"SLACK" IN THE DATA AGE

Shu-Yi Oei & Diane M. Ring

"SLACK" IN THE DATA AGE

Shu-Yi Oei & Diane M. Ring***

This Article examines how increasingly ubiquitous data and information affect the role of "slack" in the law. Slack is the informal latitude to break the law without sanction. Pockets of slack exist for various reasons, including information imperfections, enforcement resource constraints, deliberate nonenforcement of problematic laws, politics, biases, and luck. Slack is important in allowing flexibility and forbearance in the legal system, but it also risks enabling selective and uneven enforcement. Increasingly available data is now upending slack, causing it to contract and exacerbating the risks of unfair enforcement.

This Article delineates the various contexts in which slack arises and presents a bounded defense of slack, despite its risks and notwithstanding the parallel existence of formal leniency provisions in the law. It explains how increasingly available data is reshaping slack and highlights the risk of disparate contraction of slack for different populations along lines of race, political power, and sophistication. Ultimately, this Article proposes a framework for managing the complex relationship between slack and data and suggests policy solutions to address data-driven contraction of slack while minimizing slack's risks. These policy solutions include limits on data collection, construction of data silos, and fundamental rethinking of legal rules and the role of government.

INTRODUCTION

We live in an age of ubiquitous data.[1] Large stashes of data are increasingly being collected, processed, and used for a wide range of purposes, including surveillance, marketing, development of algorithms, and fighting crime.[2] In this Article, we focus on one important consequence of increasingly ubiquitous data for the legal system: how growing access to data and information has changed the availability and operation of "slack" in the law.

"Slack" is informal latitude.[3] While humans often break the law, noncompliance is not always punished in practice—there have long been informal pockets of leeway or slack in the system, instances in which someone may fall short of legal or regulatory compliance but not be sanctioned.[4] Slack

* Professor of Law & Dean's Distinguished Scholar, Boston College Law School.

** Professor of Law & Dr. Thomas F. Carney Distinguished Scholar, Boston College Law School.

We are grateful to the participants of the Cornell Law School Faculty Workshop, the University of South Carolina Law School Faculty Workshop, the Yale Law School Information Society Project Ideas Lunch Workshop, the Critical Tax Theory Workshop UC Irvine, Law & Society Conference 2021, and tax policy workshops at New York University, Northwestern, Duke, and University of Toronto law schools, for helpful feedback on drafts.

1. *See The Privacy Project*, N.Y. TIMES (Apr. 16, 2019 to Dec. 19, 2019), https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html (exploring technology, data, and privacy). The analytics field distinguishes data, information, and insights. We use the term "data" as a shorthand.

2. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (noting dangers of using data for surveillance); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017) (discussing algorithmic accountability).

3. *See Slack*, OXFORD ENGLISH DICTIONARY (2d ed. 1989).

4. *See* Woodrow Hartzog et al., *Inefficiently Automated Law Enforcement*, 2015 MICH. ST. L. REV. 1763, 1780 (2015).

captures the phenomenon whereby violations of laws or regulations are let slide in ways not formally specified in advance. The concept refers to extra-legal spaces in which governments, regulators, and other enforcers exercise discretion in deciding not to notice, not to sanction, or to sanction less harshly than the law stipulates, whether driven by information imperfections, deliberate underenforcement, resource constraints, politics, bias, or luck.[5]

Being *informal* latitude, slack exists on top of deliberately designed formal legal provisions that provide leniency and discretion (such as tiered penalties, broad standards, and other equitable features).[6] Thus, there is an argument that these formal equitable provisions are sufficient, and that slack on top of them is unnecessary, not to mention problematic. This Article argues, to the contrary, that slack remains important over and above formal equitable and leniency provisions, and that it should be safeguarded in the face of increasingly available data.

Most people intuitively understand that some slack in the system is desirable. For example, where a law is out of date or contains overly harsh penalties, slack in the sense of underenforcement can help prevent injustice. On the other hand, it is also widely recognized that some groups are routinely and systemically cut more slack than others.[7] Thus, slack in the legal system is sometimes deeply problematic. This Article presents a framework for systematizing these intuitions and for understanding how data changes the operation and existence of slack.

This Article undertakes three tasks. First, it delineates the varied contexts in which slack arises, identifies its major risks, and presents a bounded defense of the important role slack plays in the legal system, even on top of formal equitable features in the law. Despite its potential risks, slack acts as a constraint on too much law, protects against excessive government incursion into personal spaces, and provides a necessary second space for substantive debate given imperfections in our political and legislative process.[8] Slack thus acts as a safety valve in the legal system. Second, this Article explains how increasingly ubiquitous data and information put pressure on slack and cause it to contract disparately for different populations, with unfair and increasingly serious distributive impacts. Finally, this Article proposes a framework for understanding and managing the relationship between slack and data, designed to prevent problematic data-driven contractions of slack while minimizing slack's risks. It makes concrete policy recommendations, including limitations on data collection, construction of data silos, and ultimately, rethinking of the

5. *See id.*

6. In close cases, it may be hard to distinguish formal equity from informal slack. *See* discussion *infra* Part I.A.

7. *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 195 (1968).

8. *See* Christina M. Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH. J.L. & TECH. 36, 39–40, 44–45 (2008).

design of legal rules and sanctions and reconceptualization of the role of government in the data age.

A simple initial hypothetical may help highlight the tensions with which this Article is concerned. Imagine that you steal a pumpkin off your neighbor's porch. Will your larceny be punished? There are various scenarios under which it might not be, including if the authorities don't catch you, if they see but ignore you, or if they catch you but let you off the hook. These scenarios may be a function of luck (for example, whether the police happened to drive by, or whether they were in a good mood and did not arrest you), deliberate policy (for example, the number of patrols assigned to your neighborhood), bias (for example, based on your race), or unspoken norms (for example, if pumpkin larceny is a well-tolerated neighborhood joke).[9]

Now imagine a significant influx of data and information, for example, due to public or private security camera surveillance or facial recognition technologies.[10] These technologies may change behavior and punishment in a number of ways. They obviously make catching you easier. They may also make it harder for law enforcement to ignore you, particularly if your theft is more visible to outside observers who may complain about nonenforcement. There may be collateral consequences: once you have become ensnared in the enforcement web, you are more likely to be sanctioned for other (past and subsequent) offenses.[11] You yourself might stop stealing pumpkins if you think the chances of getting punished are higher.[12] On the other hand, if the increased visibility is not salient to you, you might continue stealing pumpkins.

This pumpkin hypothetical illustrates the complex ways in which slack arises, highlighting the role of information constraints, other resource constraints, selective enforcement, deliberate nonenforcement, biases, norms, and luck in creating and shaping slack. The hypothetical also shows how increased data and information might reshape slack and cause it to contract, and how both behaviors and enforcement choices may shift in response.

Further reflection on this hypothetical may also yield other insights. First, how we view slack and the impact of data on slack surely depends on the law in question; serious crimes like murder or assault will likely provoke different reactions than minor offenses like purloining a pumpkin. One might also expect a range of different feelings about medical marijuana laws;[13] laws prohibiting

9. *See generally* Becker, *supra* note 7 (arguing that the optimal amount of crime is not zero).

10. *See, e.g.*, Cade Metz, *Facial Recognition Tech is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

11. *See, e.g.*, Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOCIO. REV. 977, 986–87, 990–92 (2017) (noting that big data surveillance leads to predictive policing, more surveillance of those without previous police contact, and merging of previously separate data systems).

12. Becker, *supra* note 7 (positing rational criminal actors).

13. Michael Hartman, *Cannabis Overview: Legalization*, NAT'L CONF. OF STATE LEGISLATURES (July 6, 2021), http://www.ncsl.org/research/civil-and-criminal-justice/marijuana-overview.aspx (summarizing laws

adultery, fornication,[14] or sodomy;[15] prohibitions against physician-assisted suicide;[16] unjust laws; laws out of step with societal expectations; or areas of complex regulation such as banking or securities law.[17]

Second, uncomfortable tensions and deeply problematic practices lurk within our seemingly benign pumpkin hypothetical. A longstanding practice of looking the other way when pumpkin theft occurs between neighbors in a well-to-do neighborhood is likely to be a function of factors such as race, socioeconomic status, differential power, or other favored status.[18] If this degree of slack is not enjoyed by other communities, slack's contraction in these circumstances arguably might be viewed as positive. This ties to a third and broader point: our reaction to slack is expected to be context dependent, operating in relative rather than absolute terms. For example, if we observe that slack is shrinking disproportionately for certain populations (for example, communities of color) but not others given increasing data, we might be troubled by such uneven contraction, and might object even though the initial slack might itself have been undesirable.[19]

In short, this Article's analysis speaks to a fundamental issue confronting legal systems today: the merits of flexibility and forbearance in the law have long been in tension with the risks of selective and uneven enforcement. Slack sits at the heart of this tension, in that it facilitates the former but also enables the latter. Now comes data, which will almost certainly upend how slack operates and will thus alter the balance between law's flexibility and law's selective unfairness. Unsurprisingly, contemporary views on the relationship between data and slack reflect deep ambivalence: Most people intuitively recognize that slack holds risks, can be unfair, raises separation of powers concerns, and can create incentives to pass or retain bad laws.[20] Yet, many would argue that data's promise of more comprehensive observability and sanctioning of human conduct is also problematic, and that it is important to

decriminalizing medical marijuana); *State Medical Marijuana Laws*, NAT'L CONF. OF STATE LEGISLATURES (Aug. 23, 2021), http://www.ncsl.org/research/health/state-medical-marijuana-laws.aspx.

14. *See, e.g.*, MINN. STAT. § 609.34 (2020) (making fornication a misdemeanor); 720 ILL. COMP. STAT. § 5/11-40 (2011) (making fornication a Class B misdemeanor); S.C. CODE ANN. § 16-15-60 (1962) (criminalizing adultery and fornication; imposing fines and jail time); MICH. COMP. LAWS § 750-30 (1931) (making adultery a felony).

15. Sodomy laws were in place in the U.S. as recently as 2003. *See* Lawrence v. Texas, 539 U.S. 558, 563 (2003).

16. Physician-assisted suicide is legal in a minority of U.S. states but is a felony in others. *See generally Assisted Suicide Laws in the United States*, PATIENTS RIGHTS COUNCIL (Jan. 6, 2017), http://www.patientsrightscouncil.org/site/assisted-suicide-state-laws/.

17. *Cf.* Zachary S. Price, *Politics of Nonenforcement*, 65 CASE W. RES. L. REV. 1119, 1146 (2015) (discussing troubling dynamics that stem from not enforcing problematic laws).

18. *See* discussion *infra* notes 100–101.

19. *See generally* Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html.

20. *See* Price, *supra* note 17.

retain flexibility.[21] We therefore need a framework for analyzing how slack should interact with data and for considering how to safeguard some slack in the system while managing its risks. This Article provides that framework.

Part I explains the concept of slack or informal latitude in the legal system, maps the various ways it arises, and presents a bounded defense of slack, which recognizes its value while also acknowledging its potential risks and problems. In the interests of coherence, we largely focus on criminal law and regulatory compliance (such as taxation and licensing). But similar issues arise in private law as well. Part II discusses the effects of increasingly ubiquitous data on slack, emphasizing how data causes some types of slack to shrink, and to shrink more for some groups, such as less sophisticated populations and demographics subject to targeted enforcement. Part III articulates a framework for conceptualizing and managing the relationship between slack and data and proposes concrete policy solutions.

Our Article's focus on slack connects with themes raised by other scholars, including privacy, technology, and the harms of surveillance.[22] The literature has become increasingly attuned to the effects of data on the operation and social meaning of the legal system, and innovative proposals floated by others reflect some of these tensions and concerns.[23] Recent examples ask whether making crime impossible using technology (such as maximum vehicle speeds or algorithms that force compliance) is desirable,[24] whether there is a right to break the law,[25] or whether "personalized law" should play a greater role in legal system design in the age of technology.[26] The intuition behind these proposals is that data and technology may require fundamental shifts in how law is

21. *See*, *e.g.*, Richards, *supra* note 2.

22. *See, e.g.*, Alessandro Acquisti et al., *The Economics of Privacy*, 54 J. ECON. LITERATURE 442 (2016) (surveying privacy literature and tradeoffs); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547 (2017); Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425 (2017); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); *cf.* ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY 5 (2003) (studying privacy prior to the data age); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008); Joshua D. Blank, *Reconsidering Corporate Tax Privacy*, 11 N.Y.U. J.L. & BUS. 31 (2014); Jannis Kallinikos, *Reality Regained: An Inquiry into the Data Age*, MIT TECH. REV. (Feb. 15, 2019), https://www.technologyreview.com/s/612818/reality-regained-an-inquiry-into-the-data-age/.

23. *See, e.g.*, William Magnuson, *A Unified Theory of Data*, 58 HARV. J. LEGIS. 23 (2021); Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance*, 131 YALE L.J. (forthcoming 2021).

24. Michael L. Rich, *Should We Make Crime Impossible?*, 36 HARV. J.L. & PUB. POL'Y 795, 796 (2013); *see also* Edward K. Cheng, *Structural Laws and the Puzzle of Regulating Behavior*, 100 NW. U. L. REV. 655, 657 (2006); Hartzog et al., *supra* note 4. Such shifts may change the fundamental architecture of how conduct is regulated. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 43–44 (1999).

25. *See* Timo Rademacher, *Of New Technologies and Old Laws: Do We Need a Right to Violate the Law?*, 5 EUR. J. FOR SEC. RSCH. 39–58 (2020).

26. *See, e.g.*, Anthony J. Casey & Anthony Niblett, *The Death of Rules and Standards*, 92 IND. L.J. 1401 (2017); Anthony J. Casey & Anthony Niblett, *A Framework for the New Personalization of Law*, 86 U. CHI. L. REV. 333, 333 (2019) (arguing the personalization of law captures "[t]he idea that the law should be tailored to better fit the . . . context.").

designed and enforced. However, the literature has yet to tackle the issue of diminishing slack head on.

Our Article fills this void. Slack has long existed in law, often without fanfare or explicit recognition. Data has the potential to fundamentally transform the existence and significance of slack, and with it, the relationship among humans, governments, and law, ultimately calling many aspects of legal system design into question. Regardless of our attitudes towards slack, these dynamics ought to be better understood and managed.

I. SLACK: THE INFORMAL LATITUDE TO FALL SHORT

Legal systems intentionally incorporate flexibility and nuance through various means. Among the most traditional are the use of broad standards (such as willfulness or reasonableness), equitable relief, and penalty ranges.[27] These features may be written into statutes, may exist due to agency action, or may emerge from case law. Through them, the legal system acknowledges that not every violation of law should or will be sanctioned once equitable and contextual factors are considered.

Beyond formal features, however, legal systems universally tolerate informal spaces where law is not enforced and where those who violate it are not sanctioned.[28] In this Part, we describe this informal "slack" and discuss how it relates to formal flexibility and leniency (I.A). We then articulate a taxonomy of the various causes and sources of slack in the legal system (I.B) and present a bounded argument in favor of preserving some slack in the legal system, even conceding its risks (I.C).

A. Slack

"Slack" refers to informal spaces in which governments, regulators, and other enforcers[29] apply discretion in acknowledging violations, sanctioning, or sanctioning less harshly than the law specifies.[30] Additionally, this includes cases in which enforcers, hampered by limited resources, lack the information needed to enforce. Importantly, we distinguish slack from formal equitable features. Our definition raises questions at the boundaries but is a useful starting heuristic.

---

27. *See infra* notes 31–45 and accompanying text.

28. *See* CAL. PENAL CODE § 459.5 (2014); *see also* Lee Ohanian, *Why Shoplifting Is Now De Facto Legal in California*, HOOVER INSTITUTION (Aug. 3, 2021), https://www.hoover.org/research/why-shoplifting-now-de-facto-legal-california (explaining how the shoplifting statute is not enforced and violators are not prosecuted in California).

29. This might include third-party enforcers, such as corporations who conduct diligence on behalf of legal authorities in exchange for deferred- or non-prosecution or who serve as withholding agents in tax law.

30. ROBERT E. WORDEN & SARAH J. MCLEAN, *Police Discretion in Law Enforcement*, *in* ENCYCLOPEDIA OF CRIMINOLOGY AND CRIMINAL JUSTICE 3596 (Gerben Bruinsma & David Weisburd eds., 2014).

To see the difference between formal flexibility and informal slack, it is helpful to look at criminal law. Formal equitable features are commonplace in criminal statutes, taking the form of tiered penalties or tiered severity of crimes.[31] For example, a crime initially classified as a misdemeanor may be upgraded to a felony subject to graduated penalties if aggravating factors exist (such as use of a weapon, death, or bodily injury).[32] Federal criminal statutes—including statutes criminalizing assault, arson, and interference with federally protected activities such as voting—routinely incorporate graduated penalties and categories of offenses.[33] For example, assault of officers and employees of the United States is subject to enhanced penalties if a deadly weapon is used or the assault results in bodily injury.[34] While such provisions may not explicitly describe their features as "equitable," adoption of tiered sanctions reflects law's understanding that differing circumstances may render a crime more or less severe, which in turn anticipates taking facts, circumstances, and equities into account in rule design.

Beyond this formal flexibility, however, a good deal of conduct covered by criminal statutes goes unpunished or is informally let slide. This may be due to deliberate resource-allocation decisions, plain luck, targeted non-enforcement—including due to biases for or against certain groups—or idiosyncratic actions of on-the-ground enforcers (for example, a decision to not arrest a first-time offender but instead let them go with a warning).[35]

The interaction of formal equitable provisions and informal slack can also be observed in regulatory areas such as tax. Formal tax law includes graduated penalties that reflect the broad range of reasons that taxpayers fail to comply.[36] Minor noncompliance may simply require payment of the additional tax due plus interest.[37] More significant noncompliance, such as failure to withhold sufficient tax during the tax year, may trigger nondramatic monetary penalties.[38] More serious violations may trigger civil fraud penalties.[39] Finally, taxpayers

31. *Degree of Crime,* BLACK'S LAW DICTIONARY (11th ed. 2019).

32. *See, e.g.*, 18 U.S.C. § 242 (allowing for an upgrade of a misdemeanor offense of deprivation of rights under color of law to a felony if aggravating factors exist).

33. *See, e.g.*, 18 U.S.C. § 113 (providing more severe penalties for assault resulting in serious bodily injury); 18 U.S.C. § 81 (authorizing more severe penalties for arson if life is placed in jeopardy); 18 U.S.C. § 245(b) (allowing for graduated consequences for interference with federally protected activities if aggravating circumstances exist).

34. 18 U.S.C. § 111.

35. *See* Wayne R. LaFave, *The Police and Nonenforcement of the Law—Part 1*, 1962 WIS. L. REV. 104, 104 (1962).

36. *See* 26 U.S.C. §§ 6651–6658.

37. *See, e.g.*, 26 U.S.C. § 6651 (providing the penalty for failure to pay tax on or before the date prescribed for payment of such tax).

38. *See, e.g.*, 26 U.S.C. § 6654 (providing that the penalty for underpayment of estimated tax mirrors the interest charge); *see also* I.R.S. News Release, IR-2019-03 (Jan. 16, 2019), https://www.irs.gov/newsroom/irs-waives-penalty-for-many-whose-tax-withholding-and-estimated-tax-payments-fell-short-in-2018 (describing IRS waiver of estimated tax penalties for 2018 year).

39. *See, e.g.*, 26 U.S.C. § 6663 (civil penalty for underpayment of tax).

guilty of willful evasion may face criminal penalties and even jail time.[40] Thus, through a series of calibrated formal provisions (including differing burdens of proof, statutes of limitations, broad standards, and defenses),[41] tax law acknowledges (even if imperfectly) variations in noncompliance. But on top of these formal provisions is the reality that the IRS likely lacks the resources to enforce perfectly and may have to allocate resources to some priorities but not others, giving rise to areas of slack in the system.[42]

Another tax example comes from the innocent spouse rules. Despite the general rule that spouses are jointly and severally liable for taxes, penalties, and interest on a joint tax return, tax law provides relief for an innocent spouse in situations formally specified by statute.[43] These include situations where the fraud or error was due to the other spouse and the relief-seeking spouse had no knowledge, cases involving divorce, and other equitable reasons.[44] Running parallel to these formal statutory spousal relief provisions, however, is the reality that there will be cases in which the IRS either has difficulty detecting fraud or error, or perhaps even notices the noncompliance but deems it minor enough to ignore.[45] In these cases, taxpayers may, in effect, enjoy some informal latitude.

