial and industrial secrecy.").

[212] Panama's Law No. 81 on Personal Data Protection; GDPR art. 22(1).

[213] CCPA, Cal. Civ. Code § 1798.185(a)(16) (mandating that the Attorney General issue regulations that businesses disclose "meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.").

[214] GDPR, art. 22(2).

[215] GDPR, art. 13(2)(f) and 14(2)(g) use identical language about informing data subjects about "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." See also id. art. 15(1)(h).

problems caused by algorithmic decisionmaking.

2. Control of Inferences

The GDPR focuses on "automated" decisions, but automation is not really the key feature of what makes certain decisions problematic. A more apt focus is on the use of inference in decisions.[216] Inference involves using existing data to generate new data about a person or to make predictions about them. Inference, much more than automation, is what the law should regulate.

In practice, it remains unclear how broadly the GDPR automated decisionmaking right applies. As Aziz Huq points out, the GDPR leaves "[t]he precise range of automated machine-learning tools captured by the prohibition . . . up for grabs."[217] Margot Kaminski and Jennifer Urban observe that the "GDPR's right to contestation exists largely for now as a standard, rather than a set of specific procedural rules."[218] They further note that "Companies must allow individuals to challenge an automated decision, but there are as of yet few details about what that process must be."[219]

Restrictions on automated decisionmaking can be limited because any human involvement, even small, can make the right inapplicable, since the right involves a decision is based "solely" on automated processing. Avishai Ostrin contends that the right should be recrafted to "apply not only to decision-making algorithms but also to decision-aiding algorithms."[220]

Decisions made by humans based on data can be as problematic as automated decisions - or even worse. Margot Kaminski notes that "adding a human in the loop" could create problems, such as making "accuracy of the overall system worse, thus negatively impacting other individuals subject to the algorithm."[221]

Solon Barocas and Andrew Selbst note that automated decisions can transform bias in previous decisions into a "a formalized rule" that would have systematic effects.[222] To make matters worse, automated decisions are often mischaracterized as being free from any human taint when, in fact, they are affected by humans. As Ifeoma Ajunwa observes, "the human hand remains present in all automated decision-making."[223] Algorithmic decisions are often viewed as "oracular proclamations; they are accepted at face value without any attempt to analyze or

---

[216] Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, https://ssrn.com/abstract=3921003 (Sept. 10, 2021); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 Colum. Bus. L. Rev. 494 (2019).

[217] Aziz Z. Huq, *A Right to A Human Decision*, 106 Va. L. Rev. 611, 623 (2020).

[218] Margot E. Kaminski & Jennifer R. Urban, *The Right to Contest AI,* 121 Colum. L. Rev. 1957, 1981 (2021).

[219] *Id.* at 1981-82.

[220] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529, 1614 (2019). ("[I]t may be the case that adding a human in the loop will respect individual dignity but could make accuracy of the overall system worse, thus negatively impacting other individuals subject to the algorithm.").

[221] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529, 1614 (2019). ("[I]t may be the case that adding a human in the loop will respect individual dignity but could make accuracy of the overall system worse, thus negatively impacting other individuals subject to the algorithm.").

[222] Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671, 682 (2016);

[223] Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 40 Cardozo L. Rev. 1671, 1681 (2020).

further interpret them."[224]

Privacy law often addresses algorithmic decisionmaking superficially. A right for individuals to correct data in their records is inadequate to address situations where patterns in data might reflect biases, prejudice, and inequality.[225] The algorithm may be unobjectionable, and the data may be correct. But a problem may exist because people's behavior is based on prejudice. Data is no better than the people and society that produces it.

Algorithmic decisions tend to ossify prejudices. As Anupam Chander observes, "[a]lgorithms trained or operated on a real-world data set that necessary reflects existing discrimination may well replicate that discrimination."[226] Algorithms can amplify prejudice in existing data by using it in a widespread systematic way.

Providing people with a right to stop solely automated decisionmaking about them is an insufficient response to these problems. Discriminatory algorithms do not just affected isolated individuals; they are harmful to society.

Decisions should be reviewed for accuracy, fairness, as well as values. Regulation of inferential decisionmaking could mandate review of the output of the inferential logic. As Cathy O'Neil notes, data is often not gathered on those whom an algorithm gets wrong.[227] Algorithms can "generate their own reality" by reinforcing their own decisions.[228] O'Neil contends that "many poisonous assumptions are camouflaged by math and go largely untested and unquestioned."[229]

Of course, the algorithms might make better decisions than humans, but as Barocas and Selbst argue, "victims of inaccurate determinations may find cold comfort in the fact that certain decisions are rendered more reliably overall when decision makers employ data mining."[230] Algorithms can shift who wins and loses in certain types of decisions, but it does so in a way that is more permanent, systematic, opaque, and unquestioned.[231]

Privacy rights often totally miss the mark when addressing the problems. Privacy rights will focus on whether an individual's records were correct, whether the individual consented to the collection of her data, and so on. But the problem cannot be solved on the individual level. For example, the rights that FCRA provides ultimately do not challenge the FICO system of credit scoring. Individuals can correct errors, but they have no input or recourse about the way judgments are made about their credit. As long as individuals are given access and can correct records, the consumer reporting agencies can largely make the judgments they please. The law fails to address any problems and unfairness created by the formulas that the consumer reporting agencies use.

The missing dimension is that the law fails to provide protections to ensure that inferential decisions about people are made fairly, accurately, and consistently

[224] Ajunwa, *Paradox of Automation, supra* note X, at 1688.
[225] Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. Davis L. Rev. 133, 190 (2017).
[226] Anupam Chander, *The Racist Algorithm?*, 115 Mich. L. Rev. 1023, 1036 (2017).
[227] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 133 (2016).
[228] *Id.* at 133.
[229] *Id.* at 7.
[230] *See* Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671 (2016).
[231] O'NEIL, WEAPONS OF MATH DESTRUCTION, *supra* note X, at _.

with important societal values. The law must bring the massive web of inferential decisions about people under control, to address their skewed assumptions, troubling output, amplification of prejudice, and their massive troubling effects on society.

CONCLUSION

Although individual rights are an important part of privacy law, they are no match for many privacy problems. Rights function at an individual level, with the onus being on individuals to invoke them. Rights mainly function to give individuals the ability to have some participation in the activities involving their data, but they are not an effective way to regulate privacy. Far too often, however, privacy laws rely heavily on rights as the primary engine of protecting privacy. Rights are ill-suited for this role.

A small percentage of individuals might exercise a few rights, and they will perhaps feel the illusion of empowerment. But they lack enough knowledge to be empowered.

Rights are very limited in how much they can help a person, and they take a lot of work to use. Effective regulation of privacy must be done more systematically at a societal level in a way that does not put the onus on individuals.

Privacy law focuses on the surface. It looks at whether data is correct rather than whether data leads to good judgments about people. It looks to whether formalities were followed such as providing people with information rather than to whether people are actually informed. It looks to whether people are provided with rights to delete and correct rather than to whether organizations are engaging in data minimization and data quality.

Rights are a convenient way to make it look like privacy is being protected. In practice, rights become a set of chores that are nearly impossible to do at the necessary scale. The failure of rights can then be blamed on individuals not caring enough to exercise them.[232]

Privacy cannot be solved at the individual level. Rights should certainly be part of privacy laws, but they can only play a small supportive role. Meaningful protection must be large-scale and structural in nature.

[232] Daniel J. Solove, *The Myth of the Privacy Paradox,* 89 Geo. Wash. L. Rev. 1 (2021).