More broadly, slack is a feature of virtually all noncriminal regulatory regimes where enforcement is not 100%, such as local regulations and ordinances, occupational licensing, securities law, and banking law.[46] As Part I.B shows, slack hinges on a combination of information, resources, and discretion; because information is imperfect, resources are scarce, and discretion is pervasive, slack exists.

This Article focuses on slack in the context of civil, criminal, or regulatory transgressions, but slack also exists at a more "micro" level, allowing very small actions that might not themselves rise to the level of legal violations but that

40. *See, e.g.*, *id.* §§ 7201–7207 (criminal tax penalties).

41. *See id.*

42. *See, e.g.*, I.R.S., *Enforcement: Examinations*, *in* 2017 INTERNAL REVENUE SERVICE DATA BOOK 21 (2017), https://www.irs.gov/pub/irs-soi/17databk.pdf (showing IRS audit data and indicating a 0.5% 2017 audit rate).

43. *See* 26 U.S.C. §§ 6013(d)(3), 6015(b), (c), (f).

44. *See id.*

45. NAT'L TAXPAYER ADVOC., *Researching the Causes of Noncompliance: An Overview of Upcoming Studies*, *in* 2010 ANNUAL REPORT TO CONGRESS, 71, 81–85 (2010), https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2020/11/arc10_vol2_causes_of_noncompliance.pdf.

46. *See* Price, *supra* note 17, at 1138. Private law analogues exist, though there, the inquiry concerns negotiations between private parties and decisions by judges. For example, plaintiffs must prove duty, breach, causation, and damages to prevail on tort negligence claims. *See, e.g.*, Hayes v. D.C.I. Properties-D KY, LLC, 563 S.W.3d 619, 622 (Ky. 2018). In making these determinations, information plays a vital role. Breach and causation may be difficult to prove and may require costly and time-consuming discovery. Thus, not every tort results in a lawsuit, partly due to information and proof problems. *See e.g.*, Phillips v. PTS of Am., LLC, No. 3:17-CV-603-CHB, 2021 WL 1220997, at *27 (W.D. Ky. Mar. 31, 2021) (granting summary judgment on all claims against defendants because plaintiffs failed to prove causation). Scenarios in which one might commit a tort but not be held accountable may be described as slack.

may, if taken into account, hold economic and legal consequences. For example, various regulatory benefits (e.g., TSA PreCheck) are granted by applying metrics that may take some factors into account, such as a criminal record, but not others, such as less observable but potentially concerning behaviors.[47] Failure to examine certain behaviors in regulatory decision-making constitutes a kind of "micro-level" slack where potentially problematic indicators may pass unnoticed or may not be given weight. As another example, private and government lending decisions rely on credit scores, income, assets, and tax return data in making credit determinations.[48] Factors such as the borrower's level of alcohol consumption, level of attention to detail, and social media behaviors have traditionally not been examined, even though such factors could plausibly be correlated with creditworthiness.[49] As discussed further below, the operation of such micro-level slack is also changing in the data age.[50]

We have thus far sought to distinguish formal equitable features from informal slack, but it is sometimes unclear whether a feature is formal or informal. For example, widely recognized prosecutorial authority to not pursue a case, to charge more lightly, or to drop charges stems from the reality that prosecutorial decisions are not reviewable.[51] Such discretion could be considered a formal relief feature in that the law recognizes and allows it.[52] But it might also be better described as slack, because there is an element of luck or discretion not specified formally. Perhaps it is a mixed case. The existence of mixed cases does not undercut our broader point, which is that in many contexts, slack exists alongside formal leniency. Because of this paired existence, the assessment of the desirability of the former necessarily depends on the design and existence of the latter.

B. A Taxonomy of Slack

We now offer a taxonomy of the various drivers of slack and contexts in which it arises. This discussion shows that slack is not just about resource and information constraints but may be a function of other factors. Moreover, there may be mixed cases in which slack exists for more than one reason. It is

47. *Disqualifying Offenses and Other Factors*, TRANSP. SEC. ADMIN., https://www.tsa.gov/disqualifying-offenses-factors (last visited Aug. 23, 2021).

48. U.S. DEP'T OF AGRIC., USDA RURAL DEVELOPMENT HANDBOOK 4-1 to 4-70 (2019), https://www.rd.usda.gov/files/3550-1chapter04.pdf.

49. *See* Mandukhai Ganbat et al., *Effect of Psychological Factors on Credit Risk: A Case Study of the Microlending Service in Mongolia*, 11 BEHAV. SCI. 1, 6 (2021); Yanhao Wei et al., *Credit Scoring with Social Network Data*, 35 MKTG. SCI. 234, 234 (2015).

50. *See* discussion *infra* notes 165–167 and accompanying text (describing micro-lender Lenddo's algorithm).

51. *See, e.g.*, Rebecca Krauss, *The Theory of Prosecutorial Discretion in Federal Law: Origins and Development*, 6 SETON HALL CIR. REV. 1, 2 (2012).

52. *Id.* at 4.

important to note upfront that this taxonomy is not offered as a normative justification for slack but simply as a description of how it comes about. We do not claim that any of slack's underlying drivers are themselves fair, defensible, or optimal. In fact, it is likely that the allocation of slack throughout the system will reflect factors such as bias, politics, and privilege, and is unlikely to be distributively just.[53] While (as Part I.C argues) there are normative justifications for safeguarding slack, this normative case must be made independently.

1. Prioritization of Scarce Enforcement Resources

A key context in which slack arises is when enforcers have scarce resources, requiring prioritization.[54] Prioritization determinations can range from decisions by a local police force to allocate patrols to certain neighborhoods, which may lead to crimes in other neighborhoods not being observed, to high-level decisions by federal agencies to prioritize enforcement against certain crimes or in certain geographical areas. The IRS, for example, which has experienced highly public budget woes in recent years, regularly announces enforcement "campaigns," reflecting its focus on certain issues.[55] Immigration enforcement priorities can also shift considerably with a new presidential administration. Days after taking office, President Trump issued several executive orders[56] outlining new immigration enforcement plans, which included construction of a wall along the U.S.–Mexico border, additional border patrol agents, and expedited removals, all of which marked a sharp departure from Obama administration priorities.[57] Four years later, newly elected President Biden issued a proclamation hours after his inauguration announcing (among other immigration enforcement changes) that "no more American taxpayer dollars be diverted to construct a border wall."[58] These resource-

53. *See* Angela J. Davis, *Prosecution and Race: The Power and Privilege of Discretion*, 67 FORDHAM L. REV. 1, 3 (1998).

54. *See, e.g.*, William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 543 (2001); Leigh Osofsky, *The Case for Categorical Nonenforcement*, 69 TAX L. REV. 73, 74 (2015).

55. For example, in 2019, the IRS Large Business and International Division rolled out a total of ten new "campaigns." *See Large Business and International Compliance Campaigns*, I.R.S., https://www.irs.gov/businesses/large-business-and-international-compliance-campaigns (last updated June 10, 2021).

56. *See, e.g.*, Border Security and Immigration Enforcement Improvements, Exec. Order No. 13,767, 82 Fed. Reg. 8793 (Jan. 25, 2017), https://www.federalregister.gov/documents/2017/01/30/2017-02095/border-security-and-immigration-enforcement-improvements; Enhancing Public Safety in the Interior of the United States, Exec. Order No. 13,768, 82 Fed. Reg. 8799 (Jan. 25, 2017), https://www.federalregister.gov/documents/2017/01/30/2017-02102/enhancing-public-safety-in-the-interior-of-the-united-states.

57. *See, e.g.*, Julie Hirschfeld Davis, *Trump Orders Mexican Border Wall to be Built and Plans to Block Syrian Refugees*, N.Y. TIMES (Jan. 25, 2017), https://www.nytimes.com/2017/01/25/us/politics/refugees-immigrants-wall-trump.html.

58. Proclamation No. 10142, 86 Fed. Reg. 7225 (Jan. 27, 2021).

prioritization decisions have obvious impacts on whether the law gets enforced in the case of certain behaviors or against certain populations.

Resource prioritization and imperfect enforcement are not necessarily indefensible. In fact, some theoretical analyses deem less than 100% enforcement as welfare maximizing,[59] or suggest that high penalties with low detection probabilities may be optimal because actual action is costly but threats are free.[60] Such analysis by implication endorses a degree of imperfect enforcement. But the flip side of nonenforcement is that some unlawful behaviors are not sanctioned. This presents tradeoffs, for example, in the form of reduced morale, unfairness, expressive harms, and other impacts.[61] Further, it may be difficult in practice to specify optimal penalty and enforcement levels in advance, particularly as situations change and strategies must adjust.[62] Moreover, there is an obvious danger that selective nonenforcement of entire categories of offenses may be driven by politics or bias.[63]

2. Lack of Information

Information barriers are technically a species of resource limitation,[64] but because data and information are central to our Article, we discuss this point separately.

Information is clearly essential to enforcement, and its absence makes full enforcement difficult. Information gaps are therefore one of the most important factors contributing to slack.[65] For example, IRS tax data show that failure to declare individual business or self-employment income is a significant contributor to the gross tax gap (i.e., the difference between taxes owed and those actually paid on time).[66] This type of income is often not subject to reporting or withholding by third parties (e.g., employers, banks), and because the IRS does not receive corroborating information about its existence, taxpayers frequently underreport it.[67] Lack of information can be overcome by allocating more resources. The IRS could increase audits or could impose additional reporting obligations on third-party payors. But these options are costly to the government and to private actors.

---

59. *See* Becker, *supra* note 7. Economic approaches may treat crime (theft) as a utility transfer with a cost.

60. *See generally* Subhasish M. Chowdhury & Frederick Wandschneider, *Antitrust and the 'Beckerian Proposition': The Effects of Investigation and Fines on Cartels* 1, 4 (U. E. Anglia, Working Paper No. 13-9, 2016).

61. *See* Osofsky, *supra* note 54, at 76.

62. *See generally* Max Minzner, *Should Agencies Enforce?*, 99 MINN. L. REV. 2113 (2015).

63. *Cf.* Osofsky, *supra* note 54.

64. *See generally* Minzner, *supra* note 62, at 2131.

65. *Id.*

66. I.R.S., FEDERAL TAX COMPLIANCE RESEARCH: TAX GAP ESTIMATES FOR TAX YEARS 2011–2013 15–16 (2019), https://www.irs.gov/pub/irs-pdf/p1415.pdf.

67. *Cf.* 26 U.S.C. § 6041 (relating to information reporting at source).

In various contexts, law has been specifically designed to overcome information barriers. Returning to tax, the existence of third-party income reporting and tax withholding for some income (for example, wages) does lower information asymmetries between the IRS and taxpayers, and encourages compliance.[68] As another example, the use of nonprosecution and deferred-prosecution agreements in corporate prosecutions paired with respondeat superior liability incentivizes corporations to leverage their superior access to information and insider knowledge to monitor employees and hold them accountable.[69] However, such solutions (which themselves introduce new risks) are not universally in place, and so slack persists.

3. Deliberate Nonenforcement of Imperfect Laws

Slack may also exist where enforcers make deliberate nonenforcement decisions driven by the law's imperfections rather than by resource constraints. Such decisions stem from judgments that the law on the books is flawed or questionable, or that enforcement is inadvisable or problematic.

Flawed laws may come in different flavors:

Out-of-Step Laws. Some laws may be outdated or out of step with contemporary expectations. In South Carolina, for example, long-standing laws against minors playing a pinball machine[70] and operation of a public dance hall on Sundays[71] remain on the books despite a 2016 legislative effort to amend them.[72] Other laws may be just strange.[73] Yet others may reflect values that have become increasingly contested.

---

68. *Id.* § 3402.

69. *See, e.g.*, Jennifer Arlen & Samuel W. Buell, *The Law of Corporate Investigations and the Global Expansion of Corporate Criminal Enforcement*, 93 S. CAL. L. REV. 697, 706 (2020); Rachel Brewster & Samuel W. Buell, *The Market for Global Anticorruption Enforcement*, 80 L. & CONTEMP. PROBS. 193, 210 (2017); Brandon L. Garrett, *Globalized Corporate Prosecutions*, 97 VA. L. REV. 1775, 1778 (2011).

70. S.C. CODE ANN. § 63-19-2430 (2008) ("It is unlawful for a minor under the age of eighteen to play a pinball machine.").

71. S.C. CODE ANN. § 52-13-10 (1962).

72. S.C. H4535, LEGISCAN, https://legiscan.com/SC/bill/H4535/2015 (last updated Mar. 10, 2016) (showing the bill died in Senate Judiciary Committee).

73. *See, e.g.*, LITTLE ROCK, ARK., CODE OF ORDINANCES ch. 18, tit. II, § 18-54 (1988) ("No person shall sound the horn on a vehicle at any place where cold drinks or sandwiches are served after 9:00pm (Code 1961, § 25-74)"); OHIO REV. CODE ANN. § 2331.12 (West 1953) ("No person shall be arrested during a sitting of the senate or house of representatives, within the hall where such session is being held, or in any court of justice, during the sitting of such court, or on Sunday, or on the fourth day of July."); SKAMANIA COUNTY, WASH., ORDINANCE 1984-2 (1984) ("The slaying of Sasquatch which is deemed a misdemeanor shall be punishable by a $500.00 fine and up to 6 months in the county jail, or both."); KY. REV. STAT. ANN. § 436.600 (West 1972) ("No person shall sell, exchange, offer to sell or exchange, display, or possess living baby chicks, ducklings, or other fowl or rabbits which have been dyed or colored; nor dye or color any baby chicks, ducklings, or other fowl or rabbits; nor sell, exchange, offer to sell or exchange or to give away baby chicks, ducklings, or other fowl or rabbits, under two (2) months of age in any quantity less than six (6), except that any rabbit weighing three (3) pounds or more may be sold at an age of six (6) weeks. Any person who violates this section shall be fined not less than $100 nor more than $500.").

Society may be reluctant to enforce laws that have become controversial. For example, a Louisiana judge recently had to halt jury selection after running out of jurors in a case involving felony marijuana charges.[74] There, prospective jurors had voiced objections to marijuana criminalization, which prompted their dismissal.[75] Still, such cultural shifts that lead a community to regard certain laws as out of step and to enforce them no longer are likely to occur unevenly, so we cannot assume that such laws will never be enforced. For example, different societies—or even different geographic locations within a society—may approach differently enforcement of laws criminalizing adultery and sodomy.[76]

Too Much Law. Relatedly, slack may develop if law is perceived as too onerous or pervasive, such that demanding total compliance is viewed as excessive or impossible.[77] Some have noted how criminal laws tend to be overbroad and overinclusive, partly due to legislator incentives to enact draconian laws as a "tough against crime" signal and to leave hard enforcement choices to judges, prosecutors, and others on the ground.[78] Political process dynamics may cause norms to develop in which enforcers understand that not all criminal behavior can or should be sanctioned.[79] As discussed below, stringent laws make full compliance more difficult and noncompliance more likely, which may in turn suggest that discretion or mercy are necessary.[80] But discretion and mercy also raise rule-of-law issues and may incentivize legislatures to leave bad laws on the books.[81]

Poorly Calibrated Laws. Deliberate nonenforcement may also occur where penalties are perceived to be too severe in relation to the crime. There is some evidence that jurors may be less likely to convict as penalties become more severe.[82] This is plausibly true of other enforcers as well, including police and

74. Matt Sledge, *A New Orleans man faced a felony marijuana charge; too many potential jurors wouldn't consider it*, NOLA.COM (Oct. 9, 2019), https://www.nola.com/news/courts/article_b01d0794-eade-11e9-8114-0f789d4d4ccc.html. Ultimately, defendant pled to a misdemeanor charge instead. *Id.*

75. *Id.*

76. *See supra* sources cited in notes 14 and 15.

77. *See, e.g.*, Bayless Manning, *Hyperlexis: Our National Disease*, 71 NW. U. L. REV. 767 (1977); *cf.* Mila Sohoni, *The Idea of "Too Much Law*," 80 FORDHAM L. REV. 1585 (2012).

78. Stuntz, *supra* note 54 (noting American criminal law "covers far more conduct than any jurisdiction could possibly punish" and "the story of American criminal law is a story of tacit cooperation between prosecutors and legislators, each of whom benefits from more and broader crimes, and growing marginalization of judges, who alone are likely to opt for narrower liability rules rather than broader ones"); Robert J. Delahunty & John C. Yoo, *Dream on: The Obama Administration's Nonenforcement of Immigration Laws, the DREAM Act, and the Take Care Clause*, 91 TEX. L. REV. 781, 856–57 (2013) (noting that strict laws, combined with a large offender population and constrained enforcement resources, means executive discretion is inevitable).

79. *See* Stuntz, *supra* note 54, at 533–39.

80. *Id.* at 594–96.

81. *See* discussion *infra* accompanying note 98; *see also* Price, *supra* note 17; *cf.* Stephanos Bibas, *The Need for Prosecutorial Discretion*, 19 TEMP. POL. & CIV. RTS. L. REV. 369 (2010).

82. *See, e.g.*, Norbert L. Kerr, *Severity of Prescribed Penalty and Mock Jurors' Verdicts*, 36 J. PERSONALITY & SOC. PSYCH. 1431 (1978); James Andreoni, *Reasonable Doubt and the Optimal Magnitude of Fines: Should the Penalty*

regulators, who may choose nonenforcement as a "rough justice" solution to excessively high penalties.[83]

Unjust Laws. Slack may also arise where enforcers perceive the underlying law to be unjust and choose not to enforce it. The category of unjust laws overlaps with poorly calibrated or out-of-step laws, but we define it to include laws that are more fundamentally unfair. Particularly egregious historical examples of unjust laws commonly highlighted in the legal and philosophical literature include legal regimes in Nazi Germany and laws regarding slavery and aiding of fugitive slaves.[84] A contemporary example of an unjust law is the U.S. federal government's "zero tolerance" border-control policy announced in May 2018 and its impact on children.[85] Under that new enforcement policy, all adults crossing the border without inspection were prosecuted regardless of asylum requests or accompanying minors.[86] The policy, adopted under Trump and rescinded by the Biden administration,[87] resulted in the separation of approximately 3,000 children from their families.[88]

The problem of unjust or immoral laws has spawned a vast theoretical literature regarding whether such laws are legitimate and whether citizens have a duty to obey them.[89] Here, legal positivists (dominant in the American legal tradition) tend to view law as separate from morality, viewing even bad laws as legitimate if enacted through legitimate government authority.[90] This stands in contrast to some natural law approaches, which view immoral or evil laws as lacking the authority of law.[91] Some legal positivists may leave room for disobedience in cases of particularly unjust laws,[92] in contrast to firm adherents

---

Fit the Crime?, 22 RAND J. ECON. 385 (1991); Neil Vidmar, *Effects of Decision Alternatives on the Verdicts and Social Perceptions of Simulated Juror*s, 22(2) J. PERSONALITY & SOC. PSYCH 211 (1972); *cf.* Martin F. Kaplan & Sharon Krupa, *Severe Penalties Under the Control of Others Can Reduce Guilt Verdicts*, 10 LAW & PSYCH. REV. 1 (1986).

83. *See* Stuntz, *supra* note 54.

84. *See, e.g.,* ROBERT M. COVER, JUSTICE ACCUSED: ANTISLAVERY AND THE JUDICIAL PROCESS (rev. ed. 1984).

85. *See* WILLIAM A. KANDEL, CONG. RSCH. SERV., R45266, THE TRUMP ADMINISTRATION'S "ZERO TOLERANCE" IMMIGRATION ENFORCEMENT POLICY (2021).

86. *Id.*

87. OFF. OF THE ATT'Y GEN. OF THE U.S., MEMORANDUM FOR ALL PROSECUTORS: RESCINDING THE ZERO-TOLERANCE POLICY FOR OFFENSES UNDER 8 U.S.C. § 1325(A) (Jan. 26, 2021).

88. KANDEL, *supra* note 85.

89. *See, e.g.,* J.C. Oleson, *The Antigone Dilemma: When the Paths of Law and Morality Diverge*, 29 CARDOZO L. REV. 669 (2007).

90. *See, e.g.*, Edward A. Purcell, Jr., *Democracy, The Constitution, and Legal Positivism in America: Lessons from a Winding and Troubled History*, 66 FLA. L. REV. 1457 (2015) (exploring the rise of legal positivism in the United States and the influence of John Austin and Jeremy Bentham in the 1800s); *see also* H.L.A. HART, THE CONCEPT OF LAW (3d ed. 2012).

91. *See, e.g.*, Kent Greenawalt, *The Natural Duty to Obey the Law*, 84 MICH. L. REV. 1 (discussing five theories about natural duty to obey the law and exploring their application to unjust laws).

92. For example, those characterized as "inclusive legal positivists" do not insist on complete separation between the validity of a law and its moral merits as a rule. *See, e.g.*, Richard Dagger & David Lefkowitz, *Politcal Obligation*, STAN. ENCYC. OF PHIL. (last revised Mar. 15, 2021) (reviewing shifting positions in legal positivism), https://plato.stanford.edu/entries/political-obligation/.

of the doctrine of political obligation.[93] Yet most thinkers hold a qualified view of political obligation, conceding that political obligation's reach does not extend to some laws.[94] Philosophical debates about obligation to obey unjust laws have clear implications for the evaluation of slack. If there is no duty to obey unjust laws despite political obligation, then specific areas of slack become important and justifiable, not just because of human foibles but because of law's imperfections. Or put more bluntly, a loss of slack—due, for example, to increased data—that increases enforcement of unjust laws would be regarded as problematic.

4. Exercise of Mercy

A related reason why slack may develop is if enforcers deploy ad hoc discretion to exercise mercy and to forbear from punishment. Debates over mercy are pervasive in criminal law and moral philosophy,[95] with scholars contesting how mercy squares with the retributivist goals of criminal law.[96] Some argue that there is no role for mercy in criminal law, though equitable discretion—attenuating punishment according to the severity of the crime or to mitigating circumstances—may be appropriate and even necessary,[97] particularly given the tendency of criminal law to be overbroad.[98]

---

93. *See, e.g.*, *id.* (outlining differences between exclusive legal positivism—the more classic version (Bentham, Austin, and Hart)—and the later inclusive legal positivism); MICHAEL HUEMER, THE PROBLEM OF POLITICAL AUTHORITY: AN EXAMINATION OF THE RIGHT TO COERCE AND THE DUTY TO OBEY (2012); JOHN RAWLS, A THEORY OF JUSTICE (Harvard Univ. Press, rev. ed. 1999).

94. *See generally* Michael Huemer, *The Duty to Disregard the Law*, 12 CRIM. L. & PHIL. 1 (2018) (sketching scholarly perspectives embracing a qualified view of political obligation doctrine in evaluating jury nullification) (citing THOMAS CHRISTIANO, THE CONSTITUTION OF EQUALITY: DEMOCRATIC AUTHORITY AND ITS LIMITS (2008); Dan Markel, *Retributive Justice and the Demands of Democratic Citizenship*, 1 VA. J. CRIM. L. 1 (2012)). Of course, more behavioral and consequentialist approaches note that the relationship between the justness of laws and the propensity of the governed to obey them may be endogenous. *See generally* Janice Nadler, *Flouting the Law*, 83 TEX. L. REV. 1399 (2005).

95. *See, e.g.*, JEFFRIE G. MURPHY & JEAN HAMPTON, FORGIVENESS AND MERCY (1988); FORGIVENESS, MERCY, AND CLEMENCY (Austin Sarat & Nasser Hussain eds., 2007) (collection of essays on the subject); Dan Markel, *Against Mercy*, 88 MINN. L. REV. 1421 (2004); Rachel E. Barkow, *The Ascent of the Administrative State and the Demise of Mercy*, 121 HARV. L. REV. 1332 (2019) (arguing that ascent of the administrative state and its attendant conceptions of law furthered skepticism of executive clemency and jury nullification).

96. *See generally* MICHAEL S. MOORE, PLACING BLAME: A GENERAL THEORY OF THE CRIMINAL LAW (Oxford Univ. Press 1997) (defending retributivism); Douglas N. Husak, *Retribution in Criminal Theory*, 37 SAN DIEGO L. REV. 959 (2000) (critiquing Moore and offering a more "tempered" defense of retributivism).

97. *See, e.g.*, MURPHY & HAMPTON, *supra* note 95, at 172; Markel, *supra* note 95, at 1431–32, 1435–37. *See generally* Carol S. Steiker, *Tempering or Tampering? Mercy and the Administration of Criminal Justice*, *in* FORGIVENESS, MERCY, AND CLEMENCY 16, 26 (Austin Sarat & Nasser Hussain eds., 2007) (referring to those that argue from feelings of retributive anger as "mercy skeptics"); Markel, *supra* note 95, at 1435–43 (distinguishing equitable discretion from mercy by defining mercy as "remission of deserved punishment" that is suspect because it awards lesser punishment for reasons of "compassion, bias, corruption, or caprice" and equitable discretion as "leniency that is motivated by other reasons that are more properly viewed as triggering equitable or justice-enhancing discretion").

98. *See supra* note 78 and accompanying text.

The analytical distinction between mercy and equitable discretion reflects a tension in criminal law: Discretion and forbearance are necessary, but discretion can lead to bias and uneven enforcement.[99] Carol Steiker has described the "paradox of mercy" as follows: Mercy in criminal justice "is extremely attractive as a way of mitigating the draconian harshness of our current penological regime"[100] but at the same time "it is likely that the institutional opportunities for the exercise of mercy in the criminal justice system are also sources of . . . [much] of the system's disparate impact along the lines of race, ethnicity, and class."[101] The issue for mercy-skeptical scholars is that while some discretion and flexibility are necessary to do justice, unprincipled mercy and compassion based on warm feelings can be fed by conscious and unconscious biases and may lead to disparities.[102] These risks may be greater if some groups are more adept at expressing remorse or asking for lighter punishment because, for example, they possess more cultural capital.[103] The problem is compounded by the fact that it can be difficult in practice to distinguish between appropriate exercise of discretion and unprincipled grants of mercy.

5. Executive Politics

Another important context in which slack arises is in Executive Branch nonenforcement.[104] Presidential executive orders are sometimes issued not to enforce certain laws. Examples include marijuana prohibitions and immigration laws—as was the case with President Obama's Deferred Action for Childhood Arrivals (DACA) program and Deferred Action for Parents of Americans and Lawful Permanent Residents (DAPA) initiatives.[105] As scholars have noted, the Reagan and the two Bush administrations also engaged in so-called

99. Steiker, *supra* note 97, at 19.

100. *Id.*

101. *Id.*

102. *See*, *e.g.*, Susan A. Bandes, *Remorse and Demeanour in the Courtroom: Cognitive Science and the Evaluation of Contrition*, *in* THE INTEGRITY OF THE CRIMINAL PROCESS: FROM THEORY TO PRACTICE 309 (Jill Hunter et al. eds., 2016).

103. *See, e.g.*, M. Eve Hanan, *Remorse Bias*, 83 MO. L. REV. 301 (2018); Bandes, *supra* note 102; Stephen Porter & Leanne ten Brinke, *Dangerous Decisions: A Theoretical Framework for Understanding How Judges Assess Credibility in the Courtroom*, 14 LEGAL & CRIMINOLOGICAL PSYCH. 119 (2009) (examining problems with determinations of trustworthiness based on defendant criminal expressions); Jeremy A. Blumenthal, *A Wipe of the Hands, A Lick of the Lips: The Validity of Demeanor Evidence in Assessing Witness Credibility*, 72 NEB. L. REV. 1157 (1993).

104. See Peter L. Strauss, *The President and Choices Not to Enforce*, 63 LAW & CONTEMP. PROBS. 107 (2000) for an earlier treatment. *See also* Kate Andrias, *The President's Enforcement Power*, 88 N.Y.U. L. REV. 1031 (2013); Mary M. Cheh, *When Congress Commands a Thing to be Done: An Essay on* Marbury v. Madison*, Executive Inaction, and the Duty of the Courts to Enforce the Law*, 72 GEO. WASH. L. REV. 253 (2003).

105. *See*, *e.g.*, Jeffrey A. Love & Arpit K. Garg, *Presidential Inaction and the Separation of Powers*, 112 MICH. L. REV. 1195 (2014); Zachary S. Price, *Enforcement Discretion and Executive Duty*, 67 VAND. L. REV. 671 (2014); Delahunty & Yoo, *supra* note 78; Michael Sant'Ambrogio, *The Extra-Legislative Veto*, 102 GEO. L.J. 351 (2014).

"deregulation through nonenforcement."[106] We treat executive nonenforcement decisions as slack because, even though they do not happen off the books, it is difficult to predict upfront when such orders will be given. Thus, in terms of impact and popular understanding, executive nonenforcement functions more like informal latitude.

A substantial literature addresses the extent to which the president may legitimately order blanket nonenforcement of laws and the risks such executive nonenforcement presents.[107] Scholars have questioned whether deliberate nonenforcement violates separation of powers principles, whether it contravenes the "Take Care" Clause, whether it causes bad laws to remain on the books,[108] and whether it undermines the rule of law.[109] Scholars have also attempted to articulate the boundaries of permissible presidential nonenforcement.[110] Most, but not all, have argued that while nonenforcement based on resource constraints is permissible and unavoidable, nonenforcement based on blanket substantive policy preferences is not.[111] It is unclear, however, whether these lines can be effectively administered in practice, nor is it easy to determine whether lines drawn are well placed from a welfarist perspective.

Scholars also have debated administrative agency nonenforcement.[112] Because agencies are part of the Executive Branch, agency nonenforcement also implicates separation of powers, fairness, and procedural concerns.[113] With a few exceptions, agency nonenforcement decisions generally are not

---

106. *See* Daniel T. Deacon, Note, *Deregulation Through Nonenforcemen*t, 85 N.Y.U. L. REV. 795 (2010); Price, *supra* note 17 (discussing nonenforcement under Republican and Democrat administrations).

107. *See* sources cited *supra* notes 104–106.

108. Price, *supra* note 17, at 1146 (noting that "[w]hile prosecutorial discretion provides a crucial safety valve against rigorous enforcement of outdated or unrealistic laws, persistent nonenforcement also permits laws to remain in place that would be politically intolerable if fully enforced").

109. Price, *supra* note 17; David S. Rubenstein, *Taking Care of the Rule of Law*, 86 GEO. WASH. L. REV. 101 (2018).

110. Andrias, *supra* note 104 (calling for more agency coordination, disclosure, and transparency).

111. *See*, *e.g.*, Price, *supra* note 105, at 675 (noting that presidential nonenforcement authorities do not extend to "prospective licensing of prohibited conduct" or to "policy-based nonenforcement of federal laws for entire categories of offenders"); Delahunty & Yoo, *supra* note 78, at 856 ("Presidential prerogative does not justify a refusal to enforce the immigration laws in ordinary, non-critical circumstances.") (setting forth defenses to presidential breach of duty including (1) law's unconstitutionality, (2) interference with another presidential constitutional power, (3) equity, and (4) resource constraints); *see also* Osofsky, *supra* note 54, at 78 ("[S]cholars have reached a near consensus that policy-based nonenforcement is impermissible, whereas nonenforcement resulting from enforcement resource limitations may be permissible."); *cf.* Peter L. Markowitz, *Prosecutorial Discretion Power at Its Zenith: The Power to Protect Liberty*, 97 B.U. L. REV. 489 (2017) (arguing that presidential nonenforcement power reaches its "zenith" when physical liberty and its deprivation are at stake).

112. *See* Osofsky, *supra* note 54; Aaron L. Nielson, *How Agencies Choose Whether to Enforce the Law: A Preliminary Investigation*, 93 NOTRE DAME L. REV. 1517 (2018) [hereinafter Nielson, *Agencies*]; AARON L. NIELSON, WAIVERS, EXEMPTIONS, AND PROSECUTORIAL DISCRETION: AN EXAMINATION OF AGENCY NONENFORCEMENT PRACTICES (2017) [hereinafter NIELSON, WAIVERS].

113. *See* Nielson, *Agencies*, *supra* note 112, at 1520 (noting that "nonenforcement implicates basic notions of fairness and administrative regularity," raising concerns about abuse, and noting that "'government by waiver,' if taken too far, is antithetical to liberty").

reviewable by courts.[114] While some scholars have argued that there are merits to allowing agencies to categorically underenforce the law,[115] others have identified risks. These include the risk of regulatory capture,[116] the risk of undesirable dynamics between state and private actors,[117] and the risk that underenforcement discretion may be fed by—and may in turn feed—the passage of overly broad or aggressive laws.[118] Yet, it is also clear from administrative law scholarship that nonenforcement is inevitable in agency practice due to resource constraints and the need to prioritize.[119]

The foregoing discussion has shown that slack arises in different and potentially overlapping contexts, including resource and informational constraints, deliberate underenforcement of problematic laws of various kinds, decisions to exercise mercy, and executive branch politics. Existing strands of scholarly literature have touched on these phenomena from different angles. Part I tied these threads together conceptually.

Our discussion suggests that slack holds both positives and negatives, depending on the underlying contexts in which it arises. On the positive side, when paired with law's formal equitable features, slack permits flexibility to accommodate human failures and imperfect laws, particularly in light of resource constraints. But the flip side is that slack also holds risks of bias and politically driven decisions, and may raise rule of law and separation of powers concerns. Throughout the above examination of slack's sources, it is obvious that racial, ethnic, socioeconomic, gender, and other biases are likely to play an important role in determining how and where slack appears in the system.[120] Thus, for example, mercy may be disproportionately bestowed upon privileged groups, executive-branch enforcement and nonenforcement decisions may disproportionately ensnare more vulnerable populations, and resource-prioritization decisions may result in intentional or unintentional targeting.

---

114. Heckler v. Chaney, 470 U.S. 821 (1985); *see also* Cass R. Sunstein, *Reviewing Agency Inaction After* Heckler v. Chaney, 52 U. CHI. L. REV. 653 (1985); Jentry Lanza, Note, *Agency Underenforcement as Reviewable Abdication*, 112 NW. U. L. REV. 1171 (2018).

115. *See* Osofsky, *supra* note 54.

116. Minzner, *supra* note 62, at 2116 (challenging superiority of specialized agency enforcement and noting that "regulatory capture can produce underenforcement").

117. *See* Richard A. Epstein, *Government By Waiver*, NAT'L AFFS., Spring 2011, at 39.

118. *Id.* (identifying the Patient Protection and Affordable Care Act and the Wall Street Reform and Consumer Protection Act as two complex statutes that will implicate and exacerbate nonenforcement and "government by waiver").

119. *See* Osofsky, *supra* note 54, at 82–83; Nielson, *Agencies*, *supra* note 112, at 1532–34; Delahunty & Yoo, *supra* note 78, at 856 (Obama Administration's immigration nonenforcement "is the almost inevitable outcome of . . . a de facto delegation system that Congress has established in the immigration area" and that "the combination of a massive illegal immigrant population, extremely stringent laws regarding deportability, and inadequate resourcing for enforcement gives the President virtually unfettered control to decide who remains in the country and who is removed.").

120. *See* Stuntz, *supra* note 54, at 575.

C. The Bounded Case for Slack

Thus far, this Article has focused on slack in the legal system, showing how it is valuable but holds risks. Part II will turn to the follow-up question of how ubiquitous data affects slack. But first, we need to evaluate whether slack is desirable in the first place. Part I.C articulates a bounded argument in favor of preserving some slack in the legal system, even conceding its risks.

1. A Constraint on Too Much Law

Slack serves as an aggregate constraint on government power. As discussed in Part I.B, there may be a cumulative tendency to enact too many laws such that enforcing them all would be impossible.[121] In criminal law, for example, some have noted that legislators have incentives to enact overbroad criminal laws and then leave it to judges and prosecutors to determine when to forbear or not prosecute.[122] Similar forces are at work in compliance and regulatory systems, although the net accumulation of too much law can arise even where lawmakers are not specifically driven to demonstrate they are "tough on crime."[123]

The existence of too many laws creates problems for both governments and the governed. Even in a relatively stable participatory democracy with laws that are individually plausible, the sheer volume of rules could make consistent compliance difficult, particularly with respect to rules that are not morally intuitive but regulatory in nature.[124] For example, even if a single penalty for failure to file a required business form on time does not seem unduly onerous, if there are hundreds of similar filing requirements, definitions, and exceptions, we might find that modest penalties and compliance burdens, while unproblematic alone, become onerous in totality.

Where over-legislation or over-regulation exists but enforcement is imperfect, it might be argued that we have in effect accepted a system in which a wide range of conduct is eligible for sanction, but in reality, only some percentage of violations (call it x%) is actually sanctioned. Compliance and enforcement may be random with respect to each individual act, but in the aggregate, the average person can reliably expect that there is some slack with respect to (100 - x)% of violations.[125] Taking the argument a step further, if people start getting punished for significantly more than x% of violations such

121. *Id.* at 507; Delahunty & Yoo, *supra* note 78, at 856–57.

122. *See* Stuntz, *supra* note 54, at 529–33; Delahunty & Yoo, *supra* note 78, at 792–95.

123. *See* Stuntz, *supra* note 54, at 509–10.

124. *See* Osofsky, *supra* note 54, at 82.

125. We are not claiming that legal enforcement is distributed evenly across society. Studies across a range of legal regimes reveal enforcement biases. *See, e.g.*, NAT'L TAXPAYER ADVOC. SERV., ANNUAL REPORT TO CONGRESS 79–93 (2014). Our point is that individuals are all likely "caught" for only a fraction of violations (even if that fraction is not uniform across individuals).

that they are bearing impossibly high penalties or compliance burdens, then the system is not working as designed. If so, then the underlying legal regime should be revisited.[126]

2. A Constraint on Government Incursions into the Personal

Total enforcement would require total surveillance, or at least much more aggressive attempts at observation and detection. But, as recognized in the privacy literature, it is risky for the government to possess substantially complete information about everyone. Perhaps most importantly, total information risks an unintended shift in the relationship between government and individuals and ultimately in the individual's sense of self separate from government and government institutions.[127] Literature on the implications of government surveillance, including "total surveillance," details a range of potential harms, such as chilling of personal liberties and intellectual freedom, ensnaring of subjects in increasingly broad surveillance dragnets, and unleashing of abusive behaviors—e.g., blackmail, coercion, and discrimination—triggered by power disparities.[128]

In the abstract, we may find that many (though not everyone) would trade the advantages of full enforcement of the law for continued space between government and individuals.[129] However, that commitment to a world in which the government does not know everything will be tested in cases of shocking, heinous, or high-impact events, such as violent crimes, terrorist attacks, or public health crises, or if and when individuals become victims themselves. In those situations, we might see demands that the government aggressively use data to bring perpetrators to justice, regardless of the incursions that would result, and regardless of philosophical commitments voiced *ex ante*.

---

126. Relatedly, one of us has argued that nonenforcement of tax debts can serve a valuable social insurance function. *See* Shu-Yi Oei, *Who Wins When Uncle Sam Loses? Social Insurance and the Forgiveness of Tax Debts*, 46 U.C. DAVIS L. REV. 421, 462–63 (2012) [hereinafter Oei, *Who Wins*]; Shu-Yi Oei, *Getting More by Asking Less: Justifying and Reforming Tax Law's Offer-in-Compromise Procedure*, 160 U. PA. L. REV. 1071, 1096 (2012) [hereinafter Oei, *Getting More*].

127. *See, e.g.*, Richards, *supra* note 2, at 1956; DAVID LYON, SURVEILLANCE STUDIES 89–92 (2007); SURVEILLANCE AND DEMOCRACY 35 (Kevin D. Haggerty & Minas Samatas, eds., 2010); THE SURVEILLANCE STUDIES READER 35–49 (Sean P. Hier & Josh Greenberg, eds., 2007); *see also* Andrej Zwitter, Oskar J. Gstrein & Evan Yap, *Digital Identity and the Blockchain: Universal Identity Management and the Concept of the 'Self-Sovereign' Individual*, FRONTIERS IN BLOCKCHAIN, 11 (2020); Anuj Puri, *A Theory of Group Privacy*, 30 CORNELL J.L. & PUB. POL'Y (forthcoming 2021) (manuscript at 27–28), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3686202.

128. *See* sources cited *supra* note 127; Brayne, *supra* note 11, at 986–89; *cf.* Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2786 (2021) (discussing how data privacy law harms defendants' rights).

129. Some advocates of the "information wants to be free" view of data might prioritize free movement of data. *See, e.g.*, R. Polk Wagner, *Information Wants to Be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 999 n.14 (2003).

3. A Second Space for Substantive Debate

Scholars have long recognized that the legislative process contains numerous imperfections, pathologies, and misaligned incentives.[130] For example, statutes are often drafted hastily and reviewed by legislative aides rather than elected representatives.[131] In the criminal law context, as noted, legislators have incentives to enact harsh and overinclusive laws that generate messaging benefits, leaving discretionary sentencing to prosecutors and judges.[132] Highly technical legislation (such as tax statutes) may be poorly drafted and require revisions after the fact.[133] Legislators may feel compelled to push legislation through in the absence of sufficient information as to whether the law is really administrable or well-designed or whether the penalties are fair.[134] These pathologies exist even in the case of well-intentioned laws. And laws, once passed, may be difficult to amend or repeal, for example, due to partisan politics.[135]

In light of these pathologies, slack offers an imperfect second space for reevaluating laws that have been enacted and for mitigating problematic effects, serving as a safety valve in the event problematic laws are passed and not repealed, or serving a transition management function even if they are.[136] For example, marijuana laws, notably those directed at individual consumption, contain penalties many consider disproportionate, particularly given rapidly shifting societal views on marijuana use and increasing information regarding discriminatory enforcement.[137] Here, informal latitude in enforcement of possession laws would provide the legal system time to incorporate this information into a revised statutory scheme without leaving some demographic groups to bear the brunt of the problematic regime. If legislative pathologies

130. *See* sources cited *infra* notes 131–135.

131. *See, e.g.*, Abbe R. Gluck & Lisa Schultz Bressman, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part I*, 65 STAN. L. REV. 901, 983 (2013); Lisa Schultz Bressman & Abbe R. Gluck, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part II*, 66 STAN. L. REV. 725, 755–56 (2014); Shu-Yi Oei & Leigh Osofsky, *Legislation and Comment: The Making of the § 199A Regulations*, 69 EMORY L.J. 209, 217 (2019).

132. *See, e.g.*, Stuntz, *supra* note 54, at 529–33.

133. For example, the speed with which the 2017 tax reform was enacted (due in part to political process realities) is widely viewed as contributing to errors and problematic provisions. *See, e.g.*, Oei & Osofsky, *supra* note 131, at 211.

134. *See* Oei & Osofsky, *supra* note 131, at 217–19.

135. *See* Leigh Osofsky, *Agency Legislative Fixes*, 105 IOWA L. REV. 2107, 2122 (2020).

136. Repeated violations of a law may illuminate problems with the law itself and suggest amendment or repeal. Thus, some have advised that "impossibility structures" should be used with caution and that "conscious inefficiencies," which allow individuals space to violate the law, should be preserved. *See* Hartzog, *supra* note 24, at 1791–92 (quoting Michael L. Rich, *Should we Make Crime Impossible?*, 36 HARV. J.L. & PUB. POL'Y, 795, 846–47 (2013)); Rademacher, *supra* note 25, at 1–20.

137. *See, e.g.*, Steven W. Bender, *The Colors of Cannabis: Race and Marijuana*, 50 U. C. DAVIS L. REV. 689, 697 (2016).

were to ultimately stymie repeal, then slack's function would be even more important.

An obvious counterargument is that allowing informal nonenforcement will create even stronger incentives for legislators to pass bad laws and may cause such laws to remain on the books longer since they are infrequently or never enforced and hence not salient. But it is empirically uncertain whether these dynamics really occur. Time constraints and legislative process realities already place significant pressure on legislatures to push imperfect laws through, often without understanding their content.[138] Moreover, legislative fixes for the most part do not happen immediately, if at all.[139] This is particularly so if the law is not one of broad application.[140] For example, rules regarding eligibility for the Earned Income Tax Credit or the U.S. Department of Agriculture's Supplemental Nutritional Assistance Program (SNAP) by their very nature apply to a segment of the population that is not politically powerful.[141] If these laws are flawed, there may be little legislative impetus to fix them. Simply put, if those most capable of making their voices heard are not affected by the law, it is unlikely that effective coalitions for repeal will form.

Finally, because of changing compositions of legislatures and the vote trading that inevitably occurs, enacting legislative corrections may simply be difficult. Technical corrections of flawed tax legislation are notoriously hard to pass.[142] Legislators of party *A* may be unwilling to help party *B* correct legislation that party *A* had resisted in the first place, or may try to extract concessions, leading to gridlock.[143]

Whether this "second space" argument proves powerful enough to justify the existence of slack depends on factors such as what proportion of laws are problematic and whether there are countervailing harms to rule-of-law norms and enforcement. In general, we suggest that slack is probably valuable where it is unfeasible for legislatures to refrain from passing legislation, where laws, once enacted, are difficult to repeal, and where continuing to enforce the law until it is repealed may be harmful or unfair to some groups.

II. THE IMPACT OF DATA ON SLACK

We now examine data and information's impact on slack and how this will transform the relationship among humans, governments, and the law. Part II.A describes the proliferation of increasingly ubiquitous data in society. Part II.B

138. *See* sources cited *supra* note 131.
139. *See* Osofsky, *supra* note 135, at 2128–29.
140. *See id.* at 2122–23.
141. *See* Oei, *Getting More*, *supra* note 126, at 1091 n.81.
142. *See, e.g.*, Oei & Osofsky, *supra* note 131, at 251–52.
143. *Id.*

identifies the potential impacts of data on slack in the legal system and the implications for design of legal rules.

In sum, increased data has made human lapses, noncompliance, and violations more detectable, traceable, memorable, and thus easier to detect and hard to ignore. Accordingly, slack is expected to shrink. But given that increases in such data are not uniform, and that some individuals have greater capacities to manage their data, shrinkage in slack will likely be uneven and disproportionate in impact.

A. Ubiquitous Data

In analytics' parlance, data, information, and insights mean different things. Data refers to raw and discrete facts or statistics.[144] It becomes useful when it can be processed into information that generates usable insights.[145] In this Article, we use the shorthand "data" to refer to data as well as the information and insights it generates.

The lifecycle view of data that permeates the data management literature highlights key phases in data use. These include planning, collection, use, storage, and reuse.[146] This conceptual breakdown helps illuminate the fact that while some ethical and policy considerations run through all phases of the data lifecycle, specific considerations may become particularly relevant at each different phase.

Data is found in many places, including government and private databases, private emails or communications, and public or semi-public online postings.[147] It takes various forms, including photos, video, and text.[148] It is collected when humans engage in mundane activities, including going to the doctor, surfing the internet, and walking down the street. It is gathered via mechanisms ranging from cell phones to hand-filled-out forms.[149] Massive amounts of data on the ideas, finances, and behaviors of humans and entities are increasingly being collected, normalized,[150] analyzed, and used for social, economic, and

144. *See generally* Brent Dykes, *Actionable Insights: The Missing Link Between Data and Business Value*, FORBES (Apr. 26, 2016), https://www.forbes.com/sites/brentdykes/2016/04/26/actionable-insights-the-missing-link-between-data-and-business-value/#2f5a28b951e5.

145. *Id.*

146. *See, e.g.*, Jeannette M. Wing, *The Data Life Cycle*, HARV. DATA SCI. REV. (July 1, 2019), https://doi.org/10.1162/99608f92.e26845b4.

147. Dykes, *supra* note 144.

148. *Id.*

149. *Id.*

150. Normalization means making data into comparable units. *See Introduction to Data Normalization*, AGILE DATA, http://agiledata.org/essays/dataNormalization.html.

commercial purposes.[151] Data has, in the words of one analyst, become the "new oil," a critical raw material for business, commerce, and government.[152]

Owing to the growing hunger for data, human activity is increasingly susceptible to being surveilled, often without the subject's knowledge or consent, and there is significant risk that such data will never be "forgotten."[153] This raises questions about privacy rights in the data age. As an indicator of the issue's importance, the *New York Times* launched a "Privacy Project" in 2019, consisting of a series of articles discussing data and surveillance and evaluating the repercussions for privacy.[154] Privacy debates aside, ubiquitous data also carries critical implications for law's operation and design, as this Article explores.

The claim of data's ubiquity is not a claim that until now, we have operated in a world of little or no data; rather, it is an acknowledgement of the drastically changing scale and scope of data collection and analysis.[155] Recognition of this tectonic shift has prompted analogies to Jeremy Bentham's *Panopticon*[156] in analyzing data-driven dynamics and relationships in society.[157]

---

151. Dykes, *supra* note 144. *See, e.g.*, Zhijun Chen et al., *Data-Driven Mergers and Personalization* (Inst. of Soc. and Econ. Rsch., Osaka Univ., Discussion Paper No. 1108, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725312 (exploring the role of data acquisition in prompting merger transactions).

152. *The World's Most Valuable Resource is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. The original quote is usually attributed to mathematician Clive Humby. *See also* José Parra-Moyano, Karl Schmedders & Alex Pentland, *What Managers Need to Know About Data Exchanges,* 61 MIT SLOAN MGMT. REV. 39 (2020) (exploring data as a factor of production and how its production is changing).

153. Currently there is no systematic path by which data is effectively "forgotten" in the United States. *See generally* Tim Wu, Opinion, *How Capitalism Betrayed Privacy*, N.Y. TIMES (Apr. 10, 2019), https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html. A sweeping literature examines the theoretical underpinning of a right to be forgotten and the tradeoffs. *See, e.g.*, Urs Gasser et al., *Internet Monitor 2014: Reflections on the Digital World: Platforms, Policy, Privacy, and Public Discourse* (Berkman Center Rsch. Publ'n No. 2014-17, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538813; Giancarlo F. Frosio, *The Right to Be Forgotten: Much Ado About Nothing,* 15 COLO. TECH. L.J. 307 (2017)*;* Robert Kirk Walker, *The Right to be Forgotten,* 64 HASTINGS L.J. 257 (2012)*;* Stefan Kulk & Frederik Zuiderveen Borgesius, *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 301 (Jules Polonetsky, Omer Tene & Evan Selinger eds., 2018).

154. *The Privacy Project*, *supra* note 1; Bill Hanvey, Opinion, *Your Car Knows When You Gain Weight*, N.Y. TIMES (May 20, 2019), https://www.nytimes.com/2019/05/20/opinion/car-repair-data-privacy.html; Michael Kwet, Opinion, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. TIMES (June 14, 2019), https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

155. Stuart Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Data, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

156. JEREMY BENTHAM, *Panopticon, in* 4 THE WORKS OF JEREMY BENTHAM 43, 44 (John Bowring ed., Russell & Russell 1962) (1838–43).

157. *See, e.g.*, Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 317–20 (2003) (exploring the Panoptic qualities of cyber peer-to-peer networks); Tjerk Timan, Maša Galič & Bert-Jaap Koops, *Surveillance Theory and Its Implications for Law*, *in* THE OXFORD HANDBOOK OF LAW, REGULATION, AND TECHNOLOGY 731 (Roger Brownsword, Eloise Scotford & Karen Yeung eds., 2017) (offering an overview of surveillance theory and techniques); Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 184 (2008) (noting that "[a]cademic privacy theorists have tended to favor the motif of the Panopticon" in evaluating the relationship between privacy and visibility); OSCAR H. GANDY, JR., THE

Four key features of the contemporary data landscape inform data's impacts on slack:

1. A Wide Range of Topical Categories

Widespread collection, processing, and use of data take place for at least seven different purposes: financial, security, medical, social, commercial, political, and regulatory.[158] We briefly discuss these in turn. Notably, because data is non-rivalrous, multiple actors may derive value from the same data, and data collected and processed for one purpose can be used for another.[159] In fact, how boundaries between uses are managed is an important emerging policy issue.[160] Thus, our delineation of data's different purposes in no way implies ultimate separation of uses.

Data has long been used in making financial forecasting decisions.[161] Such data may be person-specific, such as credit scores, or may consist of broader statistics on markets, investments, and debts.[162] Financial data is processed by humans as well as by algorithms.[163] Data sources that are not obviously financial in nature may increasingly be used for finance purposes.[164] For example, micro-lender Lenddo uses a cutting-edge algorithm that relies on non-traditional data to illuminate "social nuances," including whether the prospective borrower uses one-word subject lines in emails (signaling attention to detail), uses financial

---

PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993) (offering a vision of the surveillance society); Thomas McMullan, *What Does the Panopticon Mean in the Age of Digital Surveillance?*, THE GUARDIAN (July 23, 2015), https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham.

158. *See* Thompson & Warzel, *supra* note 155.

159. Data's non-rivalry has provided the foundation for economic theories regarding ideal property rules for data ownership. Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data*, 110 AM. ECON. REV. 2819, 2822 (2020). For early studies in the field, see, for example, George Joseph Stigler, *The Economics of Information*, 69 J. POL. ECON. 213 (1961); George Joseph Stigler, *Information in the Labor Market*, 70 J. POL. ECON. 94 (1962); Michael Spence, *Job Market Signaling*, 87 Q.J. ECONOMICS 355 (1973).

160. Wu, *supra* note 153 ("[D]ata and surveillance networks created for one purpose can and will be used for others."); Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police* (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (noting the "if you build it, they will come" principle, i.e., "anytime a technology company creates a system that could be used in surveillance, law enforcement inevitably comes knocking"); *see also* Acquisti et al., *supra* note 22 (discussing economic theories of privacy).

161. Thompson & Warzel, *supra* note 155.

162. *Id.*

163. *See, e.g.*, Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era* (Nat'l Bureau of Econ. Rsch., Working Paper No. 25943, 2019), https://www.nber.org/system/files/working_papers/w25943/w25943.pdf (examining discrimination in algorithmic lending); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (exploring growth, use, and risks of scoring).

164. Emily Bary, *How Artificial Intelligence Could Replace Credit Scores and Reshape How We Get Loans*, MARKET WATCH (Oct. 29, 2018), https://www.marketwatch.com/story/ai-based-credit-scores-will-soon-give-one-billion-people-access-to-banking-services-2018-10-09; s*ee also supra* notes 159–160 and accompanying text.

apps on their smartphone (signaling whether they take finances seriously), and has a high ratio of smartphone selfies (signaling youth, and enabling the lender to group prospective borrowers).[165] Such alternative algorithms are often justified on grounds that they open the lending market up to the "unbanked."[166] The use of these types of metrics will likely become increasingly widespread.[167]

Data has also been gathered for security purposes, including for both personal safety (home burglar alarms) and public safety (law enforcement, antiterrorism, national security, border control, and protection of business assets).[168] This data may be gathered through surveillance videos, locational tracking, and biometric information.[169] It may be organized in databases created for one purpose, which may then be used for other, perhaps unanticipated, purposes.[170] For example, the data sources available to U.S. Immigration and Customs Enforcement (ICE) have expanded and now include driver's license photos, phone records, jail bookings, insurance information, utility bills, social media accounts, and tax records.[171]

Data has long been at the heart of medicine. Comprehensive medical records enable healthcare providers to make patient-care decisions. Personal health data plays a critical role in contact tracing and related pandemic-management measures.[172] Large population data sets provide valuable insights

165. Bary, *supra* note 164; *see also* George Popescu, *Lenddo—The Google of Lending Algorithms*, LENDING TIMES (Feb. 29, 2016), https://lending-times.com/2016/02/29/lenddo-the-google-of-lending-algorithms/.

166. *See* Popescu, *supra* note 165.

167. *See* Bary, *supra* note 164; Adair Morse & Karen Pence, *Technological Innovation and Discrimination in Household Finance* 2–3 (Nat'l Bureau of Econ. Rsch., Working Paper No. 26739, 2020), https://www.nber.org/papers/w26739.

168. *See, e.g.*, Glenn S. Gerstell, *I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution*, N.Y. TIMES (Sept. 10, 2019), https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html; *cf.* Richards, *supra* note 2, 1936–38.

169. *See* Richards, *supra* note 2, at 1938–40.

170. *See* Wu, *supra* note 153.

171. McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES MAG. (June 7, 2021), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

172. *See, e.g.*, Karla Grossenbacher, Richard Lutkus & Eric Suits, *Workplace Contact Tracing Apps—Legal Implications and Considerations*, BLOOMBERG LAW (July 2, 2020), https://news.bloomberglaw.com/us-law-week/insight-workplace-contact-tracing-apps-legal-implications-and-considerations; Arshad R. Zargar, *Privacy, Security Concerns as India Forces Virus-Tracing App on Millions*, CBS NEWS (May 27, 2020), https://www.cbsnews.com/news/coronavirus-india-contact-tracing-app-privacy-data-security-concerns-aarogya-setu-forced-on-millions/; Luis Felipe M. Ramos, *Evaluating Privacy During the COVID-19 Public Health Emergency: The Case of Facial Recognition Technologies*, SSRN (Nov. 13, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3729470; David O. Argente, Chang-Tai Hsieh & Munseob Lee, *The Cost of Privacy: Welfare Effects of the Disclosure of COVID-19 Cases*, (Nat'l Bureau of Econ. Rsch., Working Paper No. 27220, 2020), https://www.nber.org/system/files/working_papers/w27220/w27220.pdf; Mark Findlay et al. *Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-Crisis* (Sing. Mgmt. Univ. Ctr. for AI & Data Governance, Rsch. Paper No. 2020/02, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592283.

into promising drug and treatment options.[173] In the data age, individual and population medical data collection and analysis have ramped up exponentially. For example, health monitoring devices (e.g., pedometers and heart-rate monitors) can generate minute-by-minute data on different dimensions of health.[174] Online genetic tests have given rise to vast databases of information.[175] Like financial and security data, health-related data has the potential for unexpected cross-uses such as employee monitoring, insurance, marketing, and law enforcement.[176] In 2018, San Jose police arrested a man for murder based in part on data from the victim's Fitbit, which pinpointed a spike in heart rate followed by slowing and finally termination.[177]

Perhaps the most universally recognized context in which data has become ubiquitous is through online social networking platforms that accumulate and track user data and behavior. Data collected may be used by platforms themselves (e.g., for advertising), sold to others, or provided to governments.[178] Contractual clauses and privacy policies described in user agreements offer limited protection: policies may be unintelligible,[179] may not be salient to users, may not prevent data theft or illegal use,[180] and may not protect users from government requests for social media data (e.g., for national security purposes).[181]

---

173. Wullianallur Raghupathi & Viju Raghupathi, *Big Data Analytics in Healthcare: Promise and Potential*, HEALTH INFO. SCI. & SYS. (Feb. 7, 2014) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4341817/pdf/13755_2013_Article_14.pdf.

174. Min Wu & Jake Luo, *Wearable Technology Application in Healthcare: A Literature Review*, HEALTHCARE INFO. & MGMT. SYS. SOC'Y (Nov 25, 2019), https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review.

175. *See* Julian Segert, *Understanding Ownership and Privacy of Genetic Data*, HARV. UNIV. SCI. IN THE NEWS: BLOG (Nov. 28, 2018), http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data/.

176. *See*, *e.g.*, Sarah Zhang, *A DNA Company Wants You to Help Catch Criminals*, THE ATLANTIC (Mar. 29, 2019), https://www.theatlantic.com/science/archive/2019/03/a-dna-company-wants-your-dna-to-catch-criminals/586120/; Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)*, N.Y. TIMES (Feb. 1, 2018), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

177. Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y. TIMES (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html. Such law enforcement use of a Fitbit is not an isolated instance. *Id.*

178. Kalev Leetaru, *Social Media Companies Collect So Much Data Even They Can't Remember All the Ways They Surveil Us*, FORBES (Oct. 25, 2018), https://www.forbes.com/sites/kalevleetaru/2018/10/25/social-media-companies-collect-so-much-data-even-they-cant-remember-all-the-ways-they-surveil-us/?sh=2344aae07d0b; Kalev Leetaru, *What Does It Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=58b56d952d6c.

179. Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

180. *See, e.g.*, Shu-Yi Oei & Diane Ring, *Leak-Driven Law*, 65 UCLA L. REV. 532, 536–39 (2018); Adam B. Thimmesch, *Tax Privacy?*, 90 TEMP. L. REV. 375, 377–79 (2018).

181. *See, e.g.*, Agency Information Collection Activities: Generic Clearance for the Collection of Social Media Information on Immigration and Foreign Travel Forms, 84 Fed. Reg. 46557 (proposed Sept. 4, 2019)

Data is also used for commercial purposes such as advertising, employee monitoring, business strategy, inventory management, and product development.[182] In some cases, businesses have the data under their control and simply need to convert it into usable information and intelligence. In other cases, businesses must acquire the data, in which case a market for data may develop. Commercial use and acquisition of data may or may not be legal.[183]

Data is central to seizing and maintaining political power. Data about prospective voters can enable politicians, political parties, and others to determine messaging or vote-garnering strategies.[184] Such data may be combined with other information (e.g., academic research findings) about voter behavior to suggest political strategies.[185] The political use of data is not limited to internal actors in a political system. The use of fake Facebook accounts to influence the 2016 U.S. presidential election by parties acting on behalf of the Russian government spotlighted how outside actors use data to influence a country's internal politics.[186] The political relevance of data is not limited to the voting booth: data can be used to determine levels of support for policies and may suggest strategies for engagement with various constituencies or with other countries.[187] More sinisterly, data about political opponents or grassroots opposition may be used to quash such opposition, either directly or through pretextual means.[188]

(collecting social media data for border and immigration admissions); Sandra E. Garcia, *U.S. Requiring Social Media Information from Visa Applicants*, N.Y. TIMES (June 2, 2019), https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html; Karen Zraick & Mihir Zaveri, *Harvard Student Says He Was Barred from U.S. Over His Friends' Social Media Posts*, N.Y. TIMES (Aug. 27, 2019), https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html; Yoko Kubota, *China's Cyber Cop Ups the Pressure to Control Online Speech*, WALL ST. J. (Nov. 15, 2018), https://www.wsj.com/articles/chinas-cyber-cop-ups-the-pressure-to-control-online-speech-1542291470 (requiring online service providers to maintain detailed records of user information); *see also* Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. (forthcoming 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3564480# (arguing protection of privacy rights must be achieved through both property and liability rules).

182. Yeginsu, *supra* note 176.

183. *See Internet Privacy Laws Revealed–How your Personal Information is Protected Online*, THOMPSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online (last visited Sept. 15, 2021).

184. Elizabeth Culliford, *How Political Campaigns Use Your Data*, REUTERS (Oct. 12, 2020), https://graphics.reuters.com/USA-ELECTION/DATA-VISUAL/yxmvjjgojvr/.

185. *See id.*

186. *See, e.g.*, Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, 20 PITT. J. TECH. LAW & POL'Y 41 (2020).

187. *See* Kil Huh, Amber Ivey & Dan Kitson, Opinion, *Using Data to Improve Policy Decisions*, PEW (Aug. 14, 2018), https://www.pewtrusts.org/en/about/news-room/opinion/2018/08/13/using-data-to-improve-policy-decisions.

188. *See, e.g.*, Joe Parkinson et. al., *Huawei Technicians Helped African Governments Spy on Political Opponents*, WALL ST. J. (Aug. 15, 2019), https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017; Freek van Gils, Wieland Müller & Jens Prüfer, *Big Data and Democracy* (Tilburg Univ. L. & Econ. Ctr., Discussion Paper No. 2020-003, 2020), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3556512# (examining how big data can impact the electoral process).

Finally, state, local, and national governments collect, demand, maintain, and share information to assist with a host of regulatory functions, including taxation, welfare benefits, and regulation of markets. Tax law, for example, is replete with record keeping and information reporting requirements about taxpayers and third parties. Examples include offshore financial asset reporting, multinational cross-border reporting, employee withholding, and property tax databases.[189] More recently, governments have also used data to score both people and businesses on a wide range of metrics.[190] In some cases, stringent rules may restrict access and sharing of data, such as rules protecting tax return data.[191] But in other contexts, there is evidence that information accumulated for one government function has been used for an unrelated one, such as use of driver's license databases by ICE.[192]

It cannot be emphasized enough that data collected for one objective may be sold, shared, or used for other purposes.[193] As the information-economics literature has recognized, the same information can mean very different things to different actors (e.g., a Facebook post seen by a friend as opposed to ICE), the value of information can change over time (e.g., Trump's tax return information before and after he became President), and perhaps most powerfully, "the value and sensitivity of one piece of personal information will change depending on the other pieces of data with which it can be combined."[194] Secondary uses of data may be more widespread than primary uses, a point reflected in the final "dissemination" step of the life cycle of data concept.[195]

As recognized by the information economics literature, data's nonrival character—particularly in light of digitization and the increasing efficiencies that data can generate in combination with other data sources—renders the

189. *See, e.g.*, 26 U.S.C. §§ 1471–1474 (FATCA provisions), 26 U.S.C. § 6041 (information reporting); 26 U.S.C. § 3402 (employee withholding).

190. *See, e.g.*, Nizan Geslevich Packin & Yafit Lev Aretz, *Algorithmic Analysis of Social Behavior for Profiling, Ranking, and Assessment*, *in* CAMBRIDGE HANDBOOK ON THE LAW OF ALGORITHMS 632 (Woodrow Barfield & Ugo Pagallo eds., 2020); John Butcher, *China to Companies: Show Tax Compliance or Risk Punishment*, BLOOMBERG TAX (Dec. 19, 2018), https://news.bloombergtax.com/daily-tax-report-international/china-to-companies-show-tax-compliance-or-risk-punishment (detailing China's tax portion of its "social credit system").

191. *See, e.g.*, 26 U.S.C. § 6103.

192. Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

193. *See* sources cited *supra* note 159; Kirsten Martin, Privacy Governance for Institutional Trust (June 12, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3394979 (explaining secondary use decisions are made without reference to original consumer); *see, e.g.*, Adam B. Thimmesch, *Transacting in Data: Tax, Privacy, and the New Economy,* 94 DENV. L. REV. 145, 146 (2016).

194. *See* Acquisti et al., *supra* note 22, at 447.

195. *See, e.g.*, Wing, *supra* note 146.

issue of secondary uses absolutely critical.[196] The potential for secondary use, paired with law's reticence in proscribing such uses, transforms widely available data into truly ubiquitous data. That is, if rights to use and share data are expansive and data is nonrival, then the commercial interest in acquiring vast quantities of data will undoubtedly grow, particularly as processing capabilities increase.

2. Myriad Collectors

Data is collected, stored, used, and reused by different actors including governments, businesses, and individuals. Different actors have distinctive advantages and disadvantages with respect to data. Governments may demand data by law, for example, accumulating data through census taking, tax and immigration records, or surveillance.[197] Governments may also require that data be turned over by private actors like Facebook, Google, or counterparties to business transactions.[198]

Businesses have different advantages. They can condition access to goods, services, or employment on provision of data and can obscure how such data is collected and used.[199] Businesses "request" data by linking it to discounts or other benefits.[200] Websites use cookies to hold and store data, which may be

196. Some strands of information economics advocate designing data rights to expand the ability to create, use, and disseminate data, and to generate increased efficiencies. *See, e.g.*, Jones & Tonetti, *supra* note 159.

197. *See, e.g.*, 26 U.S.C. § 6041 (collection of tax information at source). The contemporary international tax framework, for example, stipulates country-by-country (CbC) reporting of a huge amount of tax and business activity information by multinational corporations to governments. ORG. FOR ECON. COOP. & DEV., COUNTRY-BY-COUNTRY REPORTING: HANDBOOK ON EFFECTIVE TASK RISK ASSESSMENT (2017), https://www.oecd.org/tax/beps/country-by-country-reporting-handbook-on-effective-tax-risk-assessment.pdf. CbC reporting has been adopted by ninety countries and requires multinational corporations to provide certain data for each country in which they operate. *Action 13 Country-by-Country Reporting*, ORG. FOR ECON. COOP. & DEV., http://www.oecd.org/tax/beps/beps-actions/action13/ (last visited Sept. 28, 2021); *see also Signatories of the Multilateral Competent Authority Agreement on the Exchange of Country-by-Country Reports (CbC MCAA) and Signing Dates*, ORG. FOR ECON. COOP. & DEV., http://www.oecd.org/tax/beps/CbC-MCAA-Signatories.pdf (last updated Aug. 12, 2021).

198. *See Government Requests for User Data*, FACEBOOK TRANSPARENCY CENTER, https://transparency.fb.com/data/government-data-requests/ (last visited Sept. 15, 2021); Alfred Ng, *Google Reports All-Time High of Government Data Requests*, CNET (Sept. 28, 2017), https://www.cnet.com/tech/services-and-software/google-reports-all-time-high-of-government-data-requests/.

199. *See, e.g.*, Yeginsu, *supra* note 176.

200. Mekebeb Tesfaye, *Financial Service Consumers Are Willing to Share Their Personal Data for Benefits and Discounts*, INSIDER (Mar. 18, 2019), https://www.businessinsider.com/financial-service-consumers-share-personal-data-for-benefits-discounts-2019-3?op=1.

used for advertising and other purposes.[201] While cookie use is now usually disclosed, options to decline remain limited.[202]

Individuals—with the help of digital technologies, the internet, and social media platforms—also have increasing ability to disseminate, access, and analyze data, both about themselves and others.[203] In the digital age, individuals can easily disseminate both contemporary and historic information about others through online reviews, social media shaming, and "internet vigilantism."[204] While individual actors have less ability to demand provision or maintenance of data than governments or businesses, they may be less constrained and more erratic in using data once obtained.[205]

3. Changing Uses

Another important point is that uses of data are changing, spurred by the growing ease with which data can be accessed and analyzed and by improvements in available technologies. Data analytics is, for example, transforming how policing is done and how national security surveillance is performed.[206] Data analytics is also transforming tax administration.[207] Although the IRS has long relied on data-driven methods to identify audit targets (including its famous Discriminate Inventory Function (DIF) score originating in the 1960s), new technologies are enabling it to move its data use to a new level.[208] The IRS's commitment to building capacity and using data analytics in tax administration is evidenced by its formation of the Research, Applied Analytics, and Statistics Division in November 2016.[209] Businesses can also process and analyze data in unanticipated ways, as the Lenddo example

---

201. *Internet Cookies*, FED. TRADE COMM'N, https://www.ftc.gov/site-information/privacy-policy/internet-cookies (last updated May 2021).

202. Noah Ramirez, *Cookie Consent Requirements: Are You Doing Enough?*, OSANO (May 23, 2021), https://www.osano.com/articles/cookie-consent-requirements.

203. *See, e.g.*, Kevin Roose, *A Machine May Not Take Your Job, But One Could Become Your Boss*, N.Y. TIMES (June 23, 2019), https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html (detailing ways in which AI "make[s] workers more effective by giving them real-time feedback" on their performance).

204. *See, e.g.*, Jessica A. Clarke, *The Rules of #MeToo*, 2019 UNIV. CHI. LEGAL F. 37, 58 (2019); Audrey Jiajia Li, Opinion, *Who's Afraid of China's Internet Vigilantes,* N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/opinion/china-privacy.html.

205. *See, e.g.*, Nellie Bowles, *How 'Doxxing' Became a Mainstream Tool in the Culture Wars*, N.Y. TIMES (Aug. 30, 2017), https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html.

206. *See, e.g.*, Brayne, *supra* note 11.

207. Justin Rohrlich, *The IRS Wants to Use Social Media to Catch Tax Cheats*, QUARTZ (Dec. 26, 2018), https://qz.com/1507962/the-irs-wants-to-use-facebook-and-instagram-to-catch-tax-evaders/.

208. Carina C. Federico & David B. Blair, *Insight: Automation and Data Analytics to Drive LB&I Audit Selection*, BLOOMBERG TAX (June 5, 2019), https://news.bloombergtax.com/daily-tax-report/insight-automation-and-data-analytics-to-drive-lb-i-audit-selection; Thimmesch, *supra* note 193. Bruce Zagaris, *Data Analytics Show the Way to Progress in International Tax Enforcement*, 95 TAX NOTES INT'L 623, 625–27 (2019).

209. *See* Federico & Blair, *supra* note 208.

reveals,[210] and may hold funding and technological advantages over governments in acquiring and working with evolving types and quantities of data.

An important new frontier in how data is used is machine learning, in which computers are fed large quantities of training data selected via mathematical models in order to learn to perform tasks.[211] This enables computers to learn automatically, without human intervention or instruction, and to do tasks such as filtering spam email, image recognition, targeted advertising, and medical diagnosis.[212] Machine learning enhances our capacity to improve behavior, detect and prove criminal conduct, and *predict* who will be the next criminal, tortfeasor, or tax evader.[213] It also has the capacity to change law. For example, the computational-law movement asks, as its organizing questions, whether artificial intelligence and machines can replace judicial decision-making and whether "legal singularity," in which law becomes increasingly perfectly specified, can be reached.[214] The rapid rise in algorithm use across many fields has instigated questions about the risks of algorithmic decision-making given that underlying data may be inaccurate, and that both data and algorithms may reflect racial or other biases.[215] The answers to these questions will become ever more crucial as direct human decision-making decreases and algorithmic decision-making increases.

There are other, related uses of data. As noted, technologies and products—such as cars with maximum speed limits—can now be designed to make unlawful or ill-advised behaviors impossible, and such technologies necessarily rely on data and information to operate.[216] In the political sphere, social media platforms have been used to manipulate voter attitudes and

210. *See supra* notes 165–167 and accompanying text.

211. *See* Benjamin Alarie, Anthony Niblett & Albert H. Yoon, *Regulation by Machine* (Univ. of Toronto Working Paper, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2878950; Benjamin Alarie, Anthony Niblett & Albert H. Yoon, *Using Machine Learning to Predict Outcomes in Tax Law* (Univ. of Toronto Working Paper, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2855977. There are many machine-learning variations; for example, it can be supervised or unsupervised. Devin Soni, *Supervised vs. Unsupervised Learning*, TOWARDS DATA SCI. (Mar. 22, 2018), https://towardsdatascience.com/supervised-vs-unsupervised-learning-14f68e32ea8d.

212. Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 89–93 (2014); *see also* Stuart A. Thompson, Opinion, *These Ads Think They Know You*, N.Y. TIMES (Apr. 30, 2019), https://www.nytimes.com/interactive/2019/04/30/opinion/privacy-targeted-advertising.html; Kwet, *supra* note 154.

213. Neil Shah, Nandish Bhagat & Manan Shah, *Crime Forecasting: A Machine Learning and Computer Vision Approach to Crime Prediction and Prevention*, VISUAL COMPUTING FOR INDUS., BIOMEDICINE & ART (Apr. 29, 2021) https://vciba.springeropen.com/track/pdf/10.1186/s42492-021-00075-z.pdf.

214. Benjamin Alarie, *The Path of the Law: Toward Legal Singularity* (Univ. of Toronto Working Paper, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2767835; Michael A. Livermore, *Rule by Rules*, *in* COMPUTATIONAL LEGAL STUDIES: THE PROMISE AND CHALLENGE OF DATA-DRIVEN LEGAL RESEARCH 238 (Ryan Whalen ed. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3387701.

215. *See, e.g.*, Kroll, *supra* note 2.

216. *See* sources cited *supra* note 24.

preferences and to sow misinformation.[217] In business, misinformation is increasingly used to market products and influence consumer preferences, and "disinformation for hire" public relations firms can be engaged to sow misinformation.[218] These technologies and uses are ever changing and becoming more sophisticated.[219]

The evolving uses of data open up many possibilities for more efficient and effective regulation and enforcement of law, and with it, declining space for slack. But this trend carries risks, including the risk of algorithmic discrimination, risks to individual self-determination, and risks to democracy. The speed and likelihood of changing uses means that the evaluation of data's benefits and risks is an evolving, yet increasingly critical, exercise.

4. Changing Methods of Collection

How data is collected is also changing. For one thing, even when individuals do not actively surrender data, "big data" technologies allow inferences to be made based on the behaviors of those around them.[220] For example, Facebook can garner information about a person, even if they never post or are not a user, by compiling information distilled from their social circle.[221] This ability to lose privacy and control over one's data through social links has been described as "privacy dependencies,"[222] a reality that complicates efforts to protect data rights, privacy, and access.

Data can also increasingly be obtained illegally, such as through hacks and leaks.[223] Legitimately collected data that is hacked or leaked may become subject to illegitimate uses[224] but may also help with law enforcement, as we have described in previous work.[225] Current data protection regimes, such as

---

217. Craig Silverman, Jane Lytvynenko & William Kung, *Disinformation for Hire: How a New Breed of PR Firms Is Selling Lies Online*, BUZZFEED NEWS (Jan. 6, 2020), https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms.

218. *Id.*

219. *See* Trautman, *supra* note 186; Matthew Rosenberg, Nicole Perlroth & David E. Sanger, *'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020*, N.Y. TIMES (Sept. 10, 2020), https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

220. *See* Zeynep Tufekci, *Think You're Discreet Online? Think Again*, N.Y. TIMES (Apr. 21, 2019), https://www.nytimes.com/2019/04/21/opinion/computational-inference.html.

221. *Id.*

222. Solon Barocas & Karen Levy, *Privacy Dependencies,* 95 WASH. L. REV. 555, 555 (2020) (articulating how "our privacy depends on the decisions and disclosure of other people"); *see also* Zraick & Zaveri, *supra* note 181 (discussing a Harvard student denied entry to the United States based on friends' social media posts).

223. *See, e.g.*, David S. Wall, *How Big Data Feeds Big Crime*, 117 CURRENT HIST. 29 (2018); Michael Hatfield, *Cybersecurity and Tax Reform*, 93 IND. L.J. 1161 (2018).

224. *See, e.g.*, Jeb Su, *Data Breach Alert: Over 1 Million Credit Card Data from the U.S., South Korea Have Been Leaked*, FORBES (Aug. 5, 2019), https://www.forbes.com/sites/jeanbaptiste/2019/08/05/data-leak-alert-over-1-million-credit-card-from-the-u-s-south-korea-have-been-stolen/#55e89e06928e.

225. *See* Oei & Ring, *supra* note 180.

fiduciary obligations on data custodians, have proven insufficient to protect against illegal transmission.

B. Data's Potential Impacts on Slack

Given the complex data landscape, it is not surprising that the national conversation about data has underscored both its benefits (such as increased security)[226] and its negative effects (such as bias, compromised privacy, and excessive surveillance).[227] We now examine how data affects slack in the legal system. The upshot is that just as slack itself is a mixed bag, data may have positive effects on the allocation of slack but also carries risks.

1. Less Slack

Data has made human missteps more detectable, traceable, memorable, and subject to monitoring. This shift has put pressure on slack, particularly slack originating in information imperfections. Perhaps most problematically, increasingly available data makes it easier to enforce unjust or out-of-step laws.[228] But data also affects other types of slack, for example, by casting sunshine on politically driven or mercy driven slack.

At the risk of stating the obvious, it is worth explicitly delineating the mechanisms through which data reduces slack. First, digitization has created greater capacity to store, transfer, and steal information. Second, data is nonrival.[229] Thus, various actors are collecting large quantities of data, much of which is tangential to their own interests, on the theory that such data can be resold and used by others. Third, data can be integrated into new artificial intelligence and algorithmic systems to generate predictions and insights.[230] The ability of intelligent machines and algorithmic systems to process data, generate insights, and suggest responses means that consequences for actions, inactions, or mere possession of personal characteristics may occur more swiftly.[231] Fourth, law often permits data sharing, or is powerless to stop it.[232] The end

226. *See, e.g.*, James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html; Gerstell, *supra* note 168.

227. *See, e.g.*, Richards, *supra* note 2; Harmon, *supra* note 19.

228. *See, e.g.*, Will Douglas Heaven, *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled*, MIT TECH. REV. (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/. Of course, extremely weird laws that are not very consequential are unlikely to become more enforced after data.

229. Acquisti et al., *supra* note 22, at 446.

230. *See* Brayne, *supra* note 11, at 981.

231. *See* sources cited *supra* notes 206–215 and accompanying text.

232. *See generally* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (describing the U.S. as having "only a patchwork of sector-specific laws").

result is that information about imperfect behaviors is more likely to be detected and processed and is more likely to generate consequences.

Some real-world examples add texture. Social media sites contain vast quantities of digitized information. This allows authorities to use this information for law enforcement, as recent examples from tax and immigration attest.[233] Other sources of digitized information can be used for various purposes: a Washington Post story recently described how ICE uses facial recognition technology to search state driver's license photos for undocumented immigrants.[234] We now know that the Department of Homeland Security is using cellphone location data purchased from a commercial vendor for immigration enforcement.[235] Searchable health and financial records can be used to prove false claims to insurers or lenders.[236] Mobile phone location technologies allow law enforcement to use location information to monitor and sanction.[237] Data from personal activity trackers can provide evidence to convict persons of a crime.[238] The use of big data in policing has effectively amplified surveillance activities, lowered thresholds for inclusion in enforcement databases, and drawn increasing numbers of individuals into the surveillance net.[239] On a micro level, nontraditional algorithms employed by governments or businesses such as Lenddo[240] mean that personal traits or shortcomings can now have legal and economic repercussions (such as being turned down for loans).[241]

These examples illustrate how a combination of digitizable, monetizable, and transferable information—which can be used by human enforcers or fed

---

233. *See* Rohrlich, *supra* note 207 (describing IRS monitoring of social media sites to detect noncompliance); Zraick & Zaveri, *supra* note 181 (describing immigration enforcement using social media information).

234. Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

235. Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=hp_lead_pos5.

236. Trevor Lloyd-Jones, *The Power of Analytics for Insurance Fraud Detection*, LEXISNEXIS (Apr. 4, 2018), https://blogs.lexisnexis.com/insurance-insights/2018/04/the-power-of-analytics-for-insurance-fraud-detection/.

237. Valentino-DeVries, *supra* note 160.

238. *See, e.g.*, Hauser, *supra* note 177 (describing police reliance on victim's Fitbit to document time of murder and presence of accused); Christine Hauser, *In Connecticut Murder Case, a Fitbit Is a Silent Witness*, N.Y. TIMES (Apr. 27, 2017), https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html (noting Fitbit data contradicted husband's claim that intruders broke into their home and tied him up and shot his wife).

239. Brayne, *supra* note 11, at 985.

240. *See, e.g.*, Michal Gromek, *Social Scoring in Finance: We are Partly Already There*, FORBES (July 25, 2018), https://www.forbes.com/sites/michalgromek/2018/07/25/social-scoring-in-finance-we-are-partly-already-there/#4fde589760bd.

241. *See* Bary, *supra* note 164.

to machine enforcers[242] and whose transfer is allowed by law—has led to more pressure on slack, whether in the form of punishment, exclusion from benefits or protections, increased surveillance, or more stringent terms of engagement. As data collection, processing, transfer, and usage become more prevalent, this pressure is likely to increase.

2. Inconsistent Impacts of Data on Slack

Data has become increasingly ubiquitous through a gradual and uneven process. Some types of information are generated more quickly, and some technologies will take hold more rapidly than others. This suggests that the impacts of data on slack will be inconsistent, particularly with respect to pockets of slack stemming from information imperfections. The following are some of the likely disparities.

Sophisticated Actors. Contraction of slack is likely occurring in a way that favors sophisticated actors. Those who understand how their data is accessed and what steps they can take to protect or hide it may better resist slack's contraction.[243] From a life cycle of data perspective,[244] there are several points where sophisticated actors with more knowledge, power, or resources can minimize the flow of their data. Most obviously, they can better prevent acquisition but may also be better equipped to stop any sharing or repurposing of their data and may even have the capacity to withdraw data from the pool.[245] Conversely, data trails left by less sophisticated actors may be low-hanging fruit, readily available to enforcers. Particularly in the now-pervasive situation where agencies are resource constrained, such data risks being used immediately to sort, monitor, and sanction more efficiently.[246] The confluence of resource-constrained agencies and differences in data trails can amplify disparities in the contraction of slack.

Uneven contraction of slack across different populations is troubling, particularly to the extent that sophistication correlates with factors such as race, class, or socioeconomic status.[247] It would be one thing if it could be shown that unsophisticated actors were previously accorded disproportionate amounts

242. *See*, *e.g.*, Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 15 (2019); Albert Meijer & Martijin Wessels, *Predictive Policing: Review of Benefits and Drawbacks*, 42 INT'L J. PUB. ADMIN. 1031 (2019).

243. *See, e.g.*, Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerability for Poor Americans*, 95 WASH. U. L. REV. 53 (2017); Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389 (2012); Ryan Calo, *Privacy, Vulnerability, and Affordance*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 198 (Evan Salinger, Jules Polonetsky & Omer Tene eds., 2018).

244. *See generally* Wing, *supra* note 146.

245. *See* Madden et al., *supra* note 243, at 64–67.

246. Mary Madden, *The Devastating Consequences of Being Poor in the Digital Age*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

247. *Id.*

of slack and data is now recalibrating the balance. But, in fact, the reverse is more likely.[248]

Government and Institutional Actors. Institutional actors, such as corporations, platforms, and governments, may be better positioned to access and process data than individuals who are data subjects. This raises not just privacy issues but has real consequences for slack.[249] Individuals may not fully appreciate how institutional actors collect and use their data and what legal ramifications this may hold for the future.

One important reason why institutional actors may hold advantages over individuals relates to eroding practical constraints. While government and institutional actors have long had access to data, they have confronted technological limitations, such as the limited digitalization of data.[250] But these limitations are disappearing. Another structural reason stems from the emergence of active data marketplaces that operate in an environment with relatively few legal constraints.[251] Institutional actors have more ability than individuals to participate in these marketplaces as buyers and sellers of data.[252]

Targeting and Bias. To the extent governments, institutional actors, and private-sector actors interact selectively and unevenly with different demographic groups or choose to enforce unjust laws, the diminishing slack that accompanies ubiquitous data will compound problems for those constituencies. Governments are powerful aggregators and users of data, deploying it to conduct immigration, law enforcement, and other functions.[253] And, it is well recognized that government agencies (including police departments) may disproportionately target some racial groups, may set enforcement priorities that have the indirect effect of targeting, or may selectively pursue enforcement of overbroad laws.[254] If data enables targeting

248. *See* Madden et al., *supra* note 243, at 104–08.

249. For example, the European Union's new rules requiring notification to individuals when their data is collected derive from concerns about privacy and control over one's data. *See* Andrew Rossow, *The Birth Of GDPR: What Is It and What You Need to Know*, FORBES, (May 15, 2018), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=4a32596155e5.

250. Sarah Kliff & Margot Sanger-Katz, *Bottleneck for U.S. Coronavirus Response: The Fax Machine*, N.Y. TIMES (July 13, 2020), https://www.nytimes.com/2020/07/13/upshot/coronavirus-response-fax-machines.html.

251. *See* David Tang et al., *Value of Data: The Dawn of the Data Marketplace*, ACCENTURE (Sept. 7, 2018), https://www.accenture.com/us-en/insights/high-tech/dawn-of-data-marketplace.

252. To be sure, individuals may participate, such as through aggregation of individual opinions (e.g., Consumer Reports or online reviews) but enjoy fewer opportunities. *But see id.*

253. Access to data may favor the government over criminal defendants. *See* Rebecca Wexler, *Privacy Asymmetries: Access to Data in the Criminal Justice System*, 68 U.C.L.A. L. REV. 212 (forthcoming 2021) (manuscript at 18–20), https://ssrn.com/abstract=3428607 (comparing governments' and defendants' abilities to demand evidence from third-parties in criminal cases).

254. THE NAT'L ACAD. OF SCIS., ENG'G, AND MED., PROACTIVE POLICING: EFFECTS ON CRIME AND COMMUNITIES 254–58 (2018).

to be done more easily, the latitude available to targeted groups will shrink, particularly if that group is less able to withdraw from the dragnet.

Take, for example, ICE's use of facial recognition technologies to mine state driver's license databases for undocumented immigrants.[255] This is the first known instance of facial recognition technology use on these databases,[256] and it creates two types of uneven impacts. First, undocumented immigrants as a group are being targeted, and the targeting is now more effective due to technology, so available slack will shrink for them. Second, facial recognition technologies are not perfect, and their biases, which include greater likelihood of misidentifying people of color, are increasingly appreciated.[257] Thus, government use of data to enforce the law against undocumented immigrants also creates disproportionate risks for other groups (here, misidentified individuals and people of color).[258]

Another example comes from tax. In 2010, the U.S. passed the Foreign Account Tax Compliance Act (FATCA) and tightened enforcement of the longstanding foreign bank account reporting (FBAR) rules.[259] These rules are aimed at deterring offshore tax evasion by increasing reporting of foreign financial asset information (e.g., bank accounts) to the government and tightening up enforcement.[260] As a result, a taxpayer's failure to report the existence of a foreign financial asset is now subject to extremely high penalties.[261] Although the motivation behind these initiatives was tax evasion by wealthy Americans, there is increasing recognition that these regimes have also affected immigrants in the U.S. and Americans living abroad.[262] The latter individuals, who have lives and connections in other countries, are now also subject to onerous U.S. tax and financial reporting regimes and penalties (albeit with some attenuation for those living abroad).[263] Moreover, they may have less access to good tax advice and less ability to minimize their risks by ceasing to hold assets offshore. Thus, FATCA is a case of how even a well-intentioned

255. Edmondson, *supra* note 192.

256. *Id.*

257. Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html?module=inline.

258. *See, e.g.*, Thomas B. Nachbar, *Algorithm Fairness, Algorithmic Discrimination* (Va. Pub. L. & Legal Theory, Research Paper No. 2020-11, 2020), https://ssrn.com/abstract=3530053; Robert H. Sloan & Richard Warner, *Beyond Bias: Artificial Intelligence and Social Justice*, 24 VA. J.L. & TECH. 1 (2020).

259. *See* 31 U.S.C. § 5314; 31 C.F.R. § 1010.350 (2020); Foreign Account Tax Compliance Act, Pub. L. No. 111-147, § 1471, 24 Stat. 71, 97 (2010) (codified as amended at 26 U.S.C. §§ 1471–74).

260. 31 U.S.C. § 5311.

261. *Id.* § 5321(a)(1).

262. *See, e.g.*, NAT'L TAXPAYER ADVOC. SERV., ANNUAL REPORT TO CONGRESS 79–93, *supra* note 125 (criticizing IRS Offshore Voluntary Disclosure Program penalties as being applied regressively); NAT'L TAXPAYER ADVOC., ANNUAL REPORT TO CONGRESS 400–02 (2018) (citing equity concerns with FBAR penalties).

263. 26 C.F.R. § 1.6038D-2(a)(3) (2016).

law aimed at improving enforcement through increased data gathering may inadvertently create unintended and unfair impacts.

Foreign Actors. Data may also help aggressive states and actors. As the 2016 presidential election revealed, actors beyond a nation's borders can successfully gather and manipulate domestically collected data.[264] This poses not only privacy risks but risks to fair elections, democratic processes, and political stability. The risks are not purely domestic. If foreign actors (potentially subject to fewer legal constraints and oversight) can comprehensively collect data on U.S. individuals and organizations, then U.S. actors may find themselves targeted in enforcement actions abroad. In short, the rise of data and the contraction of slack may allow aggressive state and institutional actors to weaponize their legal systems against subjects from other countries.

There is also the risk of foreign actors strategically using data they have collected to force prosecutions or enforcement actions in the United States. For example, a foreign actor could acquire data (legally or illegally), mine it to develop a case against U.S. individuals or businesses, and then advocate for enforcement by U.S. authorities by using the press or political channels. Even if the case has merit, the potential use of data to selectively pressure U.S. authorities into action should raise concerns. Moreover, there is no guarantee that such data is accurate. Past data leaks have demonstrated that data can be falsified.[265] False information can be fact checked, but only after significant disruption, loss of reputation, and expenditure of resources.[266]

Structurally speaking, the power of aggressive foreign actors stems from the difficulty of containing data within national borders. States have attempted to do so—for example, the European Union has engaged in continual efforts to control data accessible both in and outside the European Union—but it is unclear how successful these efforts will be.[267]

3. The Limits of Sunshine and Scrutiny

As outlined in Part I.B, sometimes slack stems from politically motivated nonenforcement decisions, while other times it arises from resource constraints (which can reflect deliberate and nondeliberate elements). Data can cast sunshine on these decisions by alerting observers to slack's existence. For example, the 2010 enactment of FATCA[268] and the introduction of similar tax

264. Jonathan Masters, *Russia, Trump, and the 2016 U.S. Election*, COUNCIL ON FOREIGN RELS. (Feb. 26, 2018, 7:00 AM), https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

265. Oei & Ring, *supra* note 180, at 578.

266. *See id.*

267. Case C-18/18, Glawischnig-Piesczek v. Facebook Ir., ECLI:EU:C:2019:821 (Oct. 3, 2019) (ruling that countries can force Facebook to take down posts not only in their own country but abroad); *see also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 138-147 (2017).

268. *See supra* notes 259–262 and accompanying text.

information transparency initiatives in other countries were motivated in part by whistleblower complaints and data leaks,[269] which allowed investigative journalists to expose sophisticated or politically connected taxpayers who were not held accountable by tax authorities.[270] This publicity effectively spurred the U.S. and other countries to act.

The increasing visibility of nonenforcement (particularly where it occurs disparately) may help increase accountability. However, sunshine may not be sufficient to combat inconsistent allocation and contraction of slack across populations.[271] Even with more data, the public's ability to monitor government enforcement practices will likely remain outpaced by the ability of enforcers to act quickly and the ability of sophisticated actors to hide their noncompliance. Sunshine may ultimately subject problematic data uses and enforcement choices to scrutiny, but there will inevitably be transition periods where governments and sophisticated actors have a first-mover advantage. Moreover, while the enforcement harms grounded in digital data are generally experienced by targets immediately, the remedial effects of data-driven sunshine on troubling enforcement practices can take much longer; sunshine must give rise to outrage that in turn triggers action, while enforcement is direct action.[272] Thus, increased scrutiny of government data use may be of limited value.

4. New Versions of Targeted Enforcement

Increasing access to data may generate new methods of targeted enforcement and greater opportunities to achieve it. For example, machine learning is giving rise to increased surveillance and new methods of enforcement such as predictive policing.[273] To the extent that machine-learning algorithms that monitor or predict behavior are written using data inputs, human biases may shape those algorithms.[274] As data is fed to machines that spit out decisions, discriminatory impacts may persist and disseminate, and unfair targeting may result. Under-resourced agencies may be particularly motivated to find low-cost ways of using data algorithmically to target enforcement, which exacerbates the risk of unjust outcomes.

---

269. Oei & Ring, *supra* note 180, at 537; *see also* Shu-Yi Oei, *The Offshore Tax Enforcement Dragnet*, 67 EMORY L.J. 655, 660 (2018).

270. Oei & Ring, *supra* note 180, at 559–61 (detailing consequences for various politicians). For example, the International Consortium of Investigative Journalists has helped expose offshore tax evasion and avoidance through caches of leaked data. *See* INT'L CONSORTIUM OF INVESTIGATIVE JOURNALISTS, https://www.icij.org/ (last visited Sept. 16, 2021).

271. *See supra* Part II.B.2.

272. *See* sources cited *supra* note 104.

273. *See, e.g.*, Annette Vestby & Jonas Vestby, *Machine Learning and the Police: Asking the Right Questions*, 15 POLICING: J. POL'Y & PRAC. 44 (2019).

274. *See, e.g.*, Lohr, *supra* note 257.

Importantly, even if enforcement is not undertaken, the possession of data and the ability to share and use it changes the power dynamics and relationships among various actors. For example, even if the government does not use all data in its possession, the fact that it possesses the data at all may serve as a bargaining chip over individual and firm behavior. This alters trust relationships, power dynamics, and social and economic interactions between government and the governed.

5. Changing and Directing Individual Conduct

Increasingly available data also gives individuals and other actors more information about the consequences of their actions. From cars that monitor driver reaction times[275] to portable breathalyzers to fitness trackers to financial monitoring apps, there are diverse ways to evaluate human conduct in real time and suggest corrective action. This has prompted some scholars to suggest that the era of personalized law, in which human behavior can be regulated via microdirectives, is upon us.[276]

The development of these data capabilities holds important consequences. First, the impacts of such technologies will likely vary based on factors like age or technological sophistication; some individuals will not be adept at interpreting data or acting on it, so it is highly unlikely that everyone will suddenly start behaving perfectly. Second, the availability of more information may actually cause some to put more effort into hiding, not eliminating, bad behaviors.[277] Finally, data will probably not change individual behaviors with respect to patently out-of-step or outdated laws.

If one persists in behaving badly despite data-based technologies that direct or suggest otherwise, this may eventually be viewed as deliberate bad intent, which may be used to justify harsher *ex post* consequences.[278] For example, if one persists in smoking and failing to exercise even after health trackers warn of poor health, we could envision this data being used by insurers to deny coverage or raise rates or by politicians to justify denial of public benefits based on individual responsibility arguments. A potential long-term outcome is that we may see less bad behavior (or more hiding of it) but harsher judgment of those who do behave poorly. Here too, there may be disparities and uneven impacts.

---

275. *See* Christina Rogers, *What Your Car Knows About You*, WALL ST. J. (Aug. 18, 2018), https://www.wsj.com/articles/what-your-car-knows-about-you-1534564861.

276. *See, e.g.*, Anthony J. Casey & Anthony Niblett, *The Death of Rules and Standards*, 92 IND. L.J. 1401 (2017); Anthony J. Casey & Anthony Niblett, *A Framework for the New Personalization of Law*, 86 U. CHI. L. REV. 333 (2019).

277. Casey & Niblett, *A Framework for the New Personalization of Law*, *supra* note 276, at 347–48.

278. Casey & Niblett, *The Death of Rules and Standards*, *supra* note 276, at 1408.

6. Calling Law's Design into Question

Ultimately, ubiquitous data may call the design and legitimacy of existing laws into question. Imagine a city that requires dog owners to register their dogs for a $50 fee, and whose laws provide that an owner of an unregistered dog will be fined $5,000 for each failure to register. This fine is severe in relation to the registration fee. Assuming that it is difficult to get information about each dog within the city limits, the hefty fine might have been imposed to deter nonregistration. The hope is that rational dog owners will weigh the probability of detection (low) against the magnitude of the fine (high) and register the dog.[279] Now assume that technology develops that can detect the location of every dog and transmit that information to the city. The city can now issue tickets on a mass scale to fine owners of unregistered dogs. If this were to happen, we might now view the $5,000 fine as too harsh. The newly available dog-location data arguably transforms a high penalty designed to deter nonregistration given low detection probabilities into one that is too draconian now that detection is much easier.[280]

Statutory and regulatory penalties aside, increased information may also have implications for the design and computation of court-awarded damages. For example, if increased information enables judges to more accurately assess appropriate monetary damages, this could increase the efficiency of awarding damages over injunctions, upending conventional wisdom regarding optimal design of legal regimes.[281]

Data may also call into question the use of *ex post* remedies. Take for example, bankruptcy, which offers a way to manage financial distress. Bankruptcy law traditionally comes into play after a debtor has experienced financial distress and now seeks a debt discharge. In a world of imperfect information, *ex post* remedies like bankruptcy or bailout may seem the best and perhaps only way to deal with financial misfortune. It is difficult to detect bad decisions or consumption shocks on the front end, so we discharge debts on the back end. As data becomes more ubiquitous, however, lenders and regulators may have more ability to predict, observe, and evaluate individual financial choices in real time. It may become possible to employ measures to identify those on the verge of financial distress and prevent financial distress before it occurs. With more information, regulators could use borrowing restrictions, targeted income supplements, or financial counseling to help borrowers avert financial meltdown *ex ante*, rather than managing it *ex post*.

279. *See generally* Becker, *supra* note 7.

280. *Cf.* Price, *supra* note 17, at 1146.

281. *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972); *cf.* Brian Galle & Murat Mungan, *Predictable Punishments*, 11 U.C. IRVINE L. REV. 337, 337 (2021) (suggesting regulators should rely on punishments that remain accurate even when information is limited).

The above are just a few examples of how data may change our views of law and its optimal design. The broader observation is that increased data may lead us to identify necessary adjustments to legal rules, including different remedies, penalties, and regulatory approaches. Such adjustments are not merely technical. Rather, they raise moral and ethical questions, and may transform relationships among humans, governments, and the law.[282]

III. MANAGING SLACK IN THE DATA AGE

So far, this Article has explained how slack arises in the legal system, has presented a bounded defense of its importance while acknowledging its risks, and has revealed how increasingly ubiquitous data is reshaping slack and likely causing it to contract disparately for different populations along the lines of race, political power, and sophistication. Specifically, the worry is that some populations are likely to become low-hanging enforcement targets, while institutional and more aggressive data users will probably come out ahead.[283] This is particularly concerning because unjust laws may become easier to enforce. Furthermore, the increased sunshine that comes with data will likely be insufficient to fully alleviate any of these problems.

In short, this Article has demonstrated a fundamental tension: slack is valuable, but is sometimes problematic, and the reshaping of slack that accompanies data is also sometimes valuable but sometimes problematic. The question, then, is how to juggle this tension in managing the interplay between slack and data. This Part articulates a framework for managing the slack–data relationship and suggests concrete policy solutions.

A. Managing the Slack-Data Relationship

We start with a basic, relatively straightforward framework. We then explore its limitations and offer cautions.

1. A Seemingly Obvious Four-Part Framework

The tensions inherent in the interplay between slack and data suggest four seemingly obvious guiding principles. First, data should be used to deal with serious problems created by information constraints and the slack that results. Data should certainly be used to help solve serious crimes (such as murder) and to illuminate instances of unfair and differential enforcement and unjustified exercises of mercy (such as failure to hold privileged groups accountable).

---

282. *See* Roger Brownsword & Alon Harel, Editorial, *Law, Liberty, and Technology: Criminal Justice in the Context of Smart Machines*, 15 INT'L J.L. CONTEXT 107, 111–12 (2019) (noting potential changes in regulatory signaling effects on community moral aspirations).

283. Brayne, *supra* note 11, at 1003–04.

Second, we should avoid using data in ways that diminish slack in cases where it is valuable. Thus, we should resist using data to enforce unjust, out-of-step, or controversial laws (such as marijuana prohibitions), and should evaluate such uses carefully.[284] Likewise, we should guard against uses of data by legal regimes that engage in human rights abuses or targeting of political and other minorities, or that have weak rule-of-law values. We should also be less inclined to use data in ways that eliminate slack where the law contains poorly attenuated sanctions (e.g., draconian penalties) and does not already contain formal equitable or leniency provisions or both.[285] Conversely, we should be more amenable to using data to enforce laws that do have well-attenuated formal mechanisms providing flexibility and that are proportionate and well-designed.

Third, care should be taken to use data fairly. Thus, if data and information become available and can help solve serious crimes, then presumably that data should be used, absent offsetting considerations. But we should ensure that data is not used in ways that produce discriminatory impacts. For example, when using facial recognition technology to prevent or solve crimes, we should ensure that the technology is not biased and is not used in discriminatory ways.[286]

Finally, as data increases, the design of the law should be revisited. For example, if probabilities of detection rise significantly due to data, then we should consider lowering existing penalties and sanctions.[287] If data makes it possible, perhaps the law should move towards nudging people *ex ante* rather than punishing them *ex post*.

2. Problematizing the Framework

This basic framework may seem like a relatively clear articulation of how to manage the relationship between slack and data, at least in principle. However, there are a number of complications and objections.

First, it may not be clear whether a given instance of slack is problematic or valuable. In some cases (for example, laws regarding marijuana possession) people may disagree. Relatedly, whether an instance of slack is valuable or problematic may change over time as conditions change. For example, it may

284. Historical examples include slave-ownership laws, laws prohibiting persons of Chinese origin from immigrating, laws prohibiting interracial marriage, and laws criminalizing homosexual conduct. *See, e.g.*, Chinese Exclusion Act of 1882, Pub. L. No. 47-126, 22 Stat. 58; Fugitive Slave Act of 1850, 9 Stat. 462, *repealed by* Fugitive Slave Act of 1864, 13 Stat. 200.

285. Laws with draconian sanctions include some tax provisions (such as the penalties for undeclared foreign financial assets) and drug sentencing. *See, e.g.*, NAT'L TAXPAYER ADVOC., ANNUAL REPORT TO CONGRESS, *supra* note 262; Fair Sentencing Act of 2010, Pub. L. No. 111-220, 124 Stat. 2372 (to be codified as amended in scattered sections of 21 U.S.C.) (eliminating mandatory five-year sentence for crack cocaine to reduce disparity with penalties for powder cocaine); Kyle Graham, *Sorry Seems to be the Hardest Word: The Fair Sentencing Act of 2010, Crack, and Methamphetamine*, 45 U. RICH. L. REV. 765, 770 (2010).

286. *See* Lohr, *supra* note 257.

287. *See, e.g.*, A. Mitchell Polinsky & Steven Shavell, *The Theory of Public Enforcement of Law, in* 1 HANDBOOK OF LAW AND ECONOMICS 403, 407–20 (Polinsky & Shavell eds., 2006).

depend on political conditions, the state of democracy, the strength of rule-of-law values, or the existence of a global pandemic.

Second, there may be mixed cases. There may be situations where the crime is serious and slack is a problem, but data can only be used in a way that is likely to give rise to disparities (e.g., due to technology limitations) or where the distributive fallout is uncertain or unknowable.[288] Or, we may confront a case where the crime is serious, but the sanction is too severe and there is little equitable flexibility in the law. Here, there are benefits to slack in the system but also reasons to want increased enforcement, and the framework may not tell us how to proceed.

Third, the framework may yield problematic incentives in the long run. Slack may be valuable in the current moment but may have negative effects over time, for example, by allowing bad laws to stay on the books unnoticed because they are not being enforced.[289] These dynamics may raise rule-of-law concerns.

Fourth, it is difficult to prevent cross-uses of data, so implementing the framework may not be feasible in practice. As we have noted, data legitimately obtained and processed for one purpose may later be put to different uses in a way that is hard to constrain.[290] Such repurposing and reuse may be a result of legitimate as well as illegitimate transfers (e.g., leaks, hacks, and theft). A broader concern is that policymakers' desire to punish crimes or guarantee public safety will drive ever more comprehensive data collection, and that data will inevitably be used for an increasingly broad range of purposes.[291]

Fifth, some may prioritize countervailing values (e.g., privacy, intellectual flourishing, and preservation of community values) and thus value slack even more than our framework does. For some, a highly efficient legal system in which the government has 100% transparent information about everyone and is able to use that information is fundamentally disturbing, even if such uses are perfectly and optimally attenuated.[292] Deontological-leaning arguments that prioritize slack despite potentially adverse outcomes are regularly made in the context of surveillance and national security.[293] Similar intuitions are reflected elsewhere in the law, for example, in Fourth Amendment protections against

288. *See, e.g.*, Lohr, *supra* note 257.

289. *See* Price, *supra* note 17.

290. *See* sources cited *supra* note 176.

291. *See generally* sources cited *supra* note 78; Martin, *supra* note 193 (discussing how data used for one purpose gets appropriated for another); *see also* Amy Dockser Marcus, *Customers Handed Over Their DNA. The Company Let the FBI Take a Look*, WALL ST. J. (Aug. 22, 2019), https://www.wsj.com/articles/customers-handed-over-their-dna-the-company-let-the-fbi-take-a-look-11566491162.

292. *See* Richards, *supra* note 2.

293. *See, e.g.*, *id.*

unreasonable searches and seizures that are grounded in the view that important values must be weighed against improved enforcement.[294]

Finally, and related to the point above, some may worry about the changing relationship between government and society if law's design changes dynamically to reflect changes in slack and data. For example, some might view *ex ante* nudges as unduly paternalistic and may resist their use, even if increased data permits it.[295]

These complicating factors suggest that while abstract principles are easy to articulate, reality is far messier. In practice, policymakers may have to choose between erring on the side of collecting, processing, and using data despite potentially problematic consequences and refraining from doing so despite the potential benefits. These decisions will often have to be made without complete information. As articulated in Part I.C, our view is that there remain compelling arguments in favor of preserving some slack in the legal system. As noted, though, our position does invite counterarguments, as slack holds clear risks. The case for preserving slack therefore represents a classic uneasy case.

In short, the policy approach we advance is a messy one: apply the basic four-part framework but with a clear appreciation for the complexifying factors and with a tilt in the direction of adopting data policies that protect slack where appropriate.

B. Concrete Policy for the Data Age

We now discuss three concrete policy approaches that can be taken to safeguard slack: (1) greater aggregate constraints on collection and storage of data, (2) policies that rely on data silos and the architecture of information to prevent inappropriate cross-uses, and (3) measures that attenuate data's negative impacts, including reform of legal rules such as statutes of limitations and penalties and fundamental rethinking of the role of government with respect to compliance and enforcement. Our analysis concentrates on the safeguarding of slack, rather than explicating how data can be used more effectively, in recognition of the fact that the contemporary trend is already in the direction of ever-increasing data usage. Thus, the important policy edge is the one that looks at constraints on such uses.

Two important caveats: First, we do not attempt to identify an ideal mix of interventions. Rather, our goal is simply to delineate potential responses. Second, some of our proposals map on to reforms that others have advanced

294. *See, e.g.*, Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 767–70 (2012) (noting tradeoff built into exclusionary rules if we assume officers care about securing convictions); *see also* sources cited *supra* note 22.

295. *See, e.g.*, CASS R. SUNSTEIN, WHY NUDGE?: THE POLITICS OF LIBERTARIAN PATERNALISM 128 (2014).

to manage privacy risks.[296] Our concerns and proposed solutions overlap with, but are not identical to, those raised by privacy scholars. Our argument is that in addition to constitutional and deontological concerns about privacy and its loss, data raises serious questions about how law is designed and enforced by imperfect government against the imperfect governed. These questions run parallel to privacy debates but are not the primary focus of the privacy literature. In fact, our view is that a better appreciation of the relationships among data, data privacy, and slack illuminates the consequentialist underbelly of even deontological privacy debates.

1. Limiting Data Collection and Storage

Preserving slack requires limiting data collection and accumulation.[297] Private sector actors of all kinds (companies, social media platforms, commercial actors) already collect vast quantities of data, and our current legal framework seems largely powerless to stop this.[298] Governments, too, collect extensive data through their enforcement, regulatory, and oversight functions, including through border-control, policing, licensing, registration, permitting, tax, and social security systems.[299] Governments have strong incentives to improve and expand data collection to enhance security, enforcement, and efficiency, particularly in competition with the private sector and particularly in times of crisis (such as a public health or national security emergency).[300] In crisis times, the public may be least resistant to a government data grab.[301]

Given the already pervasive data collection by private and public sector actors, a strategy that focuses on limiting collection and storage may seem doomed to fail. But some limits remain possible. Regulation can circumscribe what can be collected and stored, by either establishing upfront limitations on collection, terminating collection, or demanding erasure at a certain point. One strategy that has been explored is to use default rules that make data collection an opt-in.[302] Defaults that preserve privacy unless waived are likely to be more

296. *See* sources cited *infra* notes 311–312 and accompanying text.

297. The types of data and privacy interventions we consider go beyond "right to erasure" concerns animating European Union initiatives such as the "right to be forgotten." Directive 95/46, art. 12, 1995 O.J. (L 281) 31 (EC); Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

298. *See* Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), https://www.osano.com/articles/data-privacy-laws.

299. *See generally* Eleni Kosta & Magda Brewczynska, *Government Access to User Data: Towards More Meaningful Transparency Reports*, (Tilburg Inst. L., Tech., & Soc., Law & Tech. Working Paper Series, 2019) (discussing businesses' roles in providing transparency regarding government access to privately held data).

300. Tiffany C. Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 LOY. U. CHI. L. REV. 767 (2021); *see* sources cited *supra* note 172.

301. *See, e.g.*, Li, *supra* note 300, at 789.

302. *Cf.* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2020) (allowing consumers to opt out).

effective than disclosure-based solutions such as website cookie notifications that require the user to understand and affirmatively opt out.[303]

Serious challenges have accompanied efforts to develop more comprehensive regulation of government data collection. The trend in the European Union[304] towards more protection for individuals' data has not taken hold in the United States. Domestic agendas and concerns, such as the pressure to tighten U.S. borders,[305] favor increasing government access. Moreover, data-collection efforts of foreign governments and entities may be beyond the reach of U.S. regulation. Foreign governments, agencies, and bodies have sought to amass data on other countries' citizens, residents, corporations, and governments on matters of finance, politics, military security, and more.[306] For example, the February 2018 Department of Justice indictment of Russian individuals working with the Internet Research Agency in St. Petersburg details the alleged use of stolen identities of U.S. persons to post to social media accounts, open financial accounts, and create false identification documents.[307] Russia-based actors have also used false Facebook accounts to extract information from U.S. business owners.[308] Such foreign interventions do not directly dictate the level of data-related powers a country should permit for its own government, but they do create a potential imbalance in data access between domestic and foreign actors, which could ultimately constrain impulses to limit data collection.

2. Data Architecture and Data Silos

Given the difficulties with limiting overall data collection, another approach is to construct data silos that constrain the uses—and particularly, the cross-uses—of data after its collection. As we have discussed, examples such as the use of state driver's license databases and commercially purchased databases for federal immigration purposes vividly illustrate how data collected by one set of actors can be sold and used by another.[309] They also show how multiple data

303. *See, e.g.*, Franz Werro, *The Right to Inform v. The Right to be Forgotten*, *in* LIABILITY IN THE THIRD MILLENNIUM 285 (Ciacchi et al. eds., 2009).

304. *See*, *e.g.*, sources cited *supra* note 297.

305. *See* sources cited *supra* note 181.

306. *See, e.g.*, Indictment, United States v. Zhiyong, No. 2:30 CR 046 (N.D. Ga. Jan. 28, 2020) (charging four members of the Chinese military with hacking Equifax computers and obtaining the names, birthdates, and social security numbers of 145 million Americans).

307. Indictment ¶¶ 4, 41, 70, 89, United States v. Internet Research Agency LLC, 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

308. Shelby Holliday & Rob Barry, *Russian Influence Campaign Extracted Americans' Personal Data*, WALL ST. J. (Mar. 7, 2018), https://www.wsj.com/articles/russian-influence-campaign-extracted-americans-personal-data-1520418600.

309. *See* Harwell, *supra* note 234.

sources are increasingly easy to combine, generating unforeseen insights and unexpected consequences.[310]

As we have argued, slack may be more or less justifiable depending on context. Thus, a legal regime capable of controlling data flows and transfers based on context is a plausible solution. For example, explicit rules that permit governments to request data for serious crimes but limit access for less serious violations could be enacted. Restrictions on information access by those trying to enforce unjust laws may also be necessary. This siloing might be accomplished through restrictions on data transfers by private sector actors or limits on governments' ability to request and buy data or both.[311] Along these lines, Professors Jack Balkin and Jonathan Zittrain have suggested an "information fiduciaries" framework for considering how companies like Google and Facebook should be held responsible for how they collect, use, sell, and share data.[312]

The idea of siloing data to constrain problematic cross-uses predates the data age. The tax system, for example, has historically exercised tight controls on tax return data; a court order is required to compel the IRS to share tax return information with law enforcement agencies for investigation and prosecution of nontax criminal laws.[313] Similar restrictions could be put in place that restrict governments' ability to use data collected for one purpose for another, that constrain governments from obtaining data from private actors, or that restrict how such data, if obtained, may be used.[314]

Constructing data silos requires line drawing, which is challenging. Calibrating data access based on the formal level of the crime—such as felony versus misdemeanor status—may raise questions at the boundaries but does not seem unduly burdensome. More challenging would be drawing lines between laws that are unjust or out of step and those that are not, or

310. *See, e.g.*, Zraick & Zaveri, *supra* note 181; Funk, *supra* note 171; Tau & Hackman, *supra* note 235.

311. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1194–96 (2016) (distinguishing collection, use, disclosure, and sale of information).

312. *Id.* at 1186, 1205–09 (proposing that online service providers and cloud companies be viewed as information fiduciaries towards customers and users); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 13–29 (2020); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (proposing information fiduciaries framework); Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for; *see also* Tim Wu, *An American Alternative to Europe's Privacy Law*, N.Y. TIMES (May 30, 2018), https://www.nytimes.com/2018/05/30/opinion/europe-america-privacy-gdpr.html; Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. UNIV. L. REV. (forthcoming 2021) (manuscript at 20-22); Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. (forthcoming 2021) (manuscript at 33–49), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265#.

313. 26 U.S.C. § 6103(i)(1).

314. For a "takings clause"-inspired approach to curtailing government access to internet service provider data, see Michael C. Pollack, *Taking Data*, 86 U. CHI. L. REV. 77 (2019).

determining which governments or agencies should be denied access to data.[315] In addition, institutional questions regarding where authority for data-use decisions should rest must be resolved. Vesting such authority in courts is one possibility, but the judicial system moves slowly. Another possibility is to vest authority to protect data and curb abuses in an independent agency, an auditor within an existing agency, or another ombudsperson.

Moreover, there are possible objections to data silos. First, a tightly controlled data spigot may smell like information dictatorship, in which governments not only collect and control data but also set the terms under which the data can be used. Those who advocate an "information wants to be free" position might be skeptical of a data-silo approach.[316] Second, the fact that a business or government possesses data and is constrained from using it but can continue to monitor and surveil data subjects has impacts reaching far beyond actual liability for misconduct. The mere threat of potential future data use operates as a form of social control. Third, construction of data silos may simply be unrealistic due to data's nonrival nature and the corresponding pressure to allow markets for data to exist. Fourth, data silos may face regular illegal breaches if information exists but is not made available to resolve certain violations. Fifth, data silos may incentivize governments to put more effort into accumulating their own data troves if they find themselves shut out from obtaining data from others.

Ultimately, a silo-based approach runs counter to broader trends toward fuller transparency and disclosure. In the international tax context, for example, the trend has recently shifted to permitting broader use of taxpayer information and more widespread information exchange.[317] Implementation of such silos would require a clear shift.

---

315. We have seen these complex pressures in the international tax context when determining how to limit the exchange of tax data with jurisdictions that have corruption or rule-of-law issues and with those that might not adequately protect exchanged data. *See* Irma Mosquera Valderrama, *Exchange of Information and the Rule of Law: Confidentiality and Safeguards for the Automatic Processing of Data in a World of Big Data*, GLOBTAXGOV (Jan. 12, 2020), https://globtaxgov.weblog.leidenuniv.nl/2020/12/01/exchange-of-information-and-the-rule-of-law-confidentiality-and-safeguards-for-the-automatic-processing-of-data-in-a-world-of-big-data. One solution has been peer reviews of countries regarding compliance with data protection standards. *See Global Forum on Transparency and Disclosure of Information for Tax Purposes*, ORG. FOR ECON. COOP. & DEV., http://www.oecd.org/tax/transparency/about-the-global-forum/publications/revised-methodology.pdf.

316. *See, e.g.*, Wagner, *supra* note 129.

317. *See, e.g.*, ORG. FOR ECON. COOP. & DEV., ARTICLES OF THE MODEL CONVENTION WITH RESPECT TO TAXES ON INCOME AND ON CAPITAL 23 (2003), https://www.oecd.org/tax/treaties/1914467.pdf (furnishing an exchange of information treaty provision that serves as the basis for many bilateral treaties). Data use is now permitted if the laws of both treaty partners allow it and if authorized by the information-supplying state. *Id.* The OECD has also recently made efforts to enlarge countries' access to taxpayer data outside of the bilateral treaty context. *See, e.g.*, ORG. FOR ECON. COOP. & DEV., ACTION 13: COUNTRY-BY-COUNTRY REPORTING: AUTOMATIC EXCHANGE OF INFORMATION 9-13 (2015), https://www.oecd.org/ctp/transfer-pricing/beps-action-13-country-by-country-reporting-implementation-package.pdf.

3. Broader Strategies

Aside from data protections and siloing, the data age requires recalibration and redesign of substantive legal rules. This obviously affects the content and structure of legal regimes and sanctions. Even more fundamentally, though, it requires rethinking of the relationship between government and the governed. Redesign of technical rules and a broader reimagining of the role of government vis-à-vis the governed can help temper the effects of government overreach. As data grows more ubiquitous, enforcement-based interactions with government are likely to increase disproportionately for those who are least sophisticated and already most targeted. Recalibrating legal rules and reimagining government can help modulate the costs and burdens of these interactions.

a. Recalibrating Underlying Law

Two obvious possible adjustments to legal rules pertain to penalties and statutes of limitations. Another involves explicit protections for populations most likely to be prejudiced by decreasing slack due to data.

Design of Penalties. Where existing law relies on high fines and stiff penalties to achieve deterrence when the likelihood of detection is low, these penalties should arguably be revisited if detection becomes significantly easier after data. With easier detection, the *in terrorem* effect of high penalties is no longer needed.[318] Thus, from both an economically optimal viewpoint and a fairness one, penalties should be reduced. Take the dog registration example discussed above.[319] If, with data, it becomes easy for authorities to reliably and accurately detect all dogs in the city and their owners, then arguably the $5,000 fine should be lowered. Or, take the 2010 FATCA tax legislation discussed above, which imposed heightened penalties for foreign financial asset reporting failures.[320] FATCA penalties should perhaps be lessened now that foreign financial information is easily available given information sharing. Similar arguments apply in other areas of law and regulation.[321] Of course, policymakers should avoid the flipside risks, where overly low penalties convert penalties into a "price" that actors may simply choose to pay rather than comply.[322]

---

318. *See* Lana Friesen, *Certainty of Punishment versus Severity of Punishment: An Experimental Investigation*, 79 S. ECON. J. 399, 399–402 (2012).

319. *See supra* Part II.B.6.

320. *See supra* notes 259–263 and accompanying text.

321. *See, e.g.*, LAWS. COMM. FOR CIV. RTS. OF THE S.F. BAY AREA, PAYING MORE FOR BEING POOR 3, 9–19 (2017), https://www.lccr.com/wp-content/uploads/LCCR-Report-Paying-More-for-Being-Poor-May-2017.pdf (assessing disproportionate impacts of excessively high traffic fines and costs on the poor).

322. *See, e.g.*, Uri Gneezy & Aldo Rustichini, *The Second Day-Care Center Study*, ARIEL RUBINSTEIN (Sept. 2005), http://arielrubinstein.tau.ac.il/papers/WC05/GR1.pdf; Uri Gneezy & Aldo Rustichini, *A Fine is a Price*, 29 J. LEGAL STUD. 1 (2000); Michael N. Stagnaro, Antonio A. Arechar & David G. Rand, *From Good Institutions to Generous Citizens: Top-Down Incentives to Cooperate Promote Subsequent Prosociality But Not Norm Enforcement*, COGNITION (Oct. 2017),

Statutes of Limitation. As available data expands, more attention should also be paid to statutes of limitations for detection and sanctions. Some statutes of limitation reflect the reality that governments may need time to uncover evidence required to enforce or prosecute.[323] A risk, however, is that as data becomes ubiquitous and indefinitely storable, government authorities may sit on data, take their time to process it, and then, years down the road, impose sanctions as a "gotcha." An appropriate organizing concept for designing statutes of limitations in the data age might be something along the lines of a "right to timely use of one's data," especially in situations where it is not obvious to the data subject that they violated the law.[324] Current law already captures this sentiment in some cases where, for example, certain crimes involving high degrees of harm (such as murder) do not have a statute of limitations but others do.[325]

Well-designed statutes of limitation give enforcers an incentive to act on increasingly available data in a reasonably diligent way. Returning again to the tax example: current tax law contains extended statutes of limitations for cross-border income and financial asset reporting omissions on the theory that information about foreign assets is hard for governments to obtain.[326] As offshore data troves become increasingly available, however, extended limitations periods have become less necessary and the attendant benefits may no longer outweigh the risks.[327]

Decisions to tweak statutes of limitation may have unintended consequences. If limitations periods are shorter, this may generate even more pressure to collect and use data and to develop greater capacity to mine and process data into useable information, which may raise even greater privacy concerns. A key question going forward is whether a well-designed, middle-ground policy can be reached.

Protection of Vulnerable Populations. Finally, some populations may be sufficiently at risk that we should consider giving them special data protections. Children, young adults, digital migrants, and the elderly may each experience particular vulnerabilities. For example, children may have their images widely and publicly posted by parents, with surveillance consequences that are just now

---

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5875418/pdf/nihms864083.pdf; Kristen Underhill, *When Extrinsic Incentives Displace Intrinsic Motivation: Designing Legal Carrots and Sticks to Confront the Challenge of Motivational Crowding-Out*, 33 YALE J. ON REG. 213, 218-32 (2016).

323. For example, in tax law, some foreign asset reporting violations carry lengthy statutes of limitation. 26 U.S.C. §§ 6501(e)(1)(A)(ii), 6501(c)(8)(A).

324. *See* Scott Turow, Opinion, *Still Guilty After All These Years*, N.Y. TIMES (Apr. 8, 2007), https://www.nytimes.com/2007/04/08/opinion/08turow.html.

325. *See, e.g.*, 18 U.S.C. § 3281 (no statute of limitations under federal law for capital offenses); *see* CHARLES DOYLE, CONG. RSCH. SERV., RL 31253, STATUTE OF LIMITATION IN FEDERAL CRIMINAL CASES: AN OVERVIEW, 1–2 (2017).

326. *See, e.g.*, sources cited *supra* note 323.

327. *See* Lindsey Powell, *Unraveling Criminal Statutes of Limitations*, 45 AM. CRIM. L. REV. 115, 128–35 (2008).

becoming salient.[328] Digital migrants and the elderly may be less cognizant about how to safeguard data and the risks of sharing it and may be more susceptible to data theft.[329] While educating individuals about the risks of data sharing is important, education-based interventions are unlikely to be sufficient by themselves.

Given that vulnerable populations are likely to bear the disproportionate brunt of the expanding use of data for law enforcement and regulation, it is reasonable to think that law should be tailored to accommodate such vulnerabilities. The criminal law system already incorporates some of these ideas in its management of juvenile criminal records.[330] But going forward, the issues will be much broader and some of the solutions less obvious. In some cases, the relevant data may be in the hands of the private sector, and uses may span a wide range of legal, professional, and social contexts. At that point, a regime more comprehensive than simply sealing juvenile records would be required.

b. Rethinking Noncompliance and the Role of Government

Perhaps most fundamentally, ubiquitous data demands a deeper shift in how we understand the meaning of enforcement, compliance, and the relationship between government and governed.

Changing Meanings of Noncompliance. The social and expressive meaning of noncompliance is changing in the data age. One effect of increasingly omnipresent data is that humans have more information about their actions and can self-monitor more effectively. However, while data may improve human conduct and propel better decision-making, perfect conduct and 100% compliance remain unlikely.[331] In a society with many laws, we can expect that humans will still regularly violate the law. For example, humans will continue to speed, may forget to pay speeding tickets, or may continue to make errors in their tax returns.

We do not attempt a deep explanation of why humans comply imperfectly. Our point is that if humans are failing at perfection even with the knowledge that data is available and enforcement increasingly likely, this probably signals that at least some offenders may not be deliberately "trying to get away with it"

---

328. *See, e.g.*, Kashmir Hill & Aaron Krolik, *How Photos of Your Kids are Powering Surveillance Technology*, N.Y. TIMES (Oct. 11, 2019), https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html.

329. *See, e.g.*, Steven Petrow, *You're Sharing Your Cell Phone Number Too Frequently*, USA TODAY (June 20, 2017), https://www.usatoday.com/story/tech/columnist/stevenpetrow/2017/06/20/cell-phone-number-scams-identity-theft/102787432/.

330. *See* Joy Radice, *The Juvenile Record Myth*, 106 GEO. L.J. 365, 374 (2018).

331. *See, e.g.*, Elizabeth F. Loftus & Hunter G. Hoffman, *Misinformation and Memory: The Creation of New Memories*, 118 J. EXPERIMENTAL PSYCH.: GEN. 100 (1989); Ganapathi Bhat Manchi et al., *Study on Cognitive Approach to Human Error and its Application to Reduce the Accidents at Workplace*, 2 INT'L J. ENG'G & ADVANCED TECH. 236 (2013); JAMES REASON, HUMAN ERROR 1–19 (1990).

but rather are failing due to inattention, inability to cope, bounded rationality, processing capability, or some other human imperfection.[332] If so, then one might argue, as other scholars have, that compliance failures that continue to occur after a data and information explosion carry a different meaning and should give rise to different legal consequences.[333] This may suggest adjusting the levels of seriousness ascribed to certain offenses after data, for example, regarding them as infractions or misdemeanors rather than something more serious.

Government as Compliance Coordinator. Along the same lines, it may make more sense in a world of burgeoning data to have government act as *ex ante* compliance coordinator rather than *ex post* punisher in at least some contexts. As a compliance coordinator, the government's priority would shift toward using increasingly available data and information to affirmatively help people to comply with the law, rather than using information primarily as part of the *ex post* enforcement toolkit. A compliance coordinator approach suggests redesigning systems to make compliance easier paired with reasonable fines for noncompliance. Returning to the dog registration example,[334] we could have the city automatically register dogs and pair this with an easily accessible avenue for residents to appeal mistakes. This approach would arguably make more sense than placing the obligation on each dog owner to self-register and punishing failure with an *ex post* fine. Alternatively, the duty to register could remain with the dog owner, but the locality could have an accurate and fast system of corroboration, with failure to register treated as a foot fault given the virtual certainty of detection. In the tax context, more robust tax withholding and third-party reporting of independent contractor payments could reduce income reporting or estimated tax payment failures.[335] Such government-facilitated automation of income reporting and tax payment could increase compliance and decrease the *ex post* enforcement role of tax authorities.

Our suggested move towards a "compliance coordinator" understanding of government is not wholly new. Threads of this instinct run through various policy proposals. For example, this reasoning underpins proposals like Casey and Niblett's call for personalized "microdirectives" that can replace traditional legal rules and standards,[336] as well as arguments recommending that structures and technologies be designed to make violation of the law impossible.[337] In tax law, the so-called "ready return"—a tax return prepared by the government for

332. *See, e.g.*, HERBERT A. SIMON, MODELS OF BOUNDED RATIONALITY (1982).

333. *See, e.g.*, Brownsword & Harel, *supra* note 282, at 111; R.A. Duff, *Perversions and Subversions of Criminal Law*, *in* THE BOUNDARIES OF THE CRIMINAL LAW, 88, 88–112 (R.A. Duff et al. eds., 2010) (noting change in regulatory signal).

334. *See supra* Part II.B.6.

335. *See, e.g.*, Kathleen DeLaney Thomas, *Taxing the Gig Economy*, 166 U. PA. L. REV. 1415, 1473 (2018) (suggesting non-employee tax withholding).

336. *See* sources cited *supra* note 276.

337. Rademacher, *supra* note 25.

the taxpayer, which the taxpayer then reviews and submits—is floated as an example of how the government could use information *ex ante* to help taxpayers comply, rather than amassing data as a weapon to punish *ex post*.[338] Other countries, including the U.K. and Sweden, already employ a ready-return approach to varying degrees.[339] While the prospect of a government-prepared tax return has critics, it is an obvious example of how governments' role might change in light of data and technology.

A compliance coordinator frame may also suggest amendments to existing laws. Returning to FATCA tax reporting[340] of foreign financial assets, a compliance coordinator approach might envision that once information about offshore financial assets is available and reliable, the government should either assume primary responsibility for preparing the return or should help taxpayers prepare an accurate return (for example, by giving taxpayers a copy of the information reported to it by offshore banks). Moreover, the government should treat errors that continue to be made after data becomes widely available as good-faith foot faults rather than assuming bad intent.[341] Currently, the law continues to impose high penalties for omissions despite the government's possession of the information.[342]

An Important Role for Sunshine. A compliance coordinator approach does pose risks. It may weaken deterrence and allow those who can afford to do so to violate the law and simply pay a fine.[343] Shifts to *ex ante* coordination and monitoring rather than *ex post* sanctioning might also raise even more privacy concerns. Some might find it disturbing for the government to spy on our dogs and prepare our tax returns and give us microdirectives. A second-order concern is that once law starts to be designed this way, it may serve as an excuse for governments to become data monsters, amassing more and more data in

338. *See* Joseph Bankman & James Edward Maule, *Perspectives on Two Proposals for Tax Filing Simplification*, AM. BAR. ASS'N (Aug. 25, 2016), https://www.americanbar.org/groups/taxation/publications/abataxtimes_home/16aug/16aug-pcp-bankman-maule-perspectives-on-two-proposals-for-filing-tax-simplification/ (debating data retrieval and pro forma tax return proposals); *see also* AUSTAN GOOLSBEE, THE SIMPLE RETURN: REDUCING AMERICA'S TAX BURDEN THROUGH RETURN-FREE FILING 5–6 (2006), https://www.brookings.edu/wp-content/uploads/2016/06/200607goolsbee.pdf.

339. *See* Bankman & Maule, *supra* note 338; Ezra Klein, *What Denmark, Sweden, and Spain Could Teach America About Taxes*, VOX (Apr. 15, 2015), https://www.vox.com/2015/4/15/8420257/taxes-IRS-automatic-turbotax.

340. *See supra* notes 259–263 and accompanying text.

341. This change would equalize the treatment of reporting failures involving offshore assets with failing to include income reported on a domestic Form 1099 or W-2.

342. While there are lower penalties for non-willful violations, U.S. tax authorities have applied a strict standard for finding failures to be non-willful. *See, e.g.*, Lee A. Sheppard, *Nerds and Cops, Part 3: The New Matrix*, 94 TAX NOTES INT'L 399, 402–04 (April 29, 2019) (noting that the IRS and courts have effectively accepted a "willful blindness" standard); *see also* United States v. Williams, 489 F. App'x 655, 658–60 (4th Cir. 2012); United States. v. McBride, 908 F. Supp. 2d 1186, 1204–05 (D. Utah 2012).

343. *See* sources cited *supra* note 322.

the interests of coordinating compliance.[344] Finally, a move to *ex ante* coordination (particularly if assisted by technology) may lead to erosion of moral instincts and community moral aspirations.[345]

All this suggests that sunshine and transparency will be important in mediating the changing relationship between governments and the governed post data. As discussed, we are skeptical that sunshine alone will be enough to prevent problematic outcomes, but it may nonetheless help ameliorate enforcement disparities and other problems.[346] Sunshine may take the form of disclosure to data subjects regarding the collection and use of their data. Or, it may take the form of disclosure to the general public about data use, which can generate press coverage to help curb problematic enforcement or to foment outrage in its wake. We have already seen ways in which sunshine has been used to promote government accountability. One example that has gathered momentum in recent years is the use of police body cameras.[347] Although not a precise parallel, such cameras collect extensive data on police–public interactions and can be available to those seeking to assess potential bias.[348] Requirements that police maintain statistics on traffic stops also allow observers to monitor for bias.[349]

In some circumstances, there may be valid reasons for limiting sunshine. In tax law, for example, preserving the effectiveness of IRS audit strategies may require keeping reasons for audit decisions secret.[350] But other alternatives could offer meaningful oversight, whether through independent auditors or procedures for contesting decisions. Tax law has balanced the need for secrecy with the need for accountability by instituting the Office of the National Taxpayer Advocate, an independent ombudsperson charged with protecting taxpayer rights.[351] The creation of the Taxpayer Advocate was motivated in part by the difficulty of checking potential IRS abuses while simultaneously safeguarding its enforcement capabilities.[352] By creating an independent accountability auditor, the Taxpayer Advocate option arguably affords a

344. These types of objections have been raised to the tax "ready return." *See* Bankman & Maule, *supra* note 338.

345. Brownsword & Harel, *supra* note 282, at 112; Rademacher, *supra* note 25, at 47, 50; Rich, *supra* note 24, at 845.

346. *See supra* Part II.B.3.

347. *See generally* Alexandra Mateescu et al., *Police Body-Worn Cameras* (Data & Soc'y Rsch. Inst., Working Paper, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2569481.

348. *See* Kami Chavis Simmons, *Body-Mounted Police Cameras: A Primer on Police Accountability vs. Privacy*, 58 HOWARD L.J. 881, 884–87 (2015).

349. *See, e.g.*, WILLIAM R. SMITH ET AL., THE NORTH CAROLINA HIGHWAY TRAFFIC STUDY 1-4 (2003), https://www.ojp.gov/pdffiles1/nij/grants/204021.pdf.

350. *See* sources cited *supra* note 208.

351. 26 U.S.C. § 7803(c).

352. *See* Samuel D. Brunson, *Watching the Watchers: Preventing I.R.S. Abuse of the Tax System*, 14 FLA. TAX REV. 153, 175–78 (2013).

compromise between complete government secrecy and complete transparency to the public.[353]

In establishing an independent ombudsperson or avenues for recourse, policymakers should be careful that inequities are not perpetuated. Less sophisticated or lesser resourced demographics may be less likely to appeal decisions or turn to an ombudsperson or other procedural recourse.[354] In addition, some types of data-related complaints might prove easier to resolve than others. For example, it may be relatively easy to appeal a harsh penalty on the grounds that ten other similarly situated persons have been given a lighter penalty. But it may be harder to show that someone else has been unfairly let off the hook while one has been punished. The second species of legal challenge requires uncovering specific incidents and facts, which may require whistleblowing and due diligence reviews. Ultimately, stronger legal rules facilitating such whistleblowing and diligence may be needed.

CONCLUSION

The data age is upon us, and increasingly ubiquitous data threatens the existence of slack, the informal latitude to fall short of law's requirements without being held accountable. There are significant risks that use of data is causing slack to contract unfairly for some populations more than others. This Article has argued that slack in our legal system derives from multiple sources and is sometimes deeply problematic but nonetheless serves an important function.

A critical conundrum facing our legal system going forward is whether it is possible to use and deploy data effectively while preserving slack where appropriate and allocating it fairly. Solving this conundrum is especially challenging given that laws are heterogeneous and that data is both nonrival and hard to effectively silo. This Article has articulated a framework for managing the slack-data relationship, and it has outlined policy solutions for managing data's effects, including limits on data collection and storage, use of data silos to constrain access and use, and fundamental recalibration of legal rules and the government–governed relationship.

The solutions we have offered are not perfect. They may bump up against the First Amendment and "right to be informed" concerns,[355] may be deemed unfeasible in light of competitive pressures from foreign powers, or may clash with law enforcement and crime prevention goals. These are tensions that will have to be managed going forward. Data is already pervasive, and more is

353. *See generally* Ashley Deeks, *Secrecy Surrogates*, 106 VA. L. REV. 1395 (2020).

354. As has been shown in the property tax context, the likelihood of appealing a property tax assessment varies by demographic, with racial minorities less likely to appeal. Andrew J. Hayashi, *The Legal Salience of Taxation*, 81 U. CHI. L. REV. 1443, 1447 (2014).

355. Balkin, *supra* note 311; Werro, *supra* note 303.

coming. Failure to acknowledge data's power in shaping real-world enforcement and in reshaping the availability of slack in the system will predictably burden the most disadvantaged members of society. The design choices we make today, including inaction, will have significant distributional and expressive consequences